



Proyecto	Servicios de Valor Añadido (SVA)
Título	Plan de Privacidad

Realizado por	LLEIDANET PKI S.L.		
Dirigido a	Usuarios internos y externos		
Documento	DOC-200216.20A0509		
Fecha aprobación	02/05/2025	Revisión	2



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

1	DATOS DEL DOCUMENTO	3
2	HISTORIA DEL DOCUMENTO	3
3	ELABORACIÓN, REVISIÓN Y APROBACIÓN	4
4	INTRODUCCIÓN.....	5
5	OBJETIVO	5
6	OBJETO DE LA ACREDITACIÓN.....	5
7	DEFINICIONES Y ABREVIACIONES	6
7.1	PKI PARTICIPANTES.....	7
8	RESPONSABILIDADES DE LLEIDANET PKI S.L.	8
9	ALCANCE	9
10	PLAN DE PRIVACIDAD DE DATOS	9
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	PREVENCIÓN DEL DAÑO	13
10.6	NOTIFICACIÓN DE PRÁCTICAS	14
11	AUDITORÍA.....	14
12	REVISIÓN, ACTUALIZACIÓN Y PUBLICACIÓN DEL PLAN	14
13	RESPONSABILIDADES.....	15
14	CONFORMIDAD	15

1 DATOS DEL DOCUMENTO

Proyecto	Servicios de Valor Añadido (SVA)
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	02/05/2025
Revisión	2

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	05/10/2020	Creación del documento	Indenova SL (SBS)
2	02/05/2025	Actualizar los roles de las personas que pertenecen a la comisión de seguridad de la información	Lleidanet PKI (CJ)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de Calidad Fecha: 02/05/2025
Revisado por:	Nombre: Lleidanet PKI SL (SB) Cargo: Administrador del Servicio Fecha: 02/05/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 02/05/2025

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 Prestador de Servicios de Valor añadido - SVA, LLEIDANET PKI S.L. provee servicios través de la implementación de soluciones que utilizan los certificados digitales para asegurar las transacciones documentarias y de negocio de las organizaciones tanto en el sector privado como en el gubernamental. En este sentido, LLEIDANET PKI S.L. provee las soluciones de software y el sistema de gestión necesarios para en conjunto regular y controlar la gestión de usuarios y el intercambio seguro de información, así como la generación y protección de registros auditables de las transacciones realizadas.

Como Entidad de 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 OBJETIVO

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" 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 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación de LLEIDANET PKI S.L. cubre los sistemas de aplicaciones de software de trámite administrativo, el cual utiliza procesos de firma digital, autenticación y cifrado para resguardar la autenticidad, integridad y confidencialidad de las transacciones o trámites administrados: asimismo, la

acreditación cubre las políticas y procedimientos necesarios para gestionar y proteger los servicios y sistemas de certificación digital.

LLEIDANET PKI S.L. no provee la infraestructura de hardware, firmware, comunicaciones y entorno donde son procesados los servicios de valor añadido, sino que éstos son provistos por las organizaciones clientes de los servicios de LLEIDANET PKI S.L., por lo que no son materia de la presente acreditación.

7 DEFINICIONES Y ABREVIACIONES

Prestador de Servicios de Valor Añadido:	SVA: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la legislación vigente.
Servicios de valor añadido:	Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
Política de servicios de valor añadido:	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, modificación, suspensión de certificados digitales en el marco de la regulación establecida por el Organismo de supervisión.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que
Política de Certificación:	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Suscriptor:	Entidad que requiere los servicios provistos por la SVA 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.
Titular:	Entidad que requiere los servicios provistos por la EC 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 Autoridad 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.

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 esta CPS.

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 Director de nuevos negocios, el Administrador del Sistema y el Director técnico 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 RESPONSABILIDADES DE LLEIDANET PKI S.L.

LLEIDANET PKI S.L. establece la Política y el Plan de Privacidad que los usuarios de las SVA y proveedores de servicios de certificación digital deben cumplir para asegurar la integridad, autenticidad y confidencialidad de la información de los clientes de LLEIDANET PKI S.L. y de los activos críticos que forman parte de los servicios de certificación digital.

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 a su documento Declaración de Prácticas de Certificación, publicado en:

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

LLEIDANET PKI S.L. brinda los servicios de certificación 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 usuarios de Servicios de Valor Añadido (SVA) y proveedores de servicios de certificación digital contratados por LLEIDANET PKI S.L..

10 PLAN DE PRIVACIDAD DE DATOS

LLEIDANET PKI S.L. garantiza la protección de datos personales de los suscriptores y titulares de los servicios de registro, en cumplimiento del 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).

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 SVA, 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.

10.1.1 Uso de la información personal

La información personal colectada será usada sólo dentro de los propósitos de recolección y otros compatibles relacionados, excepto:

- Aquellos que son recolectados con el consentimiento de los individuos propietarios de la información personal.
- Cuando sea necesario para proveer un servicio o producto solicitado por el individuo.
- Por autoridad de la Ley u otro instrumento legal, proclamaciones y pronunciamientos de efecto legal.

10.2 TRATAMIENTO DE LOS DATOS PERSONALES

Deberá considerarse como información no privada, la siguiente:

- Información personal públicamente disponible

En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por el RGPD, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- 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 de 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.

Si fuere apropiado, los individuos deberían ser provistos con mecanismos claros, comprensibles, prominentes, accesibles y asequibles para ejecutar selecciones en función de la recolección, uso y revelación de su información personal. Puede no ser apropiado para los controladores de información personal proveer estos mecanismos cuando se recolecte información públicamente disponible.

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 lo establecido por la RGPD a través de Reglamento general de protección de datos respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

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 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. Rendición de cuentas

El controlador podría ser sometido a una rendición de cuentas por el cumplimiento con las medidas que debe implementar para dar efecto a los principios estipulados en el presente documento. Cuando la información personal ha de ser transferida a otra persona u organización, sea de ámbito nacional o internacional, el controlador debería obtener el consentimiento del individuo o ejecutar la debida diligencia y tomar pasos razonables para asegurar que la persona u organización receptora protegerá la información de manera consistente con estos principios.

H. 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.

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 PREVENCIÓN DEL DAÑO

Evaluar el riesgo al que la información personal se encuentra expuesta, e implementar medidas preventivas para reducir el impacto por el daño ocasionado, de manera proporcional a la probabilidad y severidad de los daños a los que se encuentra expuesta la información personal durante su recolección, uso o transferencia.

Se recogerá únicamente la información que resulte indispensable para la prestación del servicio. Todo el personal que interviene en el proceso para la prestación del servicio debe cumplir con lo

establecido en la política de seguridad, con el fin de prevenir y evitar la pérdida, alteración, acceso no autorizado, mal uso o robo de la información personal recogida.

Todo el personal que interviene en la prestación del servicio tiene que estar capacitado sobre la protección de los datos personales.

10.6 NOTIFICACIÓN DE PRÁCTICAS

Los controladores de información personal deberían proveer declaraciones claras y accesibles sobre sus prácticas y políticas respecto de la información personal que debe incluir:

- El hecho que la información personal es colectada.
- Los propósitos por los cuales la información personal es colectada.
- Los tipos de personas u organizaciones a los cuales la información personal puede ser revelada.
- La identidad y ubicación del controlador de la información personal, incluyendo información para contactarlo acerca de sus prácticas y manejos de la información personal.
- Las opciones y medios que los controladores ofrecen a los individuos para limitar el uso y revelación, y el acceso correcto a su información personal.

Todos los pasos que deben ser tomados para asegurar que la notificación ha sido provista antes o en el momento de la recolección de información personal.

Puede no ser apropiado para los controladores de información personal notificar respecto de la recolección de información disponible públicamente.

11 AUDITORÍA

LLEIDANET PKI S.L. se debe someter a procesos de auditoría periódica por parte del organismo de evaluación de la conformidad para el mantenimiento de la acreditación de la SVA.

12 REVISIÓN, ACTUALIZACIÓN Y PUBLICACIÓN DEL PLAN

La Política de Privacidad y el Plan de Privacidad serán revisados y actualizados al menos una vez por año.

Así mismo, se publicará en la web de LLEIDANET PKI S.L. una declaración de privacidad y seguridad en modo de dichos documentos.

13 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.

14 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.

Dentro del organigrama, se define la estructura o comisión encargada de la implementación de la SVA. Como se indica anteriormente el responsable de implementar la Política de Seguridad es el Responsable de Seguridad.