Proyecto	**Autoridad de Sellado de Tiempo (TSA)**
Título	**Política de Seguridad de la TSA**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Usuarios internos y externos**		
Documento	**DOC-200216.20A0710**		
Fecha aprobación	**30/04/2025**	Revisión	**2**

Firmado por: Raul Gisbert Rodas
Fecha firma: 02/05/2025 9:56:22 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 05/05/2025 9:48:48 CEST

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

Firmado por: JORDI GISBERT RODAS
Fecha firma: 05/05/2025 12:06:24 CEST

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

1 DATOS DEL DOCUMENTO

Proyecto	Autoridad de Sellado de Tiempo (TSA)
Título	Política de Seguridad de la TSA
Código	DOC-200216.20A0710
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	07/10/2020	Creación del documento	Indenova SL (SBS)
2	30/04/2025	Cambio en la denominación a Lleidanet PKI SL Ajustes en el apartado Conformidad	Lleidanet 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.U. 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 Autoridad de Sellado de Tiempo - TSA, Lleidanet PKI S.L.U. provee los servicios de emisión de sellado de tiempo, utilizando una infraestructura periódicamente auditada para cumplir la certificación ISO 27001.

Junto a los servicios de certificación digital, Lleidanet PKI S.L.U. 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 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Lleidanet PKI S.L.U., garantiza autenticidad de los servicios de sellado de tiempo que proporciona, mediante el cumplimiento por parte su infraestructura de los controles de seguridad estipulados por el estándar internacional ISO 27001, el cual es verificado periódicamente por una entidad auditora independiente.

El alcance de esta evaluación cubre infraestructura, organización y sistemas técnicos de los servicios de Sellado de Tiempo.

6 GESTIÓN DE RIESGOS

El alcance de las medidas de seguridad de la información adoptadas por Lleidanet PKI S.L.U. para la protección de los servicios que brinda su TSU ha sido determinado en función de los resultados de evaluaciones de seguridad periódicas. Mediante la evaluación de riesgos se identifican las potenciales amenazas relacionadas a los servicios de sellado de tiempo y los controles requeridos para impedir o limitar los efectos de estas amenazas.

Se realizan análisis de riesgos anuales a fin de mantener el control de los riesgos.

7 GESTIÓN DE ACTIVOS

Todos los activos que sean relevantes para garantizar la correcta operación y autenticidad de los servicios de sellado de tiempo brindados por la TSU de Lleidanet PKI S.L.U. son identificados, clasificados e inventariados de acuerdo a su relevancia.

8 SEGURIDAD FÍSICA Y DEL ENTORNO

Los equipos de la TSU de Lleidanet PKI S.L.U. han sido ingresados al Centro de Procesamiento de Datos de un proveedor de servicio debidamente avalado con ISO 27001 e ISO 20000, el cual cuenta con los siguientes controles:

- Infraestructuras de comunicaciones Tier IV, con caminos redundantes de servicio tanto para servicios eléctricos como de climatización en las salas de alojamiento.
- El centro cuenta con 6 acometidas de fibra óptica por caminos diversos, así como servicios de radiocomunicaciones, proporcionando infraestructuras adecuadas para instalaciones de alta disponibilidad y sistemas de misión crítica.
- El acceso físico a los ambientes concernientes a los servicios de sellado de tiempo es limitado a individuos autorizados. Los cuales son identificados antes de ser autorizados y son constantemente supervisados por personal del proveedor de servicio durante su estadía en el Centro de Procesamiento de Datos. Existen perímetros de seguridad definidos con controles de autenticación antes del ingreso a las áreas restringidas. Se registran los ingresos y salidas de personal y proveedores.
- El equipo del proveedor de servicio está disponible en el centro 24x7; y está especializado en servicios de gestión de incidencias en el entorno de los servicios de infraestructura y housing.
- Se controla el ingreso y salida de equipos e información, mediante procedimientos de solicitud, registro y supervisión.
- Los espacios de alojamiento con cerramiento que separan físicamente la instalación del cliente del resto de infraestructuras.
- El centro de datos cuenta con controles de seguridad ambientales para proteger los medios de procesamiento, los recursos informáticos, como controles contra incendios, de temperatura y humedad.
- Se cuenta con un plan de continuidad del negocio que permite la protección contra desastres naturales, factores de protección contra incendio, fallas en los servicios de

soporte (energía, comunicaciones), colapso de la estructura, aniego, protección contra robo, allanamiento, y recuperación de desastres.

- Infraestructura Suelo técnico: Más de 1.600 m2 de instalaciones 400m2 de suelo técnico (reforzado, antiestático y antideslizante). Separación de clientes Jaula dedicada, rack dedicado, rack compartido.
- Soporte para antenas: Posición para antenas, soporte, mástil.
- Parámetros de control ambiental: Control de temperatura, presión atmosférica y humedad.
- Temperatura controlada: 23ºC ±2,5ºC,
- Humedad relativa: 55% ± 10%.
- Refrigeración de salas: Aire acondicionado redundante independiente en cada sala, en configuración N + 1 rotativo.
- Centro de transformación: Conexión a centro de transformación redundado de 630 Kva. Sistemas de alimentación ininterrumpida: SAIS en configuración redundante 2(N+1) con provisión de caminos múltiples de servicio al CPD.
- Grupos electrógenos: Grupos electrógenos de 500 Kva. y cuadro automático de puesta en marcha. Capacidad de repostado en caliente, autonomía ilimitada.
- Corriente continua: Grupo rectificador + baterías (triplicado)
- Control de incendios: Sistemas de detección constituidos por detectores iónicos de humos y gases de combustión. Zonas de detección controladas por central analógica microprocesada con plena autonomía de señalización, centralización de fuego y avería.
- Agente extintor FE-13 de alta presión. No conductor de la electricidad.
- Seguridad con personal Centro de operaciones (NOC) 24x7 con personal técnico propio. Equipo de seguridad 24x7 en las propias instalaciones. Equipo de seguridad armado en el perímetro del centro.
- Estación de bomberos y base de Policía a 900 metros.
- Circuito cerrado TV Total cobertura de zonas externas e internas.
- Control de accesos por lectores de tarjeta por proximidad. Registro de accesos al recinto. Sistemas de control Gestión del edificio Sistema de seguimiento que supervisa las alarmas eléctricas, mecánicas, de temperatura, de humedad, de incendios, de seguridad, de control de accesos y de apertura de racks de clientes.

9 GESTIÓN DE OPERACIONES

Los sistemas de bases de datos que se interconectan a los servidores de sellado de tiempo son protegidos mediante los siguientes controles:

- Todos los servidores tienen protección antivirus.
- La instalación y desinstalaciones de aplicaciones de software es controlada.
- Se elimina de manera segura la información sensible antes de que los equipos de la TSU sean desechados.
- Se monitorean las demandas de capacidad de memoria, procesamiento y almacenamiento.

10 GESTIÓN DE ACCESOS

Los accesos a los sistemas de la TSU son restringidos mediante controles de seguridad perimetral de redes:

- Se utilizan firewalls configurados para prevenir todos los protocolos y accesos no autorizados para la operación de la TSU
- Se utilizan sistemas IPS para inspeccionar y bloquear el ingreso de código malicioso
- Se monitorean los equipos de comunicaciones.

Se gestionan las cuentas de usuario, respecto de la generación, modificación periódica o remoción de acceso.

Los accesos a la administración de los sistemas de sellado de tiempo son asignados al personal de confianza y son retirados o modificados cuando el personal se retira de la entidad de manera definitiva o temporalmente.

Los sellos de tiempo emitidos son registrados, así como las transacciones principales de gestión de las claves. Estos registros serán auditados durante los procesos anuales de auditoría interna.

Las funciones de administración y protección de logs son separadas de las de monitoreo.

El personal es apropiadamente autenticado antes de usar aplicaciones críticas relacionadas a las actividades de sellado de tiempo.

Los accesos a utilidades del sistema están restringidos a los Administradores.

11 DESARROLLO Y MANTENIMIENTO DE SISTEMAS CONFIABLES

Lleidanet PKI S.L.U. realiza los procedimientos del ciclo de vida de software conforme al estándar a la Norma ISO/IEC 33000.

12 SEGURIDAD DEL PERSONAL

El personal de Lleidanet PKI S.L.U. deberá estar calificado respecto de conocimientos y experiencia de acuerdo con su rol.

Los roles que tienen acceso a información sensible deben ser conscientes de su responsabilidad y deben ser comprometidos contractualmente a su protección mediante convenios de confidencialidad.

Todos los empleados de Lleidanet PKI S.L.U. que participan de la administración y desarrollo de los servicios de la TSA deben recibir capacitaciones periódicas sobre tecnología, políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Las capacitaciones deben incluir los siguientes temas:

- conocimiento de tecnología de sellado de tiempo.
- conocimiento de tecnología de firma digital.
- conocimiento de mecanismos para la calibración y sincronización del reloj con la UTC.
- familiaridad con procedimientos de seguridad de personal con responsabilidades de seguridad para proteger la TSU.
- experiencia en seguridad de la información y gestión de riesgos.

Los roles de confianza de la TSU deberán ser formalmente designados por el gerente responsable de la seguridad.

Todo el personal debe firmar un convenio de confidencialidad y uso adecuado de recursos.

Asimismo, existe un proceso disciplinario en caso de incumplimiento de la normatividad de la empresa.

El personal recibe formación constante sobre las medidas de seguridad para proteger los sistemas de sellado de tiempo.

12.1 ROLES DE CONFIANZA

Todo el personal en roles de confianza deberá ser libre de conflictos de interés que puedan perjudicar la operación de la TSU. El personal no deberá tener acceso a las funciones hasta que todas las verificaciones necesarias sean completadas.

Los roles de confianza incluyen los siguientes roles:

- Administrador del Sistema
- Administrador del Servicio
- Responsable del SGSI
- Auditor Interno
- Operador ER

- Proveedor CPD
- Responsable de la Información
- Responsable de la Red

13 ADMINISTRACIÓN DE LOS SERVICIOS DE SELLADO DE TIEMPO

Los responsables de las operaciones de la TSU deberán asegurar que en el caso de eventos que puedan afectar la seguridad de los servicios de sellado de tiempo, incluyendo compromisos de la clave de la TSU o pérdidas detectadas de calibración, la información relevante sea comunicada a los suscriptores y terceros que confían.

14 RECUPERACIÓN EN CASO DE COMPROMISO DE LOS SERVICIOS DE LA TSU

El plan de recuperación de desastres deberá considerar los casos de compromiso o sospecha de compromiso de la clave privada de la TSU o pérdida de calibración del reloj, que puede afectar los sellos de tiempo emitidos.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, se deberá comunicar a todos los suscriptores y terceros que confían una descripción del hecho ocurrido.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, no se deberán emitir sellos de tiempo hasta que se hayan tomado las medidas de recuperación.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, se debe poner a disposición de los suscriptores y terceros que confían la información que permita identificar los sellos de tiempo afectados, a menos que esto viole la privacidad de los usuarios o la seguridad de los servicios de la TSU.

15 SEGUIMIENTO Y MONITOREO

Se realiza monitoreo del funcionamiento de los servidores de sellado de tiempo y de los servidores de tiempo.

- Los eventos y datos específicos de la generación de los sellos de tiempo y de la gestión del certificado de la TSU y las claves privadas serán registrados.
- Se deberá proteger la confidencialidad e integridad de los registros concernientes a la operación de los servicios de sellado de tiempo, durante todo su ciclo de vida.
- Los registros concernientes a la operación de los servicios de sellado de tiempo deberán estar disponibles si son requeridos para propósitos de proveer evidencia de la operación correcta de los servicios de sellado de tiempo para propósitos de procesos legales.
- Los registros concernientes a los servicios de sellado de tiempo deberán ser protegidos y almacenados por un periodo de tiempo de un año después de la expiración de la validez del certificado digital de la TSU para proveer la evidencia legal necesaria.
- Se deben registrar los eventos relacionados a la sincronización de los relojes de los TSU, incluyendo la información de la re-calibración o sincronización de relojes.
- Se deben registrar los eventos relacionados para detectar la perdida de la sincronización del reloj de los TSU.

16 ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD

Lleidanet PKI S.L.U. proporciona servicios de soporte de segundo nivel para la gestión de incidentes y recuperación de los sistemas de software que sustentan los servicios.

Se gestionan los incidentes relacionados a la administración de los controles de acceso físico, la provisión del suministro de energía, los controles ambientales y los de seguridad perimetral de redes y comunicaciones.

Los eventos que puedan alterar el correcto funcionamiento de los servicios de sellado de tiempo respecto de los niveles de disponibilidad establecidos y de los requerimientos de autenticidad de los clientes a los que se debe brindar el servicio, así como a la integridad de las configuraciones de los sistemas y de la información que procesan estos servicios, deben ser detectados y reportados por canales de comunicación eficientes que permitan la reacción oportuna, de acuerdo a una clasificación establecida según el impacto de los incidentes sobre los servicios y a la complejidad de su solución (estimación en latencia). Estos incidentes deben ser escalados hasta su solución tomando registro de los eventos y de las soluciones de los mismos en una base centralizada de conocimiento que permita la pronta solución de eventos similares. El problema fuente de los incidentes recurrentes debe ser investigado a fin de encontrar su solución definitiva.

17 CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

Lleidanet PKI S.L.U., como Autoridad emisora de sellos de tiempo, cumple los requerimientos establecidos en la legislación vigente.

Lleidanet PKI S.L.U. no recoge información personal de los usuarios (personas naturales) de los servicios de sellado de tiempo, a pesar de ello, Lleidanet PKI S.L.U. se rige de acuerdo al Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

Lleidanet PKI S.L.U., 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 TSA.

18 REVISIÓN, ACTUALIZACIÓN Y PUBLICACIÓN DEL PLAN

La Política de Seguridad, Política de Privacidad y la Política de Sellado de tiempo de la TSA serán revisados y actualizados al menos una vez por año.

Así mismo, se publicará en la web de Lleidanet PKI S.L.U. dicho documento para conocimiento público (https://www.indenova.com/acreditaciones/eidas/).

19 RESPONSABILIDADES

Lleidanet PKI S.L.U. asume las responsabilidades de representación de los servicios de sello de tiempo, a fin de ejecutar las garantías y cláusulas contractuales con los clientes. En tal sentido establece y garantiza el cumplimiento de los niveles de servicio y requerimientos contractuales acordados con cada cliente.

El Responsable de Seguridad de la información de Lleidanet PKI S.L.U. 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.

20 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 TSA y dentro de ella su política.