ECD_CO_1001_Declaración de prácticas de certificación

Lleida SAS
Colombia- Bogotá

Contenido

1 CONTROL DOCUMENTAL

Esta sección refleja la información del documento, sus propiedades y el historial de versiones.

1.1 Histórico de versiones

Versión	Fecha	Autor	Descripción
1	30/07/2021	Eva Pané	Versión inicial
2	03/03/2022	Gloria Salvador	Incorporación servicios PKI
3	17/06/2022	Gloria Salvador	Mejoras PKI
4	13/12/2022	Gloria Salvador	Modificación certificados
4.1	03/05/2023	Gloria Salvador	Referencias acreditación ONAC
4.2	19/09/2023	Gloria Salvador	Mejoras redacción
4.3	28/11/2023	Gloria Salvador	Cambios aplicativos y tipo de firma
4.4	05/08/2024	Eva Pané	Revisión documental, modificación URLs y eliminación de apartados de "Renovación" y "Suspensión"
4.5	13/3/2025	Eva Pané	Eliminación previsión expedición software PKCS#12. Se añade definición PKCS#10. Se incorporan apartados de "Suspensión" y "Renovación" siguiendo indicaciones de auditoria tercera parte.

1.2 Lista de distribución

Empresa
Lleida SAS

1.3 Clasificación y estatus

Clasificación	Estatus
Uso Interno	Aprobado

1.4 Documentos referenciados

Descripción

2 INTRODUCCIÓN

2.1 Resumen

La **Declaración de Prácticas de Certificación** (a partir de ahora, DPC) es un documento elaborado por LLEIDA SAS, (en adelante LLEIDA.NET), que actuando como Entidad de Certificación Digital (en adelante ECD), contiene las normas, declaraciones sobre las políticas y procedimientos que la ECD como Prestador de Servicios de Certificación Digital (PSC) aplica como lineamiento para prestar los servicios de certificación digital de acuerdo a lo establecido en la Ley 527/1999, el Decreto 0019 de 2012, el Decreto 333 de 2014. el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementes, en el territorio de Colombia.

La DPC está conforme con los siguientes lineamientos:

i. Criterios Específicos de Acreditación para las Entidades de Certificación Digital CEA-3.0-07 Versión 2 (en adelante CEA) que deben ser cumplidos para obtener la Acreditación como Entidad de Certificación Digital-ECD, ante el Organismo Nacional de Acreditación de Colombia- ONAC
ii. La DPC está organizada bajo la estructura definida en el documento RFC3647 Internet x.509 Public Key Infrastructure Certificate Policy and Certificacion Practice Framework de grupode trabajo IETF-The Internet Engineering Task Force (que sustituye a la RFC2527)

La actualización y/o modificación de la DPC, se realizará a través del procedimiento establecido por LLEIDA.NET de información documentada, cualquier cambio o adecuación sobre el documento deberá ser revisado, analizado y aprobado por el Comité de Seguridad.

DATOS DE LLEIDA S.A.S.:

Razón social:	LLEIDA S.A.S.
N.I.T.	900571038-3
Dirección:	Calle 81 # 11 – 55 Oficina 903 de Bogotá D.C
Ciudad/País	Bogotá/Colombia
Teléfono:	+5713819903
Correo electrónico:	co@lleida.net
Página web:	www.lleida.net/co
Nº Certificado Acreditación	22-ECD-009
Certificado Acreditación	22-ECD-009.pdf (onac.org.co)

2.2 Peticiones, quejas, reclamos, solicitudes y apelaciones

Las peticiones, quejas, reclamos, solicitudes y apelaciones sobre los servicios prestados por LLEIDA.NET o entidades subcontratadas, explicaciones sobre esta DPC y sus políticas; son recibidas y atendidas directamente por LLEIDA.NET como ECD y serán resueltas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, para lo cual se disponen de los siguientes canales para la atención a suscriptores, responsables y terceros.

Teléfono: +57 (1) 3819903
Correo electrónico: clientes@lleida.net
Página Web: www.lleida.net/co
Responsable: Área de Atención al Cliente

Una vez presentado el caso, este es trasmitido con la información concerniente al área de Atención al Cliente según procedimiento interno establecido para la gestión de estas, una vez recibida la queja se realiza seguimiento para dar respuesta oportuna al cliente.

Recibida la PQRS se procede a realizar la investigación respectiva para determinar si existe o no la queja, reclamo o apelación. En caso de existir, se determina qué área es responsable de tomar acciones administrativas o técnicas y si se requiere adoptar acciones correctivas o preventivas, caso en el cual se debe aplicar el procedimiento de acciones.

Generada la investigación se procede a evaluar la respuesta para posteriormente tomar la decisión que resuelve la queja y su comunicación final al suscriptor, responsable o parte interesada.

2.3 Nombre e identificación del documento

La DPC para ECD se denominará "Declaración de Prácticas de Certificación (DPC). La versión cambia de acuerdo con las modificaciones sobre el mismo documento.

LLEIDA.NET es una empresa registrada (Registered Private Enterprise) ante la organización internacional IANA (Internet Assigned Numbers Authority), con el código privado No 53589 bajo la rama 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). La anterior información puede ser consultada en la URL, haciendo la búsqueda por el código 52376 https://www.iana.org/assignments/enterprise-numbers

DATOS DEL DOCUMENTO:

Nombre del documento	Declaración de Prácticas Certificación de LLEIDA S.A.S
Descripción del documento	Este documento se describe las operaciones y prácticas que utiliza LLEIDA S.A.S. para la administración de sus servicios como Entidad de Certificación Digital
Versión	2
OID	1.3.6.1.4.1.53589.1.2.1
Localización	https://www.lleida.net/docs/es/colombia-declaracion.pdf

2.4 Marco Jurídico

La ejecución, interpretación, modificación o validez de la presente DPC y sus correspondientes anexos se regirá por lo dispuesto en la legislación colombiana vigente.

Particularmente:

- Decreto Único del Sector Comercio, Industria y Turismo - DURSCIT, 1074 de 2015. Que compila todas las normas que rigen los sectores de comercio, industria y turismo del país, y entre ellas las relacionadas con el Subsistema Nacional de la Calidad, las de firmas electrónicas y firmas digitales, y la acreditación de las entidades de certificación digital.
- Ley 527 de 1999: que regula el acceso y el uso de los mensajes de datos
- Decreto 019 de 2012, que suprime la actividad de autorización de entidades de certificación digital por parte de la Superintendencia de Industria y Comercio, y establece la obligación de acreditarse ante el Organismo Nacional de Acreditación de Colombia – ONAC.
- Decreto 620 de 2020: Lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Ley 2106 del 2019: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Ley 1581 del 2012: Por la cual se dictan disposiciones generales para la Protección de Datos Personales.
- Decreto 333 de 2014 (Regulación de las entidades de certificación)
- Ley 1898 de 2018. Autenticación y Certificados Digitales.

Adicionalmente, las prácticas de los servicios de confianza provistos por Lleida SAS 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.

2.4.1 Mecanismos de Resolución de Diferencias

Si por alguna razón surge alguna diferencia entre las Partes (suscriptor/responsable y LLEIDA.NET) con ocasión de:

i. La prestación de los servicios de certificación digital descritos en esta DPC.

ii. Durante la ejecución de los servicios contratados.

iii. Por la interpretación del contrato, DPC y cualquier otro documento entregado por LLEIDA.NET.

La parte interesada notificará a la otra parte vía correo electrónico certificado la existencia de dicha diferencia, con la información completa y debidamente sustentada de la diferencia, a fin de que dentro de los quince (15) días hábiles siguientes a dicha notificación, las Partes busquen llegar a un arreglo directo entre ellas como primera instancia.

Finalizado dicho período la(s) diferencia(s) persista(n), las Partes quedaran en la libertad de acudir ante la justicia ordinaria colombiana para hacer valer sus derechos o exigencias, que se sujetará a las normas vigentes sobre la materia, los costos que se causen con ocasión de la convocatoria estarán totalmente a cargo de la Parte vencida.

2.5 Definiciones y acrónimos

Los siguientes términos son de uso común y requerido para el entendimiento de la presente DPC.

2.5.1 Definiciones

Los siguientes términos son de uso común y requerido para el entendimiento de la presente DPC.

Entidad de Certificación Digital (EDC): Es aquella persona jurídica, acreditada conforme a la ley 527 de 1999 y el Decreto 333 de 2014, facultada por el gobierno Colombiano (Organismo Nacional de Acreditación en Colombia) para emitir certificados en relación con las firmas digitales de los clientes que las adquieran, ofrecer o facilitar

los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Entidad de Certificación Abierta: es una Entidad Certificación que ofrece servicios propios de las entidades de certificación, tales que:

a. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o

b. Recibe remuneración por éstos.

Entidad de certificación cerrada: Entidad que ofrece servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

Prestador de Servicios de Certificación (PSC). En inglés "Certificación Service Provider" (CSP): persona natural o jurídica que expide certificados digitales y presta otros servicios en relación con las firmas digitales.

La Autoridad de Certificación (CA). En inglés "Certification Authority" (CA): Autoridad de Certificación, entidad raíz y entidad prestadora de servicios de certificación de infraestructura de llave pública.

La Autoridad de Registro (RA). En inglés "Registration Authority" (RA): Es la entidad 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.

Autoridades Intermedias: Son PSC Subordinados que bajo la jerarquía de un certificado raíz emiten certificados digitales a usuarios finales.

Declaración de Prácticas de Certificación (DPC). En inglés "Certification Practice Statement" (CPS): manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

La Política de Certificación (PC). Es un conjunto de reglas que definen las características de los distintos tipos de certificados y su uso.

Certificado digital: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Esta es la definición de la Ley 527/1999 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

Estampado cronológico: Según el numeral 7 del Artículo 3° del Decreto 333 de 2014, se define como: Mensaje de datos con un momento o periodo de tiempo concreto, el

cual permite establecer con una prueba que estos datos existían en un momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento que se realizó el estampado.

Autoridad de Estampado de Tiempo (TSA). Sigla en inglés de "Time Stamping Authority": Entidad de certificación prestadora de servicios de estampado cronológico.

Solicitante: toda persona natural o jurídica que solicita la expedición o renovación de un Certificado digital.

Suscriptor: persona a cuyo nombre se expide un certificado.

Tercero de buena fe, tercero que confía, parte que confía: persona o entidad diferente del suscriptor o responsable que decide aceptar y confiar en un certificado digital emitido por la ECD.

Infraestructura de Llave Pública (PKI). Sigla en inglés de "Public Key Infrastructure": una PKI es una combinación de hardware y software, políticas y procedimientos de seguridad que permite, a los usuarios de una red pública básicamente insegura como el Internet, el intercambio de mensajes de datos de una manera segura utilizando un par de llaves criptográficas (una privada y una pública) que se obtienen y son compartidas a través de una autoridad de confianza.

Iniciador: persona que, actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.

Llave Pública y Llave Privada: la criptografía asimétrica en la que se basa la PKI. Emplea un par de llaves en la que se cifra con una y solo se puede descifrar con la otra y viceversa. A una de esas llaves se la denomina pública y se incluye en el certificado digital, mientras que a la otra se denomina privada y es conocida únicamente por el suscriptor o responsable del certificado.

Llave privada (Clave privada): valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

Llave pública (Clave pública): valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada de quien actúa como iniciador.

Clave Personal de Acceso. (PIN). Sigla en inglés de "Personal Identification Number": Secuencia de caracteres que permiten el acceso al certificado digital.

Repositorio: sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.

Lista de Certificados Revocados: (CRL). Sigla en inglés de "Certificate Revocation List": Lista donde figuran exclusivamente los certificados revocados no vencidos.

Compromiso de la llave privada: entiéndase por compromiso el robo, pérdida, destrucción divulgación de la llave privada que pueda poner en riesgo el empleo y uso del certificado por parte terceros no autorizados o el sistema de certificación.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una ECD de nivel superior garantiza la confiabilidad de una o varias de nivel inferior.

Módulo Criptográfico Hardware de Seguridad: módulo hardware utilizado para realizar funciones criptográficas y almacenar llaves en modo seguro.

PKCS#10: Estándar de solicitud de certificación que cumple con la RFC 2986. Define el formato de los mensajes enviados a una autoridad de certificación o de registro para solicitar la certificación de una clave pública.

PKCS#12: Estándar de sintaxis de intercambio de información personal. Define un formato de archivo usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica, actualmente no admitido como mecanismo para almacenar claves privadas para suscriptores.

Protocolo de Estado de los Certificados En-línea. En inglés "Online Certificate Status Protocol" (OCSP): Protocolo que permite verificar en línea el estado de un certificado digital.

Titular. Entidad que requiere los servicios provistos por LLEIDA.NET y que está de acuerdo con los términos y condiciones publicados en la https://www.lleida.net/docs/es/colombia-declaracion.pdf de los servicios conforme a lo declarado en el presente documento.

ECD LLEIDA.NET: Es la Autoridad de Certificación de LLEIDA.NET, ente prestador de Servicios de Certificación digital.

AR LLEIDA.NET: Es la Autoridad de Registro de LLEIDA.NET, entre prestador del servicio de registro de LLEIDA.NET en el proceso de solicitud e identificación y aprobación de los solicitantes de un certificado digital.

TSA LLEIDA.NET: Corresponde al término utilizado por ECD LLEIDA.NET, en la prestación de su servicio de Estampado cronológico, como Autoridad de Estampado Cronológico.

2.5.2 Acrónimos

CA: Certification Authority

CA Sub: Autoridad de Certificación Subordinada

CP: Política de Certificación (Certificate Policy)

DPC: Declaración de Prácticas de Certificación (Certificate Practice Statement)

CRL: Certificate Revocation List CSP: Certification Service Provider DNS: Domain Name System

FIPS: Federal Information Processing Standard

HTTP: El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por su acrónimo HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

HSM: Módulo de seguridad criptográfico (Hardware Security Module)

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)

IP: Internet Protocol

ISO: International Organization for Standardization LDAP: Lightweight Directory Access Protocol OCSP: Online Certificate Status Protocol.

OCSP: Online Certificate Status Protocol

OID: Object identifier (Identificador de objeto único)

PIN: Personal Identification Number

PUK: Personal Unlocking Key

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Llave Pública)

PKIX: Public Key Infrastructure (X.509)

QSCD: Qualified (electronic) Signature Creation Device - Dispositivo Cualificado de Creación de Firma

RA: Registration Authority

RFC: Request For Comments (Estándar emitido por la IETF)

RRHH: Recursos Humanos

SGSI: Sistema de Gestión de Seguridad de la InformaciónURL: Uniform Resource Locator

VA: Autoridad de validación (Validation Authority)

2.5.3 Estándares y organismos de estandarización

CEN: Comité Europeo de Normalización

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

IETF: Internet Engineer Task Force

PKIX: Grupo de trabajo del IETF sobre PKI PKCS: Public Key Cryptography Standards RFC: Request For Comments

PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2.6 Participantes

2.6.1 Entidad de Certificación Digital (ECD)

Es aquella persona jurídica, acreditada conforme a la ley 527 de 1999 y el Decreto 333 de 2014, facultada por el gobierno Colombiano o el Organismo Nacional de Acreditación en Colombia para prestar servicios de certificación digital de acuerdo a lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen, es el origen de la jerarquía de certificación digital que le permite prestar los servicios relativos a las comunicaciones basadas en infraestructuras de clave pública.

LLEIDA.NET tiene como Entidad de Certificación Digital (ECD):

Nombre: LLEIDA SAS
Número de Identificación Tributaria: 900571038-3
Naturaleza: Privada (Sociedad Anónima)
Tipo de Empresa PyME
Dirección: Calle 81 # 11 – 55 Oficina 903
Ciudad / País: Bogotá D.C., Colombia.
Teléfono: +57 (1) 3819903
Correo electrónico: co@lleida.net
Página Web: www.lleida.net/co

2.6.2 Autoridad de registro (RA)

Es la entidad encargada de certificar la validez de la información suministrada por el solicitante de un servicio de certificación digital, mediante la verificación de la entidad del suscriptor o responsable de los servicios de certificación digital, en la RA se decide sobre la emisión o activación del servicio de certificación digital.

Bajo esta DPC, la figura de RA hace parte de la propia ECD y podrá actuar como Subordinada de ECD LLEIDANET.

LLEIDANET tiene como autoridad de registro RA:

Nombre: LLEIDA SAS
Número de Identificación Tributaria: 900571038-3
Naturaleza: Privada (Sociedad Anónima)
Tipo de Empresa PyME
Dirección: Calle 81 # 11 – 55 Oficina 903
Ciudad / País: Bogotá D.C., Colombia.
Teléfono: +57 (1) 3819903
Correo electrónico: co@lleida.net
Página Web: www.lleida.net/co

Las funciones de RA podrán ser tercerizadas. En este caso la RA de LLEIDA.NET evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento a dicho tercero.

La RA puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la RA, 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 RA, 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 RA.

Cabe indicar que LLEIDA.NET suministra al tercero la Plataforma de RA para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma con el certificado digital del operador.

2.6.2.1 Certificados emitidos por la Autoridad de Registro

A continuación, se indican los certificados que son emitidos por la autoridad de Registro de LLEIDA.NET

Nombre del certificado	OID	OID QCP	QCP
Políticas de Certificación Certificados de Persona Natural	1.3.6.1.4.1.53589.1.1.1		
Persona Natural Software	1.3.6.1.4.1.53589.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Persona Natural Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Persona Natural Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Persona Natural Centralizado UP	1.3.6.1.4.1.53589.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Persona Natural Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados de	1.3.6.1.4.1.53589.1.1.2		

Pertenencia a Empresa			
Pertenencia a Empresa Software	1.3.6.1.4.1.53589.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Hardware	1.3.6.1.4.1.53589.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados Representación de Empresa	1.3.6.1.4.1.53589.1.1.3		
Representación de Empresa Software	1.3.6.1.4.1.53589.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Hardware	1.3.6.1.4.1.53589.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados de Función Pública	1.3.6.1.4.1.53589.1.1.3.5		
Función Pública Software	1.3.6.1.4.1.53589.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)

Función Pública Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Función Pública Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Función Pública Centralizado UP	1.3.6.1.4.1.53589.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Función Pública Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificado de Jurídica	1.3.6.1.4.1.53589.1.1.3.4	0.4.0.194112.1.1	
Persona Jurídica Software	1.3.6.1.4.1.53589.1.1.3.4.1	0.4.0.194112.1.1	QCP-l-Sello electrónico (LLEIDA SAS SUB CA CO 001)
Persona Jurídica Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	0.4.0.194112.1.1	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Persona Jurídica Centralizado UP	1.3.6.1.4.1.53589.1.1.3.4.4	0.4.0.194112.1.1	QCP-n-qscd (Lleida SAS SUB CA CO 001)

2.6.2.2 Descripción de los Certificados emitidos por la Autoridad de Registro

Los certificados expedidos en tokens y tarjetas criptográficas NO pueden utilizarse en computadoras con sistema operativo Mac OS.

Cada Política de Certificado queda identificada con un OID diferenciado y conforme a la jerarquía de OIDs definida para LLEIDA SAS. En la siguiente tabla aparecen descritas las distintas Políticas cuyo manejo se describe en los apartados correspondientes de esta DPC:

Nombre	OID	Descripción
Persona Natural		
Persona Natural Software	1.3.6.1.4.1.53589.1.1.1.1.1	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 públicaque decida usarlo en un ámbito restringido. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con garantías legales Limitadas. GARANTÍAS LEGALES Limitadas
Persona Natural Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	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, 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 Ley 527 de 1999 y la normativa que la desarrolla..
Persona Natural Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.1.3.1	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 LLEIDA.NET, 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 ( ) 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 Ley 527 de 1999 y la normativa que la desarrolla.
Persona Natural Centralizado UP	1.3.6.1.4.1.53589.1.1.1.3.2	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 Ley 527 de 1999 y la normativa que la desarrolla.
Persona Natural Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.1.3.3	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 Ley 527 de 1999 y la normativa que la desarrolla..
Perteneciente a Empresa		
Pertenencia a Empresa Software	1.3.6.1.4.1.53589.1.1.2.1.1	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 que decida usarlo en un ámbito restringido. GARANTÍAS LEGALES Limitadas
Pertenencia a Empresa Hardware	1.3.6.1.4.1.53589.1.1.2.2.1	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, evitando así desplazamientos y esperas innecesarias. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones Ley 527 de 1999 y la normativa que la desarrolla.
Pertenencia a Empresa Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.2.3.1	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 Lleida.net Wallet (disponible para iOS y Android) en https:// https://wallet.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 Ley 527 de 1999 y la normativa que la desarrolla.
Pertenencia a Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.2.3.2	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 Ley 527 de 1999 y la normativa que la desarrolla.
Pertenencia a Empresa Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.2.3.3	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 Ley 527 de 1999 y la normativa que la desarrolla.
Representación de Empresa		
Representación de Empresa Software	1.3.6.1.4.1.53589.1.1.3.1.1	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 que decida usarlo en un ámbito restringido. GARANTÍAS LEGALES Limitadas
Representación de Empresa Hardware	1.3.6.1.4.1.53589.1.1.3.2.1	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 Ley 527 de 1999 y la normativa que la desarrolla.
Representación de Empresa Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.3.3.1	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 su smartphone para su uso desde las

		aplicaciones eSigna de LLEIDA.NET, 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 Lleida.net Wallet (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 Ley 527 de 1999 y la normativa que la desarrolla.
Representación de Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.3.3.2	Certificado cualificado que permite que una persona jurídica ostente la condición de representante legal con poderes generales sin limitaciones, de una organización y disponga de un certificado digital de firma centralizada. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones Ley 527 de 1999 y la normativa que la desarrolla.
Representación de Empresa Huella dactilar	1.3.6.1.4.1.53589.1.1.3.3.3	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 Ley 527 de 1999 y la normativa que la desarrolla.
Función Pública		
Función Pública Software	1.3.6.1.4.1.53589.1.1.3.5.1	Certificado que permite que una persona natural vinculada a la Administración Pública disponga de un certificado digital emitido en su ordenador y podrá utilizarlo con cualquier aplicación, entidad y administración pública, que decida usarlo en un ámbito restringido. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legaleslimitadas. GARANTÍAS LEGALES Limitadas
Función Pública Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	Certificado que permite que una persona natural vinculada a la Administración Pública 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, 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 Ley 527 de 1999 y la normativa que la desarrolla..

Función Pública Lleida.net Wallet	1.3.6.1.4.1.53589.1.1.3.5.3	Certificado que permite que una persona natural vinculada a la Administración Pública disponga de un certificado digital cualificado emitido en su teléfono móvil, para su uso desde las aplicaciones eSigna de LLEIDA.NET, 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 Función Pública Lleida.net Wallet ( ) 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 Ley 527 de 1999 y la normativa que la desarrolla.
Función Pública Centralizado UP	1.3.6.1.4.1.53589.1.1.3.5.4	Certificado que permite que una persona natural vinculada a la Administración Pública 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 Ley 527 de 1999 y la normativa que la desarrolla.
Función Pública Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.3.5.5	Certificado que permite que una persona natural vinculada a la Administración Pública 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 Ley 527 de 1999 y la normativa que la desarrolla..
Persona Jurídica		
Certificado de Persona Jurídica Software	1.3.6.1.4.1.53589.1.1.3.4.1	Este certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas en ámbitos restringidos y acotados. Representa a la entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal GARANTÍAS LEGALES Limitadas.
Certificado de Persona Jurídica Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	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 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 Ley 527 de 1999 y la normativa que la desarrolla.
Certificado de Persona Jurídica Centralizado UP	1.3.6.1.4.1.53589.1.1.3.4.4	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 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 Ley 527 de 1999 y la normativa que la desarrolla.

2.6.3 Suscriptor

Suscriptor es la persona natural o legal a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como suscriptor o responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC.

La figura de Suscriptor será diferente dependiendo de los servicios prestados por Lleida.net conforme lo establecido en el Políticas de Certificación.

Para el caso de certificados, 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.

2.6.4 Tercero de buena fe

Tercero de buena fe son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los servicios de certificación digital emitidos por la ECD a un suscriptor o responsable. El tercero de buena fe, a su vez puede ser o no suscriptor.

2.6.5 Otros participantes

2.6.5.1 Autoridad de sellado de tiempo

LLEIDA.NET, en su papel de Autoridad de Sellado de Tiempo, es la persona jurídica privada que presta indistintamente servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

2.6.5.2 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 Digital LLEIDA.NET, 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.

2.6.5.3 PROVEEDOR DE SERVICIOS DE FIRMA CENTRALIZADA Y SERVICIO CUALIFICADO DE VALIDACIÓN DE FIRMAS Y SELLOS (LLEIDA.NET)

LLEIDA.NET actúa como proveedor del servicio de aplicación de firma centralizada (SSASP) y del servicio de validación de firmas y sellos.

2.6.5.4 COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación LLEIDA.NET que 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.

2.7 Política de Uso de los servicios de certificación

2.7.1 Correo electrónico certificado

El servicio de Correo Electrónico Certificado permite garantizar la recepción del mensaje, asegurando en todo momento las características de trazabilidad e integridad. Para ello, el servicio permite garantizas la recepción de los mensajes por medio del documento de evidencias, documentos que se encuentra estampado cronológicamente.

El Correo Electrónico certificado puede ser usado por una persona natural o jurídica sin importar el cliente de correo que utilice. El uso del correo electrónico certificado no depende de un dispositivo por parte del receptor del mensaje de correo electrónico, posibilitando obtener garantías de la recepción distintas a las ofrecidas por el correo electrónico estándar. La plataforma se ajusta a la necesidad de dar trazabilidad y garantía en fecha y hora de generación del acuse de recibo, además de integrar información esencial dentro de la evidencia documental que posibilita total equivalencia al correo postal físico.

2.7.2 SMS Certificado

El servicio de SMS Certificado permite garantizar la recepción del mensaje de texto, asegurando en todo momento las características de trazabilidad e integridad. Para ello, el servicio permite garantizas la recepción de los mensajes por medio del documento de evidencias, documentos que se encuentra estampado cronológicamente.

El SMS Certificado puede ser usado por una persona natural o jurídica. Mediante una plataforma que se pone a disposición del suscriptor, el mensaje es enviado en tanto que Lleida.net es operador de telecomunicaciones y se obtiene información del estado de entrega del mensaje. Se genera la prueba pericial tanto si tiene confirmación de entrega o no, indicándose esta característica además de los datos de emisor/suscriptor del mensaje, el celular del destinatario y el contenido del mismo.

2.7.3 Click&Sign

Servicio que permite la composición y uso de un proceso de firma de documentos PDF por parte del usuario de Lleida.net en base a los métodos de firma proporcionados, tales como, aceptación mediante pulsación de un botón en un entorno web, introducción de un OTP, firma manuscrita biométrica o firma con certificado electrónico en la nube.

El servicio se caracteriza por ser flexible de modo que el remitente puede configurar el branding, el tipo de firma, las comunicaciones hacia el remitente, el firmante u otros, la solicitud de subida documental al firmante, el envío de recordatorios de firma y la recepción de eventos de notificación de estado de firma, entre otros.

El emisor podrá realizar solicitudes de firma definiendo los destinatarios, los documentos PDF a firmar, aspectos como el número de firmantes, si se requiere una firma en un orden concreto y que cantidad de firmantes se requiere para que la firma se considere efectiva. El servicio en todos los casos generará una evidencia firmada y con un sello de tiempo que recopilará toda la trazabilidad de comunicaciones certificadas realizadas y acciones realizadas por el firmante, acreditando así su firma. En caso de que el proceso expire se emite un documento de evidencias al efecto.

En el caso de la firma biométrica, se generará adicionalmente el documento con la firma biométrica incrustada firmado digitalmente y sellado de tiempo.

En el caso de la firma con certificado electrónico en la nube se generará adicionalmente el documento con la firma digital realizada en la nube.

2.7.4 Openum

Servicio que permite la composición y uso de un proceso de notificación de documentos PDF por parte del usuario de Lleida.net en base a los métodos de notificación

proporcionados, tales como, envío de notificación por correo electrónico certificado o no, envío de la notificación por SMS certificado o no y visualización de los documentos PDF.

El servicio se caracteriza por ser flexible de modo que el remitente puede configurar el branding, el tipo de notificación, las comunicaciones hacia el remitente, el firmante u otros, la solicitud de subida documental al destinatario, el envío de recordatorios de visualización y la recepción de eventos de notificación de estado de entrega, entre otros.

El emisor podrá realizar solicitudes de notificación definiendo los destinatarios, los documentos PDF a notificar, aspectos como el número de destinatarios, si se requiere una notificación en un orden concreto y que cantidad de visualizaciones ser requiere para que la notificación se considere efectiva.

El servicio en todos los casos generará una evidencia firmada y con un sello de tiempo que recopilará toda la trazabilidad de comunicaciones certificadas realizadas y acciones realizadas por el destinatario, acreditando así su notifiación. En caso de que el proceso expire se emite un documento de evidencias al efecto.

El servicio se ofrece mediante herramienta web de usuario y API para envío, consulta y descarga de documentos.

2.7.5 eKYC

Consiste en un procedimiento de identificación no presencial mediante videoconferencia que puede ser asistida o automática, en el que se incluye el proceso de validación de documentos identificativos.

El servicio realiza una grabación de la videoconferencia mediante tecnología WebRTC y captura de las imágenes del anverso y reverso del documento de identidad, y de una selfie. Tras la captura realizada, de la validación de las imágenes se obtiene una serie de parámetros de validación de identidad, en los que se incluye la biometría facial. Tras el análisis, el sistema realiza una validación de los parámetros obtenidos, pudiendo definir distintas lógicas según las necesidades de negocio para clasificar el proceso de identificación como positivo o negativo. El servicio emite una evidencia firmada digitalmente y con un sello de tiempo que incluye las imágenes, un hash del vídeo, los

datos de validación obtenidos, el resultado de la lógica de validación y la geolocalización si el usuario permitió su activación.

2.7.6 Certificados

2.7.6.1 Perfiles de certificado

Lleida SAS emite los siguientes perfiles de certificados con las características y garantías legales recogidas en la correspondiente política de servicio:

- Emisión de certificados digitales para persona jurídica en dispositivos locales o centralizados
- Emisión de certificados digitales para persona natural en dispositivos locales o centralizados
- Emisión de certificados digitales para persona función pública en dispositivos locales o centralizados
- Emisión de certificados digitales para representación empresa en dispositivos locales o centralizados
- Emisión de certificados digitales para representación empresa en dispositivos locales o centralizados

2.7.6.2 Firma en la Nube

El servicio de SSASC forma parte de los servicios operados por LLEIDA S.A.S. y permite prestar el servicio de firma electrónica centralizada a los firmantes que cuentan con un certificado electrónico definido para firma centralizada en su correspondiente Declaración Prácticas Servicio de Firma Centralizada.

El servicio permite la creación de firmas mediante sistemas de firma centralizada, en el cual LLEIDA S.A.S. 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 más OTP (usuario y password y PIN OTP), huella dactilar o mediante el uso de la APP móvil Lleida.net Wallet, de acuerdo a la especificación técnica ETSI TS 119 431-1.

2.7.7 Validación de certificados

La Plataforma de Validación de firmas y sellos electrónicos de LLEIDA S.A.S responde al Servicio Cualificado de validación de Firmas electrónicas y sellos electrónicos,

certificado bajo marco legal, que permite generar las correspondientes evidencias de validación de certificados cualificados, firmas y sellos electrónicos.

El Servicio Cualificado de validación de Firmas electrónicas genera evidencias, teniendo en cuenta las normas y estándares fijados por la normativa legal vigente. Se realizan comprobaciones del estado de calificación del certificado en el momento, día y hora de su emisión. En caso de existir Sello de Tiempo electrónico, se realiza también su comprobación. De igual manera, se realiza comprobación del estado del certificado en el momento de la firma. De todos los procesos, se generan las correspondientes evidencias.

Permite que el consumidor tenga pleno conocimiento sobre la validez, vigencia y cumplimiento normativo de la firma sometida a validación y le permite establecer políticas internas para blindarse frente a documentos o archivos firmados por clientes, proveedores o trabajadores que no cumplan con lo dispuesto en la normativa.

2.7.8 Estampado Cronológico

El servicio de estampado cronológico de LLEIDA.NET permite la generación de sellos de tiempo.

Sello de tiempo: Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez.
El sello de tiempo incluye:

- La firma digital de la entidad de sellado de tiempo
- Identificador electrónico único del documento (HASH o resumen)
- Fecha y hora recogida de una fuente fiable de tiempo

La Política de Sellado de Tiempo de LLEIDA.NET tiene como identificador único:

1.3.6.1.4.1.53589.1.1.5.3

2.8 Administración de políticas

2.8.1 Organización que administra el documento

LLEIDA SAS, con domicilio social en Calle 81 # 11 – 55 Oficina 903 de Bogotá D.C.

(Colombia), es la Autoridad de Certificación que presta los servicios certificados bajo esta Declaración de Prácticas de Certificación.

2.8.2 Contacto

Nombre de la ECD	LLEIDA SAS
Dirección	Calle 81 # 11 – 55 Oficina 903 de Bogotá D.C.
Dirección de email	info@lleida.net
Teléfono	(+57) 1 381 9903

2.8.3 Responsables de adecuación de la DPC

La Comisión de Seguridad de LLEIDA.NET 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.

2.8.4 Procedimiento de aprobación de las políticas de certificados

El Órgano de Aprobación de Políticas de LLEIDA.NET es el Comité de Seguridad. Aprueba los cambios finales realizados en este documento una vez que determine que cumplen con los requisitos establecidos. Una vez aprobados los cambios se procederá a la publicación en el sitio web de LLEIDANET_https://www.lleida.net/co

El Supervisor de la ECD es responsable de que la prestación de los servicios del LLEIDANET se ajuste a lo dispuesto en estas Políticas y declaración de prácticas y de asegurar la efectiva ejecución de los controles previstos. Asimismo, se encarga de la dirección, supervisión y control de la prestación de los servicios de LLEIDANET, de la operativa del servicio y del correcto de lo establecido en el presente documento.

El Supervisor de la ECD se encarga también de analizar los informes de las auditorías, totales o parciales, que se hagan de LLEIDA.NET y de sus servicios, así como de establecer y supervisar, en su caso, las acciones correctoras a ejecutar.

El Supervisor de la ECD será nombrado y cesado por la dirección de LLEIDA.NET, mediante resolución expresa de la que deberá quedar constancia escrita.

3 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

3.1 Repositorios

La ECD proporciona información de revocación para los Certificados Subordinados y los Certificados de Suscriptor disponibles de acuerdo con esta Declaración de Prácticas de Certificación.

Las políticas de certificación y la declaración de prácticas de certificación estarán disponles en la URL

- https://www.lleida.net/co/politicas-y-practicas

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

https://certs.esigna.es/root/ca_root_lleidasas.crt

Certificado Subordinada

https://certs.esigna.es/ca/lleidasas_pki_001.crt

Lista de Certificados Revocados (CRL)

https://crl1.esigna.es/sub/lleidasas_pki_001.crl

https://crl.esigna.es/sub/lleidasas_pki_001.crl

Validación de Certificados

https://ocsp2.esigna.es

3.2 Publicación de la información de certificación

La ECD divulga públicamente su Política de Certificados y/o la Declaración de Prácticas de Certificación a través de un medio on line apropiado y fácilmente accesible que esté disponible 24 horas al día, 7 días a la semana. La ECD deberá divulgar públicamente sus prácticas empresariales de ECD en la medida requerida por el esquema de auditoría seleccionado.

La URL en la que está disponible la información de políticas y la Declaración de Prácticas de Certificación es:

https://www.lleida.net/es/politicas-y-practicas

en ella también se encuentran los modelos y minutas de los contratos que utilizarán con los usuarios.

Asimismo, la página https://www.lleida.net estará disponible la información sobre los Términos y condiciones de prestación de los distintos servicios

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

La divulgación incluye todo el material requerido por RFC 2527 o RFC 3647 y se estructura de acuerdo con RFC 2527 o RFC 3647.

3.3 Tiempo o frecuencia de publicación

LLEIDANET se compromete a poner a disposición pública en su página web las Políticas de Certificación y su Declaración de Prácticas de Certificación tan pronto como sean aprobadas por el Comité de Seguridad, cuando se produzcan actualizaciones a consecuencia de cambios técnicos o legales.

LLEIDANET se compromete a desarrollar, implementar, hacer cumplir y actualizar con periodicidad bienal, sus Políticas de Certificación y su Declaración de Prácticas de Certificación, como uno de los elementos asociados a la auditoría bienal. El intervalo de actualización será menor cuando se produzcan cambios técnicos o legales que hagan necesaria una actualización.

Las auditorías de la ECD destinada a la emisión de los servicios de certificación digital serán anuales.

Certificado Raíz

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

Lista de Certificados Revocados (CRL)

La Entidad de Certificación Digital 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.

Validación de Certificados

La Entidad de Certificación Digital publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección: https://ocsp2.esigna.es

3.4 Control de acceso a los repositorios

La información relativa al estados de los servicios de certificación digital está disponible en modo lectura para las partes que confían.

LLEIDANET tiene implementados los controles de seguridad para que dicho acceso no comprometa el funcionamiento del servicio. La función de estos controles es impedir accesos no autorizados, por ejemplo, para modificar o borrar datos asociados a los servicio, solicitudes masivas.

4 IDENTIFICACIÓN Y AUTENTICACIÓN

4.1 Solicitante

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud de los servicios de certificación de Lleida.net.

Cualquier persona que requiera la prestación del servicio de correo electrónico certificado, puede solicitar la prestación a través de la página web de Lleida.net o mediante correo electrónico o teléfono dispuestos al efecto.

4.1.1 Tipos de nombres

El documento guía que LLEIDA.NET 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 LLEIDA.NET 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.

4.1.1.1 Certificado Raíz de LLEIDA.NET

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

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

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

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

Número de serie = 34376792308506

Huella digital = 4ba80d75903497f45d32efefd25f184b362f1dd0

SHA-256 =
EB2F7A6E156C096BB4D66B79AE70676E22456FA3073215AA16A0314F086040DE

4.1.1.2 Certificados de las Subordinadas

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDA.NET., tiene las siguientes características:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

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

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

Número de serie = 69782574365786

Huella digital = d73c5ac77e345b2bea98da7c31b283e83e2b13a7

SHA-256 =
C2F9D17FB87281FA9655A8E9AAEF4AC09BAA8F7597BEFD94ACE0F90C33B85C0C

4.1.1.3 Certificados de Titular

El DN del 'issuer name' de los certificados de titular de LLEIDA.NET., tiene las siguientes características generales:

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

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-220304-2242015- Perfiles Certificados.pdf.

4.1.1.4 Significados 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 8.1.4 Formato de Nombres y documento de Política de Certificación.

4.1.1.5 Anonimato o pseudónimos de los suscriptores

LLEIDA.NET. 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.

4.1.1.6 Reglas utilizadas para interpretar varios formatos de nombres

LLEIDA.NET 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.

4.1.1.7 Unicidad de los nombres

Dentro de una misma EDC 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 DPC un Firmante persona física puede pedir más de un certificado siempre que la combinación de los siguientes valores en la solicitud sea diferente:

- NIT
- Documento de identificación
- 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.

4.1.1.8 Reconocimiento, autenticación y función de Marcas Registradas y otros signos distintivos

LLEIDA.NET no asume compromisos en la emisión de certificados respecto al uso de marcas y otros signos distintivos.

LLEIDA.NET no permite deliberadamente el uso de un signo distintivo sobre el Sujeto/Firmante que no ostente derechos de uso.

Sin embargo, LLEIDA.NET 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

4.1.1.9 Procedimiento de resolución de disputas de nombres

LLEIDA.NET 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. LLEIDA.NET no arbitra este tipo de disputas que deberán ser resueltas directamente por las partes

4.2 Validación inicial de la identidad

Las funciones de identificación del solicitante so realizadas por la RA de Lleida.net, que actúa por orden del Departamento Comercial que es quién le realiza la petición.

La RA examinará la documentación necesaria para la activación del servicio y comprueba si la información suministrada es válida y si cumple con los requisitos definidos para cada política de los servicios que el cliente pretende usar.

4.2.1 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 RA ni en la ECD.

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

La RA 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:

[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

De manera presencial:

- En el caso de empresas con domicilio en Colombia, 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:

- Se podrá realizar la acreditación del representante legal de manera telemática mediante sistemas de video identificación o verificación biométrica facial. Esta videoconferencia o las pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenadas para su posterior verificación en el caso de ser necesario.
- 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.

4.2.3 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 tarjeta de identidad, célula de ciudadanía, pasaporte, célula de extranjería u otros medios admitidos en derecho. Podrá prescindirse de la personación

[2] La vigencia del certificado presentado no debe ser mayor de 30 días.

[3] La vigencia del certificado no debe ser mayor de 30 días.

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 EDC de LLEIDA SAS o por otra EDC, 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.
- Se podrá realizar la acreditación del solicitante de manera telemática mediante sistemas de video identificación o verificación biométrica facial. Esta videoconferencia o las pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenadas para su posterior verificación en el caso de ser necesario.
- Se verificará la acreditación del solicitante con los documentos indicados para cuando se realiza de manera presencial.

LLEIDA.NET dispone de un método de Video Identificación basado en el procedimiento de video identificación y reconocido en otros algunos países la Unión Europea para la expedición de certificados cualificados.

Breve descripción del proceso:

- 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.

- El Operador procederá a la validación de la prueba de vida del Solicitante y el reconocimiento facial coincidiendo con el Documento de identidad.

- 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.

Tras el proceso de identificación, el solicitante firmará mediante una firma electrónica con el servicio Click&Sign

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

4.2.4 Información no verificada del suscriptor

Bajo ninguna circunstancia LLEIDA.NET 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.

4.2.5 Validación de la autoridad

Tipo de certificado	Documentación Requerida
Persona Natural	Nacionalidad Colombiana: • Tarjeta de Identidad. • Cécula de ciudadanía Extranjeros: • Pasaporte • Célula de Extranjería Para los Documentos de identidad extranjeros se pedirá apostillado de la Haya y se podrá pedir traducción jurada si fuera necesario. Además se incluirá para acreditar el domicilio bien el RUT, bien un documento expedido por un tercero que lo verifique.
Representación de Empresa	Los mismos que para validar la identidad de la persona natural más: Fotocopia del documento que establezca su nombramiento como representante legal con fecha de expedición no mayor a treinta (30) días: - Camara de Comercio (Privados reguistrados en RUES) - Certificado de nombramiento ante la superintendencia financiera de Colombia (Entidades financieras vigiladas) - Escritura Pública (Unión Temporal y Consorcios)
Perteneciente a Empresa	Los mismos que para validar la identidad de la persona natural más: * Certificado laboral del solicitante con fecha de expedición no mayor a treinta (30) días. (Se debe adjuntar en hoja membreteada de la empresa firmada digitalmente por el representante legal o por el área de recursos humanos). * Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días
Función Pública	Los mismos que para validar la identidad de la persona natural más:

	Fotocopia del documento de nombramiento y aceptación del cargo ó certificado de vigencia del nombramiento y ejercicio del cargo (Estos documentos deben evidenciar las fechas de vigencia del nombramiento y el número de acto de posesión)
Persona Jurídica	Autorización firmada digitalmente por un representante legal o apoderado general de la entidad, con un certificado digital de representante legal o apoderado de una EDC de confianza o de LLEIDA.NET * Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días Fotocopia del documento que establezca su nombramiento como representante legal con fecha de expedición no mayor a treinta (30) días:

4.2.6 Criterios para la Interoperabilidad

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

4.3 Identificación y validación de las solicitudes de renovación

La mayoría de los servicios de certificación digital de Lleida.net se renuevan de forma automática, por lo que si el usuario no desea utilizar el servicio deberá comunicarlo a la RA.

En el caso del servicio de certificado se requiere una renovación de acuerdo a los siguientes escenarios:

4.3.1 Identificación y autenticación en tareas rutinarias de renovación

La Entidad de Certificación Digital 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 4.2 Validación inicial de la identidad de este mismo documento.

4.3.2 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 Digital, realiza un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el apartado 4.2 Validación inicial de la identidad de este mismo documento.

4.4 Identificación y autenticación para la solicitud de cancelación

El usuario puede voluntariamente solicitar la cancelación del servicio en cualquier instante, pero está obligado a solicitar la cancelación del servicio bajo las siguientes situaciones:

a) Por pérdida o inutilización de las credenciales (usuario y contraseña)

b) Las credenciales han sido expuestas o corre peligro de que se le dé un uso indebido.

c) Cambios en las circunstancias por las cuales Lleida.net autorizo el servicio.

Si el responsable no solicita la cancelación del servicio en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el servicio.

Además, debe tenerse en cuanta que se puede solicitar la revocación de un certificado y para ello es necesario autenticarse de acuerdo a los siguientes criterios:

- Para los suscriptores deben presentar en la RA el tarjeta de identidad, célula de ciudadanía, pasaporte, célula de extranjería 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[4] 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
- Los terceros (diferentes de la ECD, el suscriptor y el titular) deberán presentar en la RA pruebas fehacientes del uso indebido del certificado de acuerdo con la ley vigente, junto a la orden judicial respectiva.

El usuario reconoce y acepta que los servicios de Lleida.net debe ser cancelados cuando esta conoce o tiene indicios o confirmación de ocurrencia de alguna de las siguientes circunstancias:

a) A petición del usuario o un tercero en su nombre y representación.

b) Por cambio del usuario.

c) Por muerte del usuario.

[4] La vigencia del certificado presentado no debe ser mayor de 30 días.

d) Por liquidación en el caso de las personas jurídicas (entidad) que adquirieron el servicio.
e) Por la confirmación o evidencia de que alguna información es falsa.
f) Por el cese de actividades de la entidad de certificación.
g) Por orden judicial o de entidad administrativa competente.
h) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
i) Por incapacidad sobrevenida del responsable o entidad.
j) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
k) Por la aplicación del documento de términos y condiciones, de conformidad con las causales establecidas en el contrato.
l) Por cualquier causa que razonablemente induzca a creer que el servicio utilizado con certificado digital se haya comprometido hasta el punto de que se ponga en duda la confiabilidad del mismo.
m) Por el manejo indebido por parte del responsable del servicio.
n) Por el incumplimiento del usuario o de la persona jurídica que representa o a la que está vinculado a través del documento de términos y condiciones.
o) Conocimiento de eventos que modifiquen el estado inicial de los datos suministrados, entre otros: terminación de la Representación Legal, terminación del vínculo laboral, liquidación o extinción de la personería jurídica, cesación en la función pública o cambio a una distinta.
p) En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
q) Por incumplimiento por parte de Lleida SAS, el suscriptor o responsable de las obligaciones establecidas en la Política.
r) Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y Lleida SAS.

No obstante, para las causales anteriores Lleida SAS, también podrá cancelar alguno de los servicios , cuando a su juicio se pueda poner en riesgo la credibilidad, confiabilidad, valor comercial, buen nombre de la ECD, idoneidad legal o moral de todo el sistema de certificación.

5 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL

Esta Declaración de Prácticas de Certificación regula los requisitos operativos comunes para los servicios de certificación digital .

Las Políticas de Certificación de los distintos tipos de certificado pueden contener especificidades respecto a algún aspecto del ciclo de vida de los mismos.

5.1 Solicitud del servicio

La solicitud de los servicios puede hacerse por varios métodos, a saber:

Teléfono: +57 1 3819903

Correo electrónico: info@lleida.net

Formularios web disponibles en www.lleida.net/co

Para la solicitud de emisión de certificados se habilitan las siguientes modalidades de atención:

- De manera presencial en las instalaciones de la RA de LLEIDA.NET
- De manera presencial en las instalaciones del cliente, o un lugar asignado por este en presencia de un representante de la RA.
- 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 mediante sistemas de video identificación o verificación biométrica facial. Esta videoconferencia o las pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenadas para su posterior verificación en el caso de ser necesario.

5.2 Quién puede enviar una solicitud del certificado

Pueden solicitar un servicio de certificación las personas que:

- lo hagan en nombre y representación propia
- Los representantes de entidades con o sin personalidad jurídica, debidamente acreditados

En particular, para las solicitudes de emisión de certificados:

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.

5.3 Proceso de inscripción y responsabilidades

La RA es quién recibe la información de la solicitud, que la remitirá al Departamento Comercial para que se ponga en contacto con el suscriptor y recabe la documentación para la identificación.

LLEIDANET, a través de su Departamento Comercial, informará de qué documentación se requiere para la identificación y autenticación, que puede hacerse mecanismos de identificación a distancia, normalmente a través de correo electrónico.

La documentación a aportar deberá estar actualizada y vigente. Los documentos que se envíen digitalizados deberán ser legibles. De optar por la modalidad presencial de verificación de la identidad, los documentos que deberán aportarse deberán ser originales.

Las tareas de identificación y validación de la información para el servicio y validación y aprobación de las solicitudes de emisión y revocación serán realizadas por las Oficinas de Registro (RA) o de manera telemática mediante sistemas de video identificación o verificación biométrica facial.

Las Oficinas de Registro Propias de LLEIDA.NET o de las entidades usuarias con las que esta firme el correspondiente instrumento legal deberán asumir las siguientes obligaciones:

- Validar la identidad y otros detalles personales del solicitante, del suscriptor y o la información relevante para el fin activación de los servicios.
- Mantener toda la información y documentación relativa a los certificados, y gestionar su emisión, y revocación
- Notificar a LLEIDA.NET sobre las solicitudes de revocación de los servicios con la debida diligencia y de una manera rápida y confiable.
- Permitir a LLEIDA.NET el acceso a sus archivos de procedimiento y registros de auditoría para desempeñar sus funciones y mantener la información necesaria.
- Informar a LLEIDA.NET sobre las solicitudes de emisión, revocación y cualquier otro aspecto relacionado con los servicios prestados por LLEIDANET.

- Validar, con la debida diligencia, las circunstancias de revocación que puedan afectar a la validez del servicio.
- Cumplir con los procedimientos establecidos por LLEIDA.NET y con la legislación vigente en esta materia, en sus operaciones de gestión relacionadas con la activación , y revocación de los servicios.

5.4 Procedimiento de solicitud de certificado

Una vez haya tenido lugar una petición de uno o varios servicios , el operador de la RA mediante el acceso a la plataforma de gestión verifica que la información proporcionada es correcta.

La Autoridad de Registro de LLEIDA.NET puede emitir los siguientes certificados:

- Certificado de Persona Natural
- Certificado de Pertenencia a Empresa
- Certificado de Representación de Empresa
- Certificado de Función Pública
- Certificado de Persona Jurídica.

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
- 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[5] y que tenga la certificación FIPS 140-2 nivel 3 o Common Criterial EAL 4+[6].
- Se realiza las solicitudes en Plataforma de registro, adjuntando evidencia de información.
- Se firma contrato de emisión de certificado.
- Se genera certificado en PKI.
- Se inserta en modulo criptográfico y generan claves.
- Se recibe clave de activación y revocación a través de correo electrónico declarado.

Para la emisión de certificados remota:

[5] 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.

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

- 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[7] y que tenga la certificación FIPS 140-2 nivel 3 o Common Criterial EAL 4+[8].
- 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.

5.4.1 Realización de funciones de identificación y autenticación

Es responsabilidad de la RA llevar a cabo correctamente la identificación del suscriptor. Este proceso debe llevarse a cabo antes de la activación del servicio

En todos los casos, los usuarios deben consultar la documentación específica de cada servicio para obtener detalles sobre cada uno de ellos. Todo ello de acuerdo al apartado 4.2 Validación inicial de la identidad

5.4.2 Aprobación o rechazo de solicitudes de certificado

Una vez que se haya solicitado el servicio o servicios, la RA deberá comprobar la información proporcionada por el solicitante, incluida la validación de la identidad del suscriptor, y en su caso, de la suficiencia de poderes de representación.

Si la información no es correcta, la RA denegará la solicitud y se pondrá en contacto con el solicitante para explicar la razón. Si la información es correcta, se continuará con el proceso de activación del servicio

Igualmente, LLEIDA.NET 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

[7] 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.

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

plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal y/o de conveniencia comercial, buen nombre o reputación de ECD de LLEIDA.NET pueda poner en peligro el sistema de certificación digital.

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

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

La RA 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.

5.4.2.1 Aprobación de la solicitud de emisión de certificado

Una vez validada la información proporcionada por el suscriptor, en caso de que una solicitud sea aprobada por la RA, 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 RA enviará a la respectiva ECD la autorización de la emisión del certificado de manera inmediata.

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

5.4.2.2 Rechazo de la solicitud de emisión de certificado

La solicitud será rechazada si el resultado de la validación realizada por la ra fue negativo, conforme a lo establecido en este documento.

La ECD puede decidir establecer en su DPC u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la RA de esta.

5.4.3 Tiempo para procesar las solicitudes de activación

Una vez verificada la información requerida en el proceso de solicitud de certificados, se podrá proceder a la emisión del certificado que se requiera. El tiempo máximo estimado de activación del servicio tras la verificación es de 24 horas en días laborables.

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

5.5 Activación de los servicios

Todas las solicitudes deben ser aprobadas en su totalidad antes de que los servicios sean activados. Una vez aprobada la solicitud LLEIDANET enviará las credenciales de acceso al solicitante en la cuenta de correo electrónico que haya indicado en el proceso de solicitud.

Particularmente, 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.

El suscriptor recibirá de forma telemática el contrato, la política de certificación y prácticas de certificación que especifican las condiciones de uso.

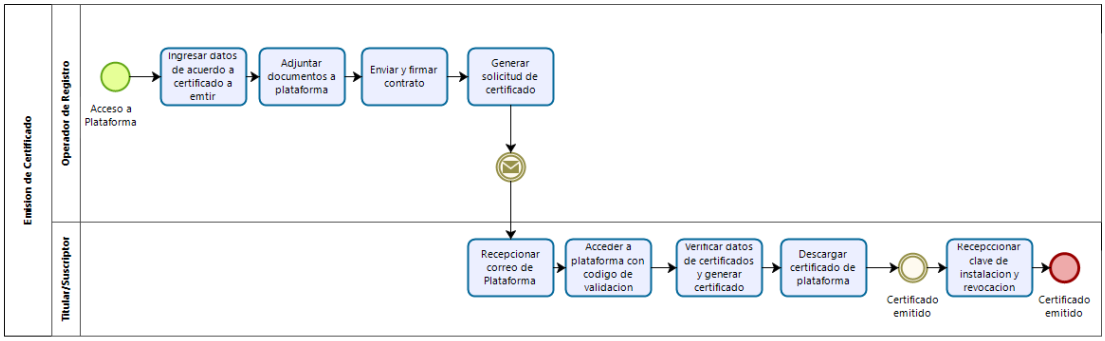
En cualquier caso, el uso de los servicios para este fin o para cualquier otro constituye la aceptación de los términos y condiciones, la política de certificación y la declaración de prácticas.

5.5.1 Acciones de la ECD 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.

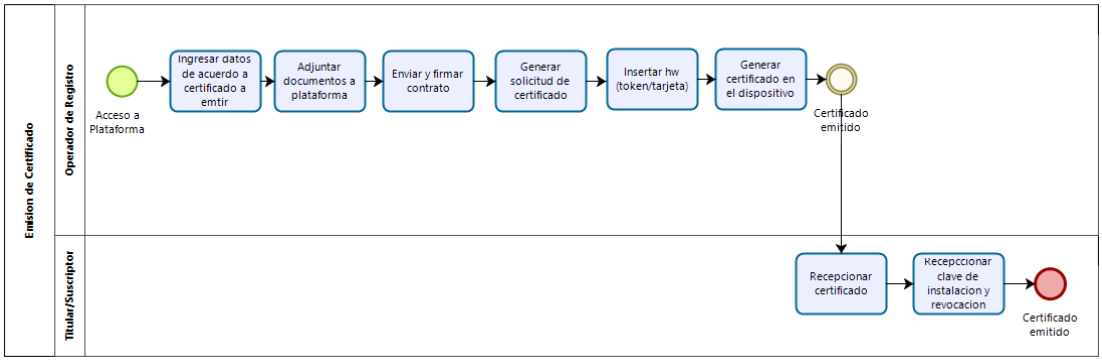
La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. La petición segura del certificado a la ECD se realizará en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

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



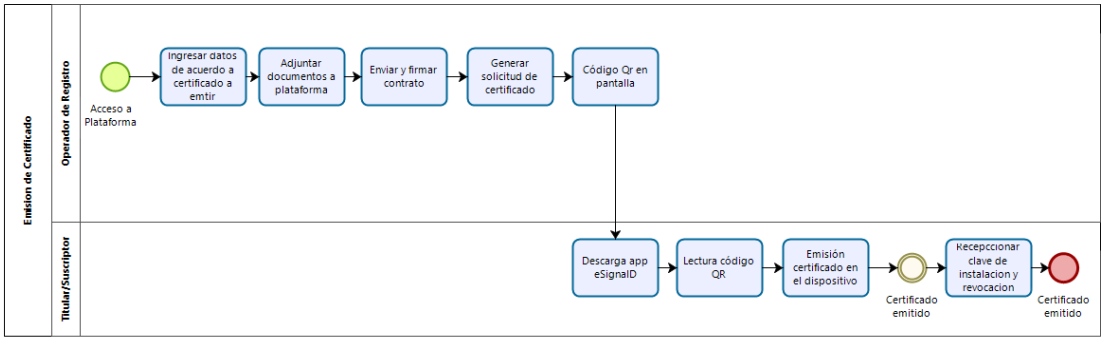
Se realizará el envío de un enlace al usuario por correo que incluye un código de validación. Una vez se acceda y se verifiquen los datos, se generará el certificado que se podrá descargar e instalar el certificado a través de un archivo p12 o pfx.

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



En este caso la RA 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+.

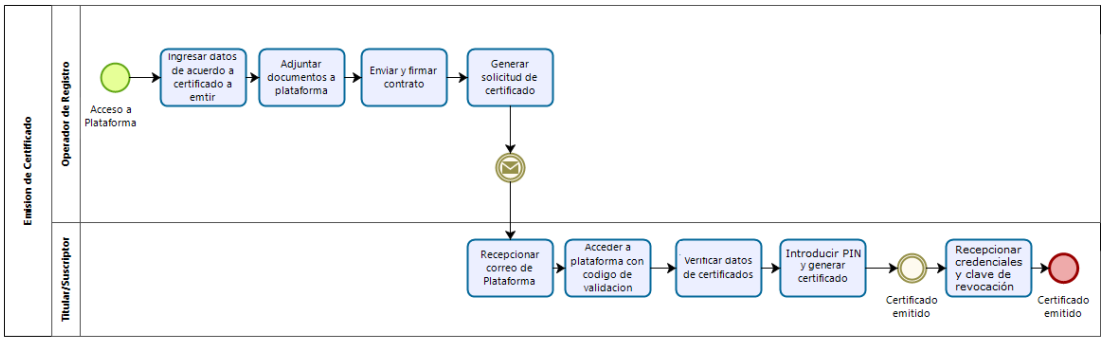
C. En el caso de que la emisión del certificado se haga usando la aplicación Lleida.net Wallet el proceso es el siguiente:



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 RA no administra ningún módulo criptográfico ya que el certificado es generado en el smartphone del usuario.

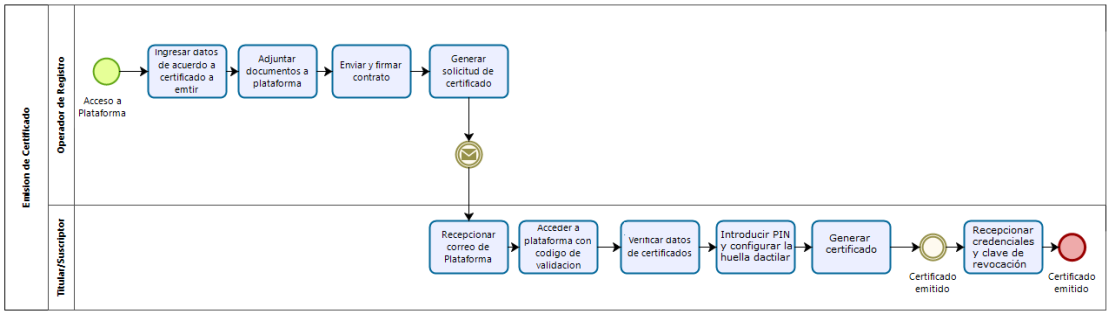
D. En el caso de que la emisión del certificado se haga en el servicio de firma centralizada con acceso mediante credenciales, el proceso es el siguiente:



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 RA no administra ningún módulo criptográfico ya que el certificado es generado en el servicio de firma centralizada de la ECD.

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 RA no administra ningún módulo criptográfico ya que el certificado es generado en el servicio de firma centralizada de la ECD.

5.5.2 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.

5.6 Aceptación del certificado

5.6.1 Conducta que constituye la 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 ECD, 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 5.9.3 Procedimiento de solicitud de la revocación del certificado de este mismo documento.

5.6.2 Consulta del estado de certificado

LLEIDA.NET ofrece un sistema de consulta del estado de los certificados emitidos, en su página web https://www.lleida.net/es/politicas-y-practicas. El acceso a esta página es libre y gratuito tanto para suscriptores como para entidades.

5.7 Par de claves y uso de los servicios

5.7.1 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. LLEIDA.NET no asume ningún tipo de responsabilidad por los usos no autorizados.

El titular o suscriptor deberá notificar a la ECD o RA 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.

5.7.2 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 LLEIDA.NET, sin permiso previo por escrito de la ECD.
- No comprometer intencionadamente la seguridad de la Jerarquía de LLEIDA.NET.
- 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 ECD 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).

5.8 Renovación de los servicios

El servicio de certificado no se renueva automáticamente y su renovación funciona de acuerdo a los siguientes apartados

5.8.1 Renovación del certificado

La ECD no ofrece el servicio de renovación de un certificado digital.

Se seguiría el proceso descrito en el apartado 5.8.1.1 Circunstancias para la renovación del certificado.

5.8.1.1 Circunstancias para la renovación del certificado

Para la Entidad de Certificación LLEIDA.NET., 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 ECD. 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.

5.8.2 Suspensión del certificado

En Colombia no está permitido el proceso de suspensión de un certificado digital, por lo que la ECD no ofrece este servicio.

5.8.3 Renovación con regeneración de las claves del certificado

La ECD no ofrece el servicio de renovación de un certificado digital.

Para la Entidad de Certificación Digital, 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 ECD 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.

5.9 Modificación de los servicios

Cualquier necesidad de modificación de certificados implicará una nueva solicitud.

Los certificados digitales emitidos por la Entidad de Certificación Digital, 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.

5.9.1 Circunstancias para la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.2 Quién puede solicitar la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.3 Procesamiento de las solicitudes de renovación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.4 Norificación de la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.5 Conducta que constituye la aceptación de la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.6 Publicación del certificado modificado

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.9.7 Notificación del certificado modificado a otras entidades

No aplica ya que los certificados digitales emitidos por LLEIDA.NET no pueden ser modificados.

5.10 Cancelación de los servicios

En las políticas de cada servicio se establecen las circunstancias, requisitos de los solicitantes y el procedimiento de cancelación de los servicios.

En particular, la revocación de los certificados tendrá que tener en cuenta los siguientes apartados:

5.10.1 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 LLEIDA.NET
- 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 ECD.
- 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.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del servicio.

- Además, el certificado de un titular debe ser revocado por la ECD cuando:
  - Se produce la renovación del certificado.

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

5.10.2 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.

5.10.3 Procedimiento de solicitud de 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 LLEIDA.NET, 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 LLEIDA.NET En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los titulares.
- Servicio de Revocación telefónica. A través de la línea de atención telefónica permanente los titulares y terceros pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC.
- Servicio de Revocación vía correo electrónico. Por medio de nuestro correo electrónico, los titulares y terceros pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC.

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.

5.10.4 Periodo de gracia de la solicitud de revocación del certificado

Previa validación de la autenticidad de una solicitud de revocación, LLEIDA.NET 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 LLEIDA.NET 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 LLEIDA.NET toda vez que reconoce y acepta que el control, custodia y confidencialidad de la clave privada es responsabilidad exclusiva de este.

5.10.5 Plazo 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 5.10.3 Procedimiento de solicitud de la revocación del certificado, de este documento, lo que implica que se realizará en menos de 60 minutos.

5.10.6 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 LLEIDA.NET en https://www.lleida.net/es/politicas-y-practicas.

5.10.7 Frecuencia de generación de las CRLs

Cada vez que se produzca una revocación de un certificado, LLEIDA.NET 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.

5.10.8 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.

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

LLEIDA.NET 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. LLEIDA.NET ofrece un servicio de consulta en línea basada en el protocolo OCSP en la dirección https://ocsp2.esigna.es.

5.10.10 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 https://ocsp2.esigna.es para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC 6960. La mayoría de los navegadores ofrecen este servicio.

5.10.11 Otras formas de aviso de revocación de claves comprometidas

Los mecanismos que LLEIDA.NET pone a disposición de los usuarios del sistema, estarán publicados en su página Web https://www.lleida.net/es/politicas-y-practicas.

5.10.12 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.

5.10.13 Circunstancias para la suspensión

Tal y como se indica en el documento "CEA-3.0-07" apartado 10.9.1 c) no se permite la suspensión de certificados digitales.

5.10.14 Quién puede solicitar la suspensión

Ver apartado 5.10.13 Circunstancias para la suspensión

5.10.15 Procedimiento para la petición de la suspensión

Ver apartado 5.10.13 Circunstancias para la suspensión

5.10.16 Límites sobre el periodo de suspensión

Ver apartado 5.10.13 Circunstancias para la suspensión

5.11 Servicios de estado de los servicios

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.lleida.net/es/politicas-y-practicas 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 LLEIDA.NET como Entidad de Certificación Digital, queda garantizada mediante la transferencia, al organismo supervisor o a otra EDC con la 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 LLEIDA.NET puede ser consultada mediante CRLs y/o el Servicio de información y consulta del estado de los Certificados mediante el protocolo OCSP.

5.11.1 Características operacionales

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

5.11.2 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.

LLEIDA.NET 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 LLEIDA.NET y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.

5.11.3 Características opcionales

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

5.12 FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción finaliza a solicitud del suscriptor o por las causas recogidas en esta Declaración de Prácticas de Certificación.

La Entidad de Certificación Digital 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.

5.13 DEPÓSITO Y RECUPERACIÓN DE CLAVES

5.13.1 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, LLEIDA.NET realiza la custodia de las claves en dispositivos seguros de creación de firma HSM. Las claves almacenadas por LLEIDA.NET. en sus instalaciones cuentan con mecanismos de encriptación que sólo el usuario conoce o tiene. LLEIDA.NET 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.

5.13.2 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.

6 CONTROLES DE INSTALACIONES, DE GESTIÓN Y OPERACIONALES

6.1 Controles físicos

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

LLEIDA.NET tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

- Controles físicos de entrada
- Seguridad de oficinas, despachos e instalaciones
- Protección contra las amenazas externas y ambientales
- Trabajo en áreas seguras
- Áreas de carga y descarga
- Emplazamiento y protección de equipos
- Instalaciones de suministro
- Seguridad del cableado
- Mantenimiento de los equipos
- Retirada de materiales propiedad de la empresa
- Seguridad de los equipos fuera de las instalaciones
- Reutilización o eliminación de equipos
- Política de dispositivos móviles

6.1.1 Localización y construcción de las instalaciones

LLEIDA.NET cuenta con infraestructura adecuada para prestar servicios de confianza digital en sus instalaciones de Lleida

Para la infraestructura del servicio de certificados LLEIDA.NET. 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 LLEIDA.NET 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.

6.1.1.1 Situación del Centro de Proceso de Datos

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

6.1.2 Acceso físico

Las instalaciones de LLEIDANET cuentan con un sistema completo de control de acceso físico que consiste en:

- Seguridad perimetral para evitar el acceso no autorizado.
- Control sobre el acceso físico a la instalación.
  - Sólo se permite el acceso al personal autorizado.
  - Los derechos de acceso al área de seguridad son revisados y actualizados periódicamente.
  - Todo el personal debe estar identificado y no es posible circular en el edificio sin estar identificado y acompañado por un empleado.
  - El personal que no está en la lista de acceso de LLEIDA.NET y que puede estar trabajando en el sitio está debidamente supervisado
- El acceso a las instalaciones que acogen los servidores implica la videograbación de la actividad y requiere identificación biométrica y control dual de los accesos.
- Se lleva a cabo el registro de los accesos a las instalaciones que acogen los servidores.
  Se cuenta con medidas adicionales de limitación de accesos al edificio en las oficinas de LLLEIDANET.
- Las RAs cumplen con los criterios de seguridad necesarios definidos en el documento de securización del sitio de registro.

El acceso a los sistemas que proveen los servicios de certificación digital está protegido con 3 niveles de acceso: Oficinas, CPD y acceso a servidores

El acceso a la zona de oficinas y salas de reuniones por personal ajeno a la entidad se controla mediante un registro de visitas.

El detalle técnico de la infraestructura del servicio de certificados se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

6.1.3 Electricidad y aire acondicionado

El centro de procesamiento de datos dispone de energía y aire acondicionado suficientes para crear un entorno operativo fiable.

Todos los servidores de todos los centros de datos disponen de sistemas de alimentación interrumpida (SAI) que aseguran que los servicios no se interrumpan ante caídas puntuales del suministro eléctrico (micro cortes) o que no se dañen los equipos ante subidas inesperadas de la tensión eléctrica. Así mismo proporcionan cierta autonomía ante un cese de suministro más prolongado (entre 15 y 30 minutos según el caso).

En la sede central se dispone de un grupo electrógeno exclusivo que permite el funcionamiento de los servicios ante un fallo de suministro más largo. Existe un contrato de mantenimiento para asegurar la disponibilidad y la carga de combustible.

En el centro de datos secundario se dispone también de un grupo electrógeno que permite el funcionamiento de los servicios ante un fallo de suministro más largo.

Por lo que se refiere a la infraestructura del servicio de certificados, 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.

6.1.4 Exposición al agua

LLEIDA.NET ha tomado las precauciones necesarias para minimizar el impacto de la exposición al agua. Sus instalaciones se encuentran en un emplazamiento geográficamente elevado.

Por lo que se refiere a la infraestructura del servicio de certificados, 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.

6.1.5 Prevención y protección contra incendios

El centro de procesamiento de datos de LLEIDA.NET tiene barreras físicas que se extienden desde el suelo hasta el techo, así como sistemas automáticos de detección de incendios con el propósito de:

- Notificar a los vigilantes y al personal de LLEIDA.NET del inicio de un incendio.
- Desconectar el sistema de ventilación, cerrar las puertas ignífugas, apagar la fuente de alimentación y activar la instalación automática de extinción de incendios.

Además, existe equipamiento de extintores debidamente señalizados.

6.1.6 Almacenamiento de soportes

Los soportes que contienen información de backup se almacenan de forma segura en un CPD separado con las medidas de seguridad necesarias.

6.1.7 Eliminación de residuos

Existe una política para regular los procedimientos que rigen la destrucción de los medios de información.

Los soportes de almacenamiento que contienen información confidencial se destruyen para garantizar que los datos no sean legibles o recuperables después de la eliminación

6.1.8 Copia de seguridad externa

LLEIDA.NET mantiene copias de seguridad de los soportes de almacenamiento en un entorno seguro y protegido contra accidentes ya una distancia suficiente para evitar daños en caso de un desastre en el sitio originario.

6.2 Controles de procedimiento

6.2.1 Puestos de confianza

Un "puesto de confianza" se define como las funciones asignadas a una persona que pueden conllevar problemas de seguridad si no se realizan satisfactoriamente, ya sea de forma accidental o intencionada.

Para asegurar que las personas de confianza cumplan adecuadamente sus deberes, se abordan las siguientes consideraciones:

- La primera es que la tecnología está diseñada y configurada para prevenir errores y conducta inadecuada.
- La segunda es que las tareas se distribuyen entre varios individuos de manera que cualquier conducta impropia requeriría la complicidad de varios de ellos.

LLEIDA.NET tiene definiciones completas de todas las funciones desempeñadas en la organización. Se definen los deberes y responsabilidades asociados a cada función, y cada uno tiene un conjunto de procedimientos documentados que regulan la práctica anexa a cada uno.

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[9] a los sistemas de la EDC.

6.2.2 Número de personas requeridas por tarea

Se puede asignar varias personas a la misma función.

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

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

6.2.3 Identificación y autenticación para cada puesto

Los roles de confianza requieren la comprobación de la identidad por medios seguros. Todos los roles de confianza son realizados por individuos.

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

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.

LLEIDA.NET tiene documentación específica que da más detalles de cada función

6.3 Controles de personal

6.3.1 Antecedentes, cualificaciones, experiencia y requisitos de aplicación

LLEIDANET emplea personal con la experiencia y con las cualificaciones necesarias para desempeñar sus responsabilidades laborales.

Todo el personal con funciones de confianza está libre de cualquier interés que pueda afectar su imparcialidad con respecto a las operaciones de LLEIDA.NET.

6.3.2 Requisitos de formación

LLEIDA.NET proporciona a su personal la formación necesaria para desempeñar sus responsabilidades laborales de manera competente y satisfactoria. La formación del personal incluye lo siguiente:

- Una copia de la Declaración de Prácticas de Certificación.
- Sensibilización y formación sobre la seguridad de la información
- Procedimientos de seguridad para cada función específica.
- Procedimientos de gestión y operación para cada función específica.
- Procedimiento de recuperación de desastres.
- Procedimiento de gestión de incidencias

Entre los requisitos de seguridad aplicable se encuentran los recogidos en el Sistema de Gestión de la Seguridad de la Información desarrollado en el marco de la certificación ISO 27001.

6.3.3 Frecuencia y requisitos de cursos de perfeccionamiento

Cualquier cambio significativo en las operaciones de los servicios de certificación digital de LLEIDA.NET requerirá un plan de capacitación y la implementación del plan será documentada.

6.3.4 Rotación y secuencia laboral

No existe rotación de tareas en los puestos de confianza.

6.3.5 Sanciones para acciones no autorizadas

Incidentes de seguridad de la información. LLEIDA.NET tiene un plan de gestión de incidentes de seguridad que ha sido diseñado tomando lo dispuesto en la ISO 27001

Sanciones para acciones no autorizadas. Existe un régimen disciplinario interno que define las sanciones aplicables al personal en función de la gravedad de las actuaciones.

6.3.6 Requisitos de contratación del personal

LLEIDANET mantiene una política de contratación de personal que busca los perfiles adecuados para su actividad y cuenta con criterios de idoneidad para la asignación de roles y responsabilidades.

LLEIDANET cumple con sus obligaciones en materia de igualdad y, en el marco de las relaciones con sus empleados, tiene asumido un compromiso fehaciente para la promoción e implantación efectiva de los principios de igualdad de oportunidades entre mujeres y hombres, y de no discriminación por razón de género, raza, origen, religión, etc.

En este mismo sentido manifiesta su compromiso de trabajo para garantizar la accesibilidad de sus servicios e instalaciones a todas las personas, independientemente de sus capacidades técnicas, cognitivas o físicas.

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

6.3.6.1 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.

6.3.7 Documentación proporcionada al personal

Todo el personal con funciones de confianza recibe:

- Una copia de la Declaración de Prácticas de Certificación
- Una copia del Manual de Acogida (Handbook) que incluye consideraciones específicas de confidencialidad y seguridad.
- Documentación que define las obligaciones y procedimientos asociados a cada rol.
- El personal también tiene acceso a los manuales de operaciones de los distintos componentes del sistema.

6.4 Procedimientos de registro de auditoría

Los registros de auditoría se utilizan para reconstruir los eventos significativos registrados en el sistema de LLEIDA.NET o de la Autoridad de Registro y el usuario o evento que dio origen al registro. Los registros también se utilizarán en el arbitraje para resolver cualquier posible conflicto comprobando la validez de una firma en un momento dado.

6.4.1 Tipos de eventos registrados

LLEIDANET registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la ECD.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la ECD a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la ECD.
- Encendido y apagado de la aplicación de la ECD.
- Cambios en los detalles de la ECD y/o sus claves.

- Cambios en la creación de políticas de los servicios.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- 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

LLEIDA.NET también conserva, ya sea manualmente o electrónicamente, la siguiente información:

- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de los servicios de certificación digital

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.

6.4.2 Frecuencia de procesamiento del registro

Los registros de auditoría son revisados regularmente por el auditor de LLEIDANET.

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.

6.4.3 Periodo de retención del registro de auditoría

LLEIDA.NET almacena la información de los registros de auditoria dependiendo de la naturaleza de los mismos.

Los auditores tienen derecho a acceder a los registros de auditoría.

La eliminación o modificación no autorizada de las entradas de registro se evita escribiendo registros de auditoría utilizando medios no aptos para su reescritura o borrado sin detección.

LLEIDA.NET almacena la información de los registros de auditoría del sistema de certificados durante al menos quince (15) años.

6.4.4 Protección de los registros de auditoría

La eliminación o modificación no autorizada de las entradas de registro se evita escribiendo registros de auditoría utilizando medios no aptos para su reescritura o borrado, como un CD-ROM u otros.

6.4.5 Procedimientos de copia de seguridad para registros de auditoría

Los sistemas de gestión de copias de respaldo están contemplados entre las medidas de seguridad adoptadas por la entidad.

Cuando haya cualquier gestión de ECD se hace la copia de respaldo de la situación anterior. Siempre habrá respaldo de la última modificación, y, en su caso, en ubicaciones separadas a las de prestación del servicio.

6.4.6 Sistema de recogida de información de auditoria

Los registros de auditoría y su copia de respaldo se obtienen diariamente, en general de manera automática.

6.4.7 Notificación al sujeto causa del evento

En general, no existe procedimiento de notificación a los sujetos causa de los eventos de auditoría en ninguno de los escenarios de recogida, ni en el automático ni en el manual.

En el sistema de emisión de certificados, 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.

6.4.8 Evaluaciones de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de LLEIDA.NET.

Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación UNE-ISO/IEC 27001 que están reflejados en el documento de Análisis de riesgos.

En este documento se especifican los controles implantados para garantizar los objetivos de seguridad requeridos.

Además, se contratan externamente auditorías de "White HatEthical Hacking" o "PenetrationTesting"

6.5 Archivo de informaciones y registros

6.5.1 Tipo de informaciones y eventos registrados

LLLEIDA.NET conserva los siguientes documentos implicados en el ciclo de vida de los servicios:

- Todos los registros de auditoría de sistema detallados en la sección 6.4 de esta declaración de prácticas de certificación.
- Las distintas versiones de la Declaración de Prácticas de Certificación
- Las Políticas de Certificación en sus diferentes versiones
- Solicitudes de activación y desactivación de los servicos.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Documentación recogida por la Entidad de Registro de LLEIDA.NET
- Información del ciclo de vida del servicio.
- Contratos con clientes que solicitan servicios
- Contratos con terceros para la prestación de los servicios

6.5.2 Periodo de retención para el archivo

De conformidad con la legislación vigente, LLEIDA.NET conservará durante 5 años toda la información y documentación relativa a los servicios y las declaraciones de prácticas de certificación.

El periodo de conservación de este tipo de documentación para el servicio de certificados es de quince 15 años.

6.5.3 Protección del archivo

LLEIDA.NET establece controles políticas y procedimientos que garantizan la integridad de la documentación y el acceso únicamente por personal autorizado.

El almacenamiento se realiza en un lugar con los correspondientes controles de seguridad.

6.5.4 Procedimientos de backup del archivo

LLEIDA.NET realiza backup periódico de la información, como mínimo diariamente.

6.5.5 Requerimientos para el sellado de tiempo de los registros

La información queda fechada por una fuente fiable de tiempo. No se utiliza para ello ninguna firma electrónica

6.5.6 Sistema de recogida de información de auditoría

LLEIDA.NET utiliza un sistema interno de recogida y almacenamiento de la información de acuerdo a su procedimiento en el marco de la ISO 27001.

6.5.7 Procedimientos para obtener y verificar información archivada

LLEIDA.NET en el marco de la ISO 27001 tiene procedimientos para verificar la integridad de la información almacenada.

El acceso solo es posible para personal autorizado.

6.6 Cambio de claves

6.6.1 Cambio de claves de la raíz

El procedimiento de cambio de claves de la Raíz es el equivalente a generar un nuevo certificado digital. Los certificados emitidos por las ECD 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 ECD caduque se realizará un cambio de claves. La vieja ECD y su clave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por las subordinadas de la ECD vieja. Se generará una nueva ECD 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.

6.6.2 Cambio de claves de una ECD subordinada

El procedimiento de cambio de claves de una ECD 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 ECD subordinada caduque se realizará un cambio de claves. La vieja subordinada de ECD y su clave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por la subordinada ECD 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.

6.7 Recuperación en caso de compromiso del servicio o desastre

6.7.1 Procedimientos de gestión de incidencias y compromisos

LLEIDA.NET tiene previstos procedimientos internos para la gestión de incidencias e incidentes de seguridad que puedan suponer compromiso en la seguridad de la información almacenada que les permiten gestionar diversos incidentes, particularmente:

- que el sistema de seguridad de la entidad de certificación ha sido vulnerado;
- que se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio;
- que los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.

6.7.2 Corrupción de recursos, aplicaciones o datos

En caso de corrupción de recursos, aplicaciones o datos se activan los correspondientes procesos de gestión de incidentes que permiten su detección, investigación, corrección y comunicación oportuna a los agentes afectados.

Dependiendo del tipo de incidente pueden activarse los procedimientos de continuidad de negocio.

6.7.3 Procedimiento ante compromiso de la clave privada de la entidad

La Entidad de Certificación LLEIDA.NET 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 LLEIDA.NET o de una de sus EC subordinadas. En estos casos se deben revocar de manera inmediata las claves privadas comprometidas de LLEIDA.NET 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 ECD el proveedor de servicio de Certificación:

> Informará a todos los Titulares, Tercero que confía y otras ECD'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.

6.7.4 Continuidad del negocio después de un desastre

El Plan de continuidad del negocio garantiza la recuperación frente a un desastre. En función de la criticidad de los sistemas afectados el tiempo de recuperación puede ser de 24 horas. Los servicios objeto de acreditación mantendrán una disponibilidad de 99.8% 7x24x365 al año.

6.8 Terminación o cese de la ECD o RA

6.8.1 Autoridad de certificación

LLEIDANET tiene un Plan de de Cese de la ECD que especifica el procedimiento que se llevará a cabo en caso de que tal evento ocurra.

LLEIDA.NET 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 LLEIDA.NET 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, LLEIDA.NET 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.

6.8.2 Autoridad de registro

Después de que una Autoridad de Registro deje de realizar sus operaciones, transferirá a LLEIDA.NET los registros relativos a la identificación de solicitantes de los servicios y a los registros de auditoría.

Cualquier otra información será cancelada y destruida.

7 CONTROLES TÉCNICOS DE SEGURIDAD

7.1 Generación e instalación del par de claves

7.1.1 Generación del par de claves

7.1.1.1 Generación del par de claves de la ECD

La generación del par de claves de la ECD Raíz, se realizó dentro de la sala criptográfica del proveedor de servicios de plataforma de la ECD/RA 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 LLEIDA.NET. 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.

7.1.1.2 Generación del par de claves de la RA

La generación del par de claves de las EC subordinadas de LLEIDA.NET, se realiza dentro de la sala criptográfica del proveedor de servicios de LLEIDA.NET 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.

7.1.1.3 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.

7.1.2 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.

7.1.3 Envío de la clave pública al emisor del certificado

La clave pública es enviada a la ECD como parte de la petición de solicitud del certificado digital en formato PKIX-CMP.

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

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

El certificado de la ECD Raíz puede ser consultado por los terceros de confianza en la dirección https://certs.esigna.es/root/ca_root_lleidasas.crt

El certificado de la ECD Subordinada puede ser consultado por los terceros de confianza en la dirección https://certs.esigna.es/ca/lleidasas_pki_001.crt

7.1.5 Tamaños de claves y algoritmos utilizados

El tamaño de las claves de la EC Raíz de LLEIDA.NET. es de 4096 bits.

El tamaño de las claves de las Subordinadas de LLEIDA.NET es de 4096 bits.

El tamaño de las claves de los certificados emitidos por LLEIDA.NET 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[10].

[10] 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.

En todo caso, LLEIDA.NET se mantiene informada de las tecnologías existentes y en caso de que los sistemas de cifrado pierdan vigencia por la aparición de nuevas tecnologías, se tomarán inmediatamente medidas para devolver la confiabilidad al sistema, modificándose convenientemente la presente Declaración de Prácticas de Certificación.

7.1.6 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 LLEIDA.NET 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.

7.1.7 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 LLEIDA.NET.

Todos los certificados digitales emitidos por la Entidad de Certificación LLEIDA.NET 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

7.2 Protección de la clave privada en módulo criptográfico

7.2.1 Estándares para los módulos criptográficos

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

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

Las claves privadas, de LLEIDA.NET 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 LLEIDA.NET por medio de una combinación de claves en poder de varios operadores.

7.2.3 Custodia de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDA.NET 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.

Los datos técnicos del dispositivo son los siguientes:

- nShield F3 ready, 500 TPS

- Conectividad PCI, certificado FIPS 140-2 nivel 3 Common Criteria EAL 4+, con capacidades de SEE (Motor Seguro de Ejecución de Código) y Criptografía ECC (Criptosistema de Curva Elíptica).

La clave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del titular. Bajo ninguna circunstancia LLEIDA.NET 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 LLEIDA.NET

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 LLEIDA.NET en calidad de Entidad de Certificación Digital, 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.

7.2.4 Copia de seguridad de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDA.NET 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 LLEIDA.NET, están almacenadas en dispositivos externos protegidas criptográficamente por un control dual y solo son recuperables dentro de un dispositivo igual al que se generaron.

7.2.5 Archivado de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDA.NET 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).

7.2.6 Transferencia de la clave privada al módulo criptográfico

Las claves privadas de la Entidad de Certificación LLEIDA.NET 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.

7.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Entidad de Certificación LLEIDA.NET 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.

7.2.8 Método de activación de la clave privada

Las claves privadas, de LLEIDA.NET 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 LLEIDA.NET 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 ECD. Se necesitan al menos 2 de 4 personas para la activación de las claves.

7.2.9 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 ECD. Se activa nuevamente mediante el uso de control multipersona, siguiendo los procedimientos marcados por el fabricante del módulo criptográfico.

7.2.10 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.

7.2.11 Clasificación de los módulos criptográficos

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

7.3 Otros aspectos de la gestión del par de claves

7.3.1 Archivo de la clave pública

La EDC 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.

7.3.2 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 LLEIDA.NET es de treinta (30) años.

7.4 Datos de activación

7.4.1 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.

7.4.2 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.

7.4.3 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.

7.5 Controles de seguridad informática

7.5.1 Requisitos técnicos específicos de seguridad informática

Existen una serie de controles en los diferentes componentes que conforman el sistema de para la prestación de los servicios LLEIDANET (bases de datos de LLEIDANET, servicios de Internet de LLEIDANET, funcionamiento de la ECD y gestión de redes):

- Controles operativos

- Todos los procedimientos operativos están debidamente documentados en los correspondientes manuales de operaciones. LLEIDANET mantiene un plan de contingencia
- Se han implementado herramientas para proteger contra virus y códigos maliciosos.
- El equipo se mantiene de manera continua para garantizar la disponibilidad e integridad ininterrumpidas
- Existe un procedimiento para guardar, borrar y eliminar con seguridad medios de almacenamiento, medios extraíbles y equipos obsoletos.

- Intercambio de datos. Los intercambios de datos están encriptados para garantizar la confidencialidad.
  - Transmisión de los datos de preinscripción.

- Control de acceso
  - Las identificaciones de usuario únicas se utilizan de tal manera que los usuarios están asociados y pueden ser responsables de sus acciones.
  - Los derechos se asignan de acuerdo con la norma de proporcionar a los usuarios la menor cantidad de privilegios del sistema que necesitan para hacer su trabajo.
  - Los derechos de acceso se cancelan inmediatamente cuando los usuarios cambian de trabajo o salen de la organización.
  - El nivel de acceso asignado a los usuarios se revisa cada tres meses.
  - Los privilegios del sistema se asignan caso por caso y terminan una vez que el motivo de su asignación ya no es válido.
  - LLEIDANET mantiene directrices de calidad de contraseñas.

7.5.2 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.

7.6 Controles técnicos del ciclo de vida

7.6.1 Controles de desarrollo del sistema

Se controla la implementación del software para los sistemas de producción.

Para evitar posibles problemas con estos sistemas, se aplican los siguientes controles:

- Existe un procedimiento de autorización formal para actualizar las bibliotecas del software (incluidos los parches) en la producción. La autorización se concede sólo después de asegurarse de que funciona correctamente.
- El sistema de pruebas se mantiene separado del sistema de producción para asegurarse de que funciona correctamente antes de pasar a la producción.
- Se conserva un archivo de registro en todas las actualizaciones de las bibliotecas.
- Se conservan las versiones anteriores del software.
- El software adquirido se mantiene al nivel soportado por el proveedor.
- Se cuenta con procedimientos que permiten incluir extensiones sobre el código fuente.

7.6.2 Controles de gestión de seguridad

LLEIDANET lleva a cabo auditorías internas y externas para comprobar la correcta aplicación de sus políticas. Entre ellas se incluyen:

- Auditoría respecto a la norma ISO 27001;
- Auditorías de tipo "ethical hacking" (Test de penetración);
- Auditorías respecto a la norma eIDAS.

7.6.3 Controles de seguridad del ciclo de vida

Con el fin de realizar pruebas, se requiere un gran volumen de datos lo más similar posible a los datos de producción. LLEIDANET evita el uso de bases de datos de producción con información personal.

Los controles de seguridad aplicados en el ciclo de vida de los certificados inciden, especialmente, en la solicitud de certificados y en su revocación.

7.7 Controles de seguridad de red

LLEIDA.NET 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.

7.8 Fuentes de tiempo

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

8 PERFILES DE CERTIFICADO Y CRL

8.1 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 LLEIDA.NET, 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.

Descripción del contenido de los certificados

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por LLEIDA.NET
Algoritmo de Firma	SHA1RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para LLEIDA.NET como emisor se especifica: Description =Lleida SAS Subordinate CA CO 001 CN = Certification Authority Root Lleida SAS O = Lleida SAS 2.5.4.97 = VATES- 9005710383 SERIALNUMBER = 9005710383 OU = Certification Authority Lleida SAS T = Subordinate Certificate Authority Lleida SAS L = BOGOTA C = CO
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 LLEIDA.NET 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 LLEIDA.NET 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 LLEIDA.NET 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 LLEIDA.NET. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de LLEIDA.NET, 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 LLEIDA.NET por tanto, es cero.

8.1.1 Numero de versión

Los certificados emitidos por la Entidad de Certificación LLEIDA.NET cumplen con el estándar X.509 Versión 3.

8.1.2 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.

8.1.3 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

8.1.4 Formato de nombres

El documento guía que LLEIDA.NET 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 LLEIDA.NET 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.

8.1.4.1 Certificado Raíz

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

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

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

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

8.1.4.2 Certificados de las Subordinadas

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDA.NET, tiene las siguientes características:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

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

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

8.1.4.3 Certificados de titular

El DN del 'issuer name' de los certificados de titular de LLEIDA.NET., tiene las siguientes características generales:

Description =Lleida SAS Subordinate CA CO 001

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

2.5.4.97 = VATES- 9005710383

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

T = Subordinate Certificate Authority Lleida SAS

L = BOGOTA

C = CO

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.

8.1.5 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".

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

El identificador de objeto de la Política de certificado se indica en el apartado 2.3 Nombre del documento e Identificación.

8.1.7 Uso de la extensión "Policy Constraints"

No se estipula.

8.1.8 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.

8.1.9 Tratamiento semántico para la extensión "certificate policy"

No se estipula.

8.2 Perfil de CRL

Las CRL´s emitidas por la Entidad de Certificación LLEIDA.NET cumplen con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" y contienen los siguientes elementos básicos:

8.2.1 Número de versión

Las CRL´s emitidas por LLEIDA.NET cumplen con el estándar X.509 versión 2.

8.2.2 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).

8.3 Perfil de OCSP

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

8.3.1 Número de versión

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

8.3.2 Extensiones del OCSP

No aplica.

9 AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

LLEIDA.NET ha superado anualmente desde 2015 todas las auditorías de su Sistema de Seguridad de Gestión de la Información que cumple con los requisitos de ISO/IEC 27001:2013 con el siguiente alcance que se describe en el SoA y accesibe en el certificado acreditativo: https://www.lleida.net/docs/es/IS_632576_lleidanet.pdf

LLEIDA.NET ha superado una auditoría de tipo "Ethical Hacking" para verificar la resistencia de su infraestructura a diversos ataques de seguridad potenciales.

LLEIDA.NET (matriz) obtuvo en 2018 la certificación Prestador de Servicios de Confianza para las Transacciones Electrónicas conforme a la norma técnica ETSI EN 319 401 V2.1.1. General Policy Requirements for Technical specifications Trust Service Providers (Article 44, Regulation (Eu) nº 910/2014) para sus Servicios de entrega electrónica certificada cualificada y actualmente se somete con la periodicidad indicada en el Reglamento UE 910/2014 a auditorías de cumplimiento de los requisitos relativos a los prestadores de servicios de electrónicos de confianza cualificados, para todos los servicios que presta, en base a las normas:

- ETSI EN 319 401 V2.2.1 (2018-04) - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2 (2018-04) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

La infraestructura y procedimientos de la plataforma del servicio de certificados y estampado cronológico será evaluado al menos anualmente por un organismo de evaluación de la conformidad.

El proveedor de la plataforma cuenta con la 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.

9.1 Frecuencia de los controles de conformidad para cada entidad

LLEIDA.NET lleva a cabo las auditorías de sus servicios y sistemas con la siguiente frecuencia:

- ISO 27001, ISO 9001, ISO/IEC 33000, ISO/IEC 12207, peridicidad anual
- Servicios de confianza eIDAS, periodicidad bianual

9.2 Identificación/cualificación del auditor

LLEIDANET confía sus auditorías externas a auditores con la necesaria cualificación y experiencia acreditada que actúen con total independencia e imparcialidad.

9.3 Relación entre el auditor y la entidad auditada

Las empresas auditoras no tienen ninguna vinculación con LLEIDANET y los profesionales que realizan las auditorías están libres de conflictos de intereses.

9.4 Tópicos cubiertos por el control de conformidad

Con carácter general el objetivo de la auditoría es establecer que:

a) LLEIDA.NET garantiza la calidad del servicio prestado.

b) LLEIDA.NET cumple con los requerimientos de las Políticas de Certificación y lo hace de la manera establecida en su Declaración de Prácticas de

c) LLEIDA.NET ajusta sus Políticas de Certificación y Declaración de Prácticas de Certificación, aprobado por su Comité de Seguridad y con lo establecido en la normativa vigente.

d) LLEIDA.NET gestiona de forma adecuada la seguridad de sus sistemas de información.

Para ello y con carácter general, los elementos objeto de auditoría serán los siguientes:

- Procesos y recursos relacionados con el ciclo de vida de los certificados de certificados tanto en la Autoridad de Certificación como en las Autoridades de Registros
- Sistemas de información.
- Seguridad del centro de proceso de datos.
- Documentación

9.5 Acciones a tomar como resultado de una deficiencia

Dependiendo de la severidad de la deficiencia las acciones a tomar pueden ir desde pequeñas acciones correctoras comunicadas al personal afectado de la empresa, hasta la comunicación al comité de seguridad de los resultados para que decida sobre un eventual cese temporal de actividad.

9.6 Comunicación de resultados

Los resultados de las auditorías se comunican al Comité de Seguridad de LLEIDA.NET para que emprenda las acciones oportunas en función de los resultados.

La actualización de los resultados positivos de las auditorías está disponible en la web de LLEIDA.NET

10 OTRAS CUESTIONES EMPRESARIALES Y LEGALES

10.1 Tarifas

10.1.1 Tarifas de activación de servicio

Las tarifas no sujetas a negociación comercial serán públicas en la web de LLEIDA.NET.

10.1.1.1 Tarifas de emisión o renovación de certificados

Las tarifas serán definidas por LLEIDA.NET de acuerdo a los contratos celebrados con sus clientes.

10.1.1.2 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.

10.1.1.3 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.

10.1.1.4 Tarifas de otros servicios como información de políticas

LLEIDANET permitirá el acceso gratuito a las Políticas de Certificación y a la declaración de Practicas de Certificación

Los servicios adicionales que tengan coste y no estén sujetos a negociación comercial tendrán sus tarifas publicadas en la web de LLEIDA.NET

10.1.2 Política de reintegros

No existe una política general de reintegros en la prestación de estos servicios. Únicamente se reintegrará valor del tiempo de vigencia restante de los certificados en caso de cese de la ECD, si los suscriptores lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación de dicho cese y no se a ejecutado la transferencia del certificado a otra ECD por petición del suscriptor.

10.2 Capacidad financiera

LLEIDA.NET cuenta con activos suficientes para realizar sus actividades y, en su caso, hacer frente a sus obligaciones.

10.2.1 Cobertura de seguro

LLEIDA.NET cuenta con un Seguro de Responsabilidad Civil adecuado a sus actividades, según lo dispuesto en la normativa estatal vigente.

10.2.2 Indemnización a los terceros que confían en los servicios prestados por LLEIDANET

LLEIDA.NET tiene contratado un seguro de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los servicios que proporciona esta ECD por importe de detallar cumpliendo así con la obligación que se establece en detallar.

10.3 Política de confidencialidad

10.3.1 Información confidencial

LLEIDANET considera información confidencial toda aquella información que no haya sido catalogada como pública.

La divulgación de este tipo de información queda restringida a los casos legalmente previstos.

10.3.2 Información no confidencial

LLEIDA.NET considera información de no confidencial:

- La contenida en la Declaración de Prácticas de Certificación
- La contenida en las diferentes Políticas de Certificación.
- Toda aquella información que sea calificada como pública

10.3.3 Responsabilidad para proteger la información confidencial

LLEIDA.NET 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. LLEIDA.NET 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. LLEIDA.NET 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 LLEIDA.NET 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.

10.4 Consideraciones de protección de datos de carácter personal

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal. De conformidad con la ley 1581 de 2012.

Conforme establece la citada legislación de protección de datos, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados información privada:

- Solicitudes de activación de servicios, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de los mismos, excepto las informaciones indicadas en la sección correspondiente.
- Credenciales generadas y/o almacenadas por la Entidad de Certificación
- Cualquier otra información que pudiera identificarse como "Información confidencial"

Los datos recabados por la ECD tendrán la consideración legal que corresponda a su naturaleza, siendo normalmente datos de nivel básico. La información confidencial de acuerdo con la normativa de protección de datos es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado .

10.4.1 Consentimiento para usar datos de carácter personal

LLEIDA.NET informa que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. LLEIDA.NET fundamenta el tratamiento de datos fundamentalmente en: el interés legítimo que tiene en responder solicitudes de información sobre sus servicios, la ejecución de un contrato o en el consentimiento expreso del titular del dato. Los titulares de datos pueden retirar ese consentimiento en cualquier momento.

Los datos recabados son los mínimos necesarios para la prestación de los servicios y se conservan por los períodos que establece la Ley. No se ceden a terceros, salvo obligación legal; ni se realizan perfiles o se toman decisiones automatizadas en base a estos datos.

LLEIDA.NET le informa igualmente que, en caso de solicitar los servicios amparados en esta DPC por vía telefónica, su voz podrá ser grabada durante las conversaciones telefónicas que mantenga con la Autoridad de Registro (AR) o la Entidad de Certificación Digital (ECD), con el fin de permitir una tramitación segura de la solicitud de emisión o revocación de certificados. Previo a la grabación se le ofrecerá la información básica de protección de datos estipulada en normativa de protección de datos y se le recabará su consentimiento expreso. Los datos personales recabados por esta vía se incorporarán al fichero de bases de datos del que es responsable LLEIDA.NET.

Para más información sobre el ejercicio de los derechos al amparo de la normativa y sobre el tratamiento de sus datos personales por LLEIDANET consulte la nota legal más extensa, incluida en www.lleida.net/co

10.4.2 Comunicación a terceros de datos de carácter personal

Los datos de carácter personal solo podrán ser comunicados a terceros, siempre que el titular del derecho lo consienta expresamente, o por obligación legal.

10.5 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 sin su autorización expresa.

10.6 Responsabilidad contractual y extracontractual

10.6.1 Limitación de responsabilidad

Según la legislación vigente, la responsabilidad de LLEIDANET 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, 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 en caso de duda sobre el mantenimiento de la confidencialidad;
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado;
- Superar los límites que figuren en el certificadodigital.
- 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, 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 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.
- En el caso de robo o extravío de credenciales, y en aquellas circunstancias que hagan necesario proceder a la inactivación del servicio
- LLEIDANET no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPC y en la normativa de aplicación.

10.6.2 Responsabilidades de la ECD

LLEIDA.NET responderá en el caso de incumplimiento de sus obligaciones según se indica en en la presente DPC.

LLEIDA.NET 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 LLEIDA.NET..
3. Mantener publicada en la página Web la última versión de la DPC y las Políticas de Certificación de LLEIDA.NET
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.

10.6.3 Responsabilidades de la Autoridad de registro

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los solicitantes y la comprobación de sus datos, con las mismas limitaciones que se establecen para la ECD.

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 y el titular.
7. Identificar e informar a la EC las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

   Notificar a LLEIDANET de cualquier incidencia en la actividad delegada.

10.6.4 Responsabilidades del suscriptor de los servicios

El suscriptor de los servicios asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual use el servicio.

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 LLEIDA NET
11. No monitorizar la prestación de los servicios del LLEIDA NET, ni manipularlos o alterar su correcto funcionamiento, ni realizar actos de ingeniería inversa sobre su implementación.
12. Notificar cualquier hecho o situación anómala relativa a los servicios de LLEIDA.NET y/o a las evidencias emitidas, y que pueda ser considerado como causa de revocación de las mismas.

10.6.5 Responsabilidades de las partes que confían

Los Terceros que confían en su calidad de parte que confía en los certificados digitales emitidos por la Entidad de Certificación LLEIDA.NET 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.

10.6.6 Obligaciones de otros participantes

El Comité de Seguridad como organismo interno de la Entidad de Certificación LLEIDA.NET 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 LLEIDA.NET
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 LLEIDA.NET.
6. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la Entidad de Certificación LLEIDA.NET
7. Asegurar la existencia de controles sobre la infraestructura tecnológica de la Entidad de Certificación LLEIDA.NET
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.

10.6.7 Pérdidas derivadas del uso de servicios y certificados

A excepción de lo establecido por las disposiciones de la presente DPC, y lo determinado por Ley, LLEIDA.NET no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían en los servicios.

10.7 Indemnizaciones

Revisar apartado 10.2 Capacidad financiera

10.7.1 Indemnizaciones de la ECD

Revisar apartado 10.2 Capacidad financiera

10.7.2 Indemnizaciones de los suscriptores

Revisar apartado 10.2 Capacidad financiera

10.7.3 Indemnizaciones de las partes que confían

Revisar apartado 10.2 Capacidad financiera

10.8 Quejas. Reclamaciones y jurisdicción

Las peticiones, quejas reclamos, solicitudes y apelaciones sobre los servicios prestados por Lleida SAS seran atendidas por varios mecanismos a disposición del subscriptor y seran resueltas por las personas pertinentes e imparciales.

- Por correo electrónico a clientes@lleida.net . Deberá adjuntarse la plantilla disponible en www.lleida.net/co ECD_CO 4501 Plantilla PQRSA Lleida SAS
- Por teléfono al +57 1 381 9903

En el plazo máximo de 15 días deberán ser resueltas y notificades, previa radicación, analisis y redacción de reporte formal que sera entregado al subscriptor.

La actividad de LLEIDANET se rige por la Ley colombiana y por los Tribunales de Bogotá, salvo que el usuario ostente la condición de consumidor, lo que redundará en que se aplique la normativa de protección de consumidores.

10.9 Periodo de validez de este documento

10.9.1 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 LLEIDA.NET y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

10.9.2 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.

10.9.3 Efectos de la finalización

Al finalizar esta Declaración de Prácticas y Política de Certificación, los participantes de LLEIDA.NET 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.

10.10 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 2.8.2 contacto

10.11 Enmiendas y cambios

10.11.1 Procedimiento para realizar cambios

Las modificaciones de este documento serán aprobadas por el Comité de Seguridad de LLEIDA.NET.

Estas modificaciones estarán recogidas en un documento de Actualización de la Declaración de Prácticas de Certificación cuyo mantenimiento está garantizado por LLEIDANET.

Las versiones actualizadas de la Declaración de Prácticas de Certificación junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección www.lleidanet.es y más concretamente en https://www.lleida.net/co

LLEIDA.NET podrá modificarla Declaración de Prácticas de Certificación para lo que actuará según el siguiente procedimiento:

- La modificación estará justificada desde el punto de vista técnico, legal o comercial.
- Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones.
- Se establecerá un control de modificaciones, para garantizar, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.
- Se valorarán las implicaciones que puedan tener sobre los usuarios el cambio de especificaciones, por si fuera preciso comunicarles el cambio.

10.11.2 Mecanismo y periodo de modificación

En la fase preparatoria de las auditorías, LLEIDANET revisará el presente documento para asegurarse de que permanece actualizado en relación con los cambios que se vayan produciendo en los siguientes aspectos:

- Marco legislativo de aplicación
- Pautas de funcionamiento de emitidas por ONAC
- Publicación de estándares
- Mejoras o no conformidades identificadas en las auditorías
- Mejoras realizadas en los servicios o lanzamiento de nuevos servicios

- Adopción de productos y servicios de terceros que se integren con los ofrecidos por LLLEIDANET.

LLEIDA.NET podrá realizar modificaciones de este documento sin necesidad de informar previamente a los usuarios, como, por ejemplo:

- Correcciones de errores tipográficos en el documento
- Cambios en la información de contacto.

LLEIDA.NET podrá realizar modificaciones de este documento de las que se informará a los usuarios, tales como:

- Cambios en las especificaciones o condiciones del servicio.
- Modificaciones de URLs

Los cambios de este documento se comunican a aquellos organismos y empresas terceras que emiten certificados bajo esta DPC, así como a los auditores correspondientes. Especialmente se notificarán los cambios en esta DPC a la ONAC:

Existirá un plazo de 15 días en los que las partes interesadas podrán hacer alegaciones a los cambios en la DPC y dichas observaciones, en su caso, serán tenidas en consideración en las modificaciones finales que apruebe el órgano de Aprobación de Políticas.

10.11.3 Circunstancias bajo las cuales debe cambiarse un OID

No estipulado.

10.12 Otras disposiciones

10.12.1 Acuerdo Integro

Sin estipulación.

10.12.2 Asignación

Las ECD 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 LLEIDA.NET

10.12.3 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.

10.12.4 Cumplimiento (honorarios de abogados y exención de derechos)

LLEIDA.NET 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 LLEIDA.NET no haga cumplir una disposición de esta DPC no elimina el derecho de LLEIDA.NET 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 LLEIDA.NET

10.12.5 Fuerza Mayor

LLEIDA.NET 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.

10.13 Otras Provisiones

Sin estipulación.