



Proyecto	<b>Entidad de Certificación y Entidad de Registro o Verificación</b>
Título	<b>Plan de Privacidad</b>

Realizado por	<b>LLEIDANET PKI S.L.</b>		
Dirigido a	<b>Usuarios internos y externos</b>		
Documento	<b>DOC-200216.20A0509</b>		
Fecha aprobación	<b>30/04/2025</b>	Revisión	<b>2</b>



ER-1140/2011



NMS-0009/2012



SI-0024/2013



ES-1140/2011

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

<b>1</b>	<b>DATOS DEL DOCUMENTO .....</b>	<b>3</b>
<b>2</b>	<b>HISTORIA DEL DOCUMENTO .....</b>	<b>3</b>
<b>3</b>	<b>ELABORACIÓN, REVISIÓN Y APROBACIÓN .....</b>	<b>4</b>
<b>4</b>	<b>INTRODUCCIÓN.....</b>	<b>5</b>
<b>5</b>	<b>VISIÓN GENERAL .....</b>	<b>5</b>
<b>6</b>	<b>OBJETIVO .....</b>	<b>5</b>
<b>7</b>	<b>DEFINICIONES Y ABREVIACIONES .....</b>	<b>6</b>
7.1	PKI PARTICIPANTES.....	6
<b>8</b>	<b>ENTIDAD DE CERTIFICACIÓN ASOCIADA A LA ER DE LLEIDANET PKI S.L. ....</b>	<b>8</b>
<b>9</b>	<b>ALCANCE .....</b>	<b>9</b>
<b>10</b>	<b>PLAN DE PRIVACIDAD DE DATOS .....</b>	<b>9</b>
10.1	INFORMACIÓN RECOLECTADA Y PROTEGIDA.....	10
10.2	TRATAMIENTO DE LOS DATOS PERSONALES .....	10
10.3	FLUJO TRANSFRONTERIZO DE DATOS PERSONALES.....	11
10.4	IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD .....	11
10.5	RESPONSABILIDADES .....	14
10.6	CONFORMIDAD .....	14

## 1 DATOS DEL DOCUMENTO

Proyecto	Entidad de Certificación y Entidad de Registro o Verificación
Título	Plan de Privacidad
Código	DOC-200216.20A0509
Tipo de documento	DOC - Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI S.L.
Dirigido a	Usuarios internos y externos
Fecha aprobación	30/04/2025
Revisión	2

## 2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	05/10/2020	Creación del documento	Indenova SL (SBS)
2	30/04/2025	Actualizar el apartado de conformidad	Lleidonet PKI (CJU)

### 3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de Calidad Fecha: 30/04/2025
Revisado por:	Nombre: Lleidanet PKI SL (SB) Cargo: Administrador del Servicio Fecha: 30/04/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 30/04/2025

## 4 INTRODUCCIÓN

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

Como Entidad Certificación (EC), LLEIDANET PKI S.L. provee los servicios de emisión, distribución y revocación de certificados digitales, provistos por la EC de LLEIDANET PKI S.L..

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

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

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

## 5 VISIÓN GENERAL

Este documento tiene como objeto la descripción de las diferentes políticas de privacidad de la EC y ER en el marco del cumplimiento de los requerimientos del “Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014” o también como es conocido “Reglamento eIDAS” establecida por el Parlamento Europeo y del Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

## 6 OBJETIVO

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

## 7 DEFINICIONES Y ABREVIACIONES

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

### 7.1 PKI PARTICIPANTES.

#### 7.1.1 Entidad de Certificación LLEIDANET PKI S.L. (EC LLEIDANET PKI S.L.)

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

#### 7.1.2 Entidad de Registro LLEIDANET PKI S.L. (ER LLEIDANET PKI S.L.)

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

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

La ER puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la ER, siempre que se asegure la integridad y autenticidad

de las transacciones en la autorización de solicitudes de emisión, revocación. Sin embargo, la responsabilidad legal frente al Organismo de supervisión, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. El tercero debe garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, durante la ejecución de las actividades de tercerización, quedando claro que ante el Organismo de supervisión el responsable ante terceros es la ER.

Cabe indicar que LLEIDANET PKI S.L. suministra al tercero la Plataforma de ER para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma eSignaPKI con el certificado digital del operador.

### **7.1.3 Proveedor de servicios de certificación digital (LLEIDANET PKI S.L.)**

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

Los servicios de certificación digital que ofrece LLEIDANET PKI S.L. son provistos por la Entidad de Certificación LLEIDANET PKI S.L.

### **7.1.4 Titular**

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

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

### **7.1.5 Suscriptor**

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

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

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

#### **7.1.6 Solicitante**

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo esta CPS LLEIDANET PKI S.L.

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

#### **7.1.7 Tercero que confía**

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

#### **7.1.8 Entidad a la cual se encuentra vinculado el titular**

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

#### **7.1.9 Otros participantes**

##### **7.1.9.1 El comité de Seguridad**

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

## **8 ENTIDAD DE CERTIFICACIÓN ASOCIADA A LA ER DE LLEIDANET PKI S.L.**

LLEIDANET PKI S.L. establece la Política de Seguridad que los proveedores de servicios de certificación digital deben cumplir.

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

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



LLEIDANET PKI S.L. brinda los servicios de registro o verificación conforme a la normativa de aplicación vigente, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

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

## 9 ALCANCE

El presente plan es de cumplimiento obligatorio por los proveedores de servicios de certificación digital contratados por LLEIDANET PKI S.L.

## 10 PLAN DE PRIVACIDAD DE DATOS

El tratamiento de datos de carácter personal que realiza la LLEIDANET PKI S.L. se alinea con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico, y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los suscriptores y titulares. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de registro, a excepción que exista un previo consentimiento del titular de dichos datos o medie una orden judicial o administrativa que así lo determine.

Con este fin, se implementará un Plan de Privacidad con controles para la protección contra divulgación y uso no autorizado.

Es responsabilidad de los suscriptores garantizar que la información provista a LLEIDANET PKI S.L. sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos

## 10.1 INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de certificación y registro, LLEIDANET PKI S.L. recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.
- Contrato de solicitud de servicios.
- Videofirma del contrato. Se captura un vídeo en el que el usuario debe indicar por voz un código que aparece en pantalla. Dicho vídeo se almacena en el expediente como prueba de que el usuario solicitó el certificado.
- De las imágenes extraídas del documento o capturas de vídeo realizadas en el proceso de verificación del usuario, se generan templates de biometría facial que se almacenan en el sistema para validar y verificar los datos de identidad del usuario.

## 10.2 TRATAMIENTO DE LOS DATOS PERSONALES

Los datos facilitados por el titular y suscriptor pasarán a formar parte de los archivos automatizados propiedad de la Entidad y podrán ser utilizados por el titular del archivo para el ejercicio de las funciones propias en el ámbito de sus competencias.

De conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el titular podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición mediante instancia presentada.

LLEIDANET PKI S.L. utilizará estos datos para la prestación de los servicios de confianza de certificación digital, según se describe en la Declaración de Prácticas de Certificación lo que incluye, entre otros, la emisión y gestión de certificados digitales, así como los servicios de firma electrónica.

En este proceso, LLEIDANET PKI S.L. puede contar con la colaboración de autoridades de registro (RA) y de puntos de verificación presencial dependientes de las RA.

Cualquier tercero podrá acceder a los datos que figuren en su certificado (a excepción de la clave privada) para comprobar la validez de los mismos y validar las operaciones de firma electrónica realizados con ellos. LLEIDANET PKI S.L. no puede controlar el uso que los terceros hagan de sus datos por lo que no será responsable de ello en ningún caso.

LLEIDANET PKI S.L. tratará sus datos durante el tiempo que dure la prestación de servicios y, con posterioridad, durante el tiempo necesario para la gestión de certificados suspendidos o revocados y durante los plazos de tiempo legalmente previstos para la depuración de responsabilidades propias y de terceros.

Deberá considerarse como información no privada, la siguiente:

- Toda aquella que se incorpora a los certificados electrónicos, la información relativa al estado de vigencia de los mismos, la fecha de inicio de dicho estado (activo, revocado, caducado...), así como el motivo que provocó el cambio de estado. Por tanto, los

Certificados electrónicos, las Listas de Certificados Revocados y cualquier contenido de los mismos no es considerada información privada.

Deberá considerarse como información privada, la siguiente:

- Toda la información personal sobre las personas físicas usuarias de los Servicios de Confianza que no deba ser incorporada en los certificados y en los mecanismos que utiliza el Servicio de información y consulta sobre el estado de validez de los certificados.
- Las claves privadas del certificado del suscriptor.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de sellado de tiempo.
- En todos los casos, figurará en la Política de Privacidad que deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine.

Cualquier violación a la privacidad de esta información por parte del personal de LLEIDANET PKI S.L. o de los terceros subcontratados, será sujeto de sanción.

### 10.3 FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en el certificado digital a los países donde se encuentren las EC.

### 10.4 IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta las medidas de seguridad requeridas de conformidad con el RGPD en cuanto al acceso y tratamiento que realiza sobre los datos personales de solicitantes y suscriptores de los Certificados.

A. Medidas preventivas:

- a) Se restringirá el acceso a los datos personales a personal autorizado.
- b) Estos datos serán protegidos contra acceso no autorizado.
- c) Se concientizará al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
- d) Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de sellado de tiempo, las mismas que deben informar sobre:

- i. El hecho de que se está recolectando información personal;
  - ii. Los propósitos para los cuales se recolecta dicha información personal;
  - iii. Los tipos de personas u organizaciones a las que dicha información podría ser revelada;
  - iv. La identidad y ubicación del responsable de la información personal, incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal;
  - v. Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
  - vi. Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.
- e) Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

#### B. Limitaciones a la recolección:

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

#### C. Uso de la información personal

- a) La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:
- i. que exista consentimiento del individuo al que pertenece la información personal recolectada;
  - ii. que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
  - iii. que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

#### D. Elección

- a) Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin de que puedan decidir respecto a la recolección, uso y revelación de su información personal. Puede no resultar necesario que

los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

E. Integridad de la información personal

- a) La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

F. Salvaguardas a la seguridad

- a) Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

G. Acceso y corrección

- a) Los individuos deben ser capaces de:
  - i. obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.
  - ii. comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y
  - iii. cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.
- b) Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:
  - i. La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
  - ii. la información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
  - iii. se podría violar la privacidad de la información de personas diferentes al individuo.
- c) Si una solicitud bajo el supuesto (a) o (b) o un cuestionamiento bajo el supuesto (c) es denegado, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

## 10.5 RESPONSABILIDADES

El Responsable de Seguridad de LLEIDANET PKI S.L. gestiona la implementación y vela por el cumplimiento del presente plan, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

## 10.6 CONFORMIDAD

Este documento ha sido revisado por el Administrador del Servicio y aprobado por la Comisión de Seguridad de la Información de LLEIDANET PKI S.L., y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.