Proyecto	**Entidad de Registro o Verificación**
Título	**Política de seguridad**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Usuarios internos y externos**		
Documento	**DOC-200216.20B0516**		
Fecha aprobación	**30/04/2025**	Revisión	**2**

Firmado por: Raul Gisbert Rodas
Fecha firma: 02/05/2025 9:57:44 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 05/05/2025 9:50:15 CEST

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

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

Firmado por: JORDI GISBERT RODAS
Fecha firma: 05/05/2025 12:07:20 CEST

1 DATOS DEL DOCUMENTO

Proyecto	Entidad de Registro o Verificación
Título	Política de seguridad
Código	DOC-200216.20B0516
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	05/11/2020	Creación del documento	Indenova SL (SBS)
2	30/04/2025	Actualizar los roles de las personas que pertenecen a la comisión de seguridad de la información Actualizar los roles de confianza Actualizar a la nueva plantilla	Lleidanet PKI (CJ)

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

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 LLEIDANET PKI S.L.

6 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza LLEIDANET PKI S.L. para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos del "Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo" o también como es conocido "Reglamento eIDAS" establecida por el Parlamento Europeo.

7 DEFINICIONES Y ABREBIACIONES

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. (EC 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. L 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 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 (EC 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 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 la CPS de 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 ENTIDAD DE CERTIFICACIÓN ASOCIADA A 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

La presente política es de cumplimiento obligatorio para el personal contratado por LLEIDANET PKI S.L., proveedores y terceros que participan de las operaciones críticas de los servicios de registro descritos en la Declaración de Prácticas de Registro.

10 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ER de LLEIDANET PKI S.L. tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de sellado de tiempo, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la ER en los ámbitos legales, regulatorios y contractuales.

Los controles son definidos en base a la identificación y valoración de los activos que forman parte de las operaciones de registro, así como la identificación de amenazas y vulnerabilidades de estos activos críticos, la evaluación del impacto de los riesgos, y el tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER de LLEIDANET PKI S.L.

10.1 SEGURIDAD FÍSICA

10.1.1 Ubicación y construcción del local

La ubicación y diseño de las instalaciones de la infraestructura de los proveedores de servicios de certificación digital debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre.

10.1.2 Seguridad física del personal y el equipamiento

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de LLEIDANET PKI S.L., medios que garanticen la seguridad física de los equipos y del personal, Se deben implementar los siguientes controles:

a) Señalización de zonas seguras.
b) Provisión de extinguidores contra incendios.
c) No debe existir cableado eléctrico expuesto.
d) Uso de estabilizadores y supresores de picos.

10.1.3 Perímetros de seguridad y control de acceso físico

Las áreas de archivo de documentos en papel y archivos electrónicos, deben estar protegidas constantemente contra acceso no autorizado:

a) Deben estar en ambientes separados de las áreas públicas de registro.
b) Sólo debe ingresar personal autorizado.
c) El ingreso y salida del personal debe ser registrado.
d) Los terceros y el personal de limpieza pueden ingresar con autorización del Responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área.
e) El ingreso y salida de documentos debe ser registrada.
f) Debe estar cerrada bajo llave cuando no esté siendo usada.
g) Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes.

Las operaciones de validación y registro pueden realizarse en las instalaciones de LLEIDANET PKI S.L. o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del Operador de Registro, el cual será responsable de proteger la información proporcionada por el cliente.

10.1.4 Protección contra la exposición al agua

Las instalaciones deben estar protegidas contra exposición al agua, en particular, las áreas de archivo deben estar distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

10.1.5 Protección contra incendios

Las instalaciones deben poseer las siguientes medidas para la prevención y protección contra incendios:

a) Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de la ER de LLEIDANET PKI S.L.
b) Se debe contar con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.
c) Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Administrador del Servicio, contra acceso no autorizado.

10.1.6 Archivo de material

Los archivos se digitalizan y se almacenan en la Plataforma de modo que solo se conservan a modo de backup algunos archivos en papel en las áreas de archivo, en contenedores de protección contra fuegos. Esta doble ubicación (digitalizada y en papel) elimina riesgos asociados a una única ubicación.

El acceso a estos contenedores debe estar restringido a personal autorizado.

10.1.7 Gestión de Residuos

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

10.1.8 Copia de seguridad externa

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Administrador del Servicio, contra acceso no autorizado.

10.2 GESTIÓN DE ROLES

10.2.1 Roles de confianza

Los roles de confianza deben ser definidos de la siguiente manera:

- Administrador del Sistema
- Administrador del Servicio
- Responsable del SGSI
- Auditor Interno
- Operador ER
- Proveedor CPD
- Responsable de la Información
- Responsable de la Red

Estos roles deben ser asignados formalmente por el Administrador del Servicio de LLEIDANET PKI S.L.

La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de estas.

10.2.2 Número de personas requeridas por labor

Los cambios en los documentos normativos requieren de la revisión del Administrador del Servicio y la aprobación de la Comisión de Seguridad de la Información, dichos roles no son incompatibles y pueden ser asumidos por un mismo cargo. Una persona por rol. En el caso de no estar presente el Administrador del Servicio es el máximo y último rol responsable.

El auditor deberá ser siempre una persona independiente de las operaciones de registro.

10.2.3 Identificación y autenticación para cada rol

Los roles de confianza se deben emplear controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a los sistemas de Registro dependen de la configuración de los sistemas de cada EC y no de la ER de LLEIDANET PKI S.L.

10.2.4 Roles que requieren funciones por separado

El auditor elegido para la evaluación de Entidad de registro debe ser siempre una persona independiente de las operaciones de registro.

10.3 GESTIÓN DEL PERSONAL

10.3.1 Acuerdos de confidencialidad

Los empleados y contratistas deben ser requeridos de cumplir términos de confidencialidad y provisiones de no revelación de información confidencial o privada, así como la legislación que rige a las transacciones que se realizan bajo el marco eIDAS, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la RGPD.

Esta información debe ser entregada por escrito a sus empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al de conocimiento de toda esta información.

Esta información debe ser incorporada en todos los contratos de trabajo o servicio.

10.3.2 Cualidades y requisitos, experiencia y certificados

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de registro digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos.

Asimismo, deben tener experiencia relacionada a los temas de certificación digital.

10.3.3 Procedimiento para verificación de antecedentes

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro.

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

Para los roles de confianza que pertenecen a oficina principal o casa matriz se homologan con los controles de verificación de antecedentes ya implementados para sus operaciones.

En el caso de Operadores de registro que actúen en la ER de LLEIDANET PKI S.L., la validación de sus antecedentes se realiza de acuerdo a la legislación vigente.

10.3.4 Requisitos de capacitación

Todos los empleados de la organización que participan de los servicios de registro deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.
- Los aspectos de la CPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos con relación a sus funciones.
- Sus roles con relación al Plan de Contingencia.

- Actualización de contraseña de correos de manera permanentes.
- Actualización de contraseña de ordenadores.
- Asistir a charlas de concientización programadas por ER.

10.3.5 Frecuencia y requisitos de las re-capacitaciones

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

10.3.6 Frecuencia y secuencia de la rotación en el trabajo

No se implementará rotación de los trabajadores. De realizar rotación o contar con nuevos trabajadores, estos serán capacitados antes de realizar las actividades designadas.

10.3.7 Sanciones por acciones no autorizadas

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

Dichas sanciones deben estar establecidas en los contratos de cada empleado y/o contratista.

10.3.8 Requerimientos de los contratistas

El personal contratado para fines específicos dentro de las operaciones de la ER de LLEIDANET PKI S.L., será evaluado respecto de sus antecedentes de conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC.

10.3.9 Documentación suministrada al personal

Se debe entregar al personal la documentación necesaria para el desempeño de sus funciones:

- Una declaración de funciones y autorizaciones.
- Manuales para los equipos de software que deben de operar.
- Aspectos de la CPS, política de seguridad y otra documentación relevante en relación con sus funciones.

- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencia.

10.4 PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

10.4.1 Tipos de eventos registrados

Los sistemas de información sensible son provistos por la EC, por lo que la ER de LLEIDANET PKI S.L. sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC.

Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.

La ER de LLEIDANET PKI S.L. genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

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

10.4.2 Frecuencia del procesamiento del registro

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

10.4.3 Periodo de conservación del registro de auditorías

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro deben conservarse por un periodo de quince (15) años.

10.4.4 Protección del registro de auditoría

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.

10.4.5 Copia de seguridad del registro de auditoría

Todas las solicitudes y contratos físicos serán generados se digitalizan y adjuntan en plataforma, los originales se custodian en la caja fuerte.

Los documentos electrónicos tendrán que estar custodiados en la plataforma de ER, las cuales están protegidas contra acceso no autorizado por el Administrador del Servicio de LLEIDANET PKI S.L..

10.4.6 Auditoría

Las auditorías internas se llevarán a cabo al menos una vez al año en la ER de LLEIDANET PKI S.L.

Las evaluaciones técnicas del organismo de evaluación de la conformidad se llevarán a cabo una vez al año y cada vez que el Organismo de supervisión lo requiera.

10.4.7 Notificación al titular que causa un evento

Las notificaciones automáticas dependen de los sistemas de la EC, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

10.4.8 Valoración de vulnerabilidad

Los sistemas de registro son administrados por cada EC, por lo que la protección perimetral de redes corresponde a la infraestructura de cada EC certificada la certificación ISO 27001.

10.5 ARCHIVO

10.5.1 Protección del archivo

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos deben estar firmados de manera manuscrita y digital respectivamente para prevenir cualquier modificación.

El ingreso y salida de documentos físicos y digitales debe ser registrado para impedir la pérdida o destrucción no autorizada.

Los datos archivados deben consignar la fecha y hora, y la firma digital de la organización que genera dichos datos según la RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado.

10.5.2 Procedimiento para obtener y verificar la información del archivo

Mensualmente, la integridad del archivo debe ser verificada por la EC.

10.6 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

10.6.1 Plan de contingencias

La ER de LLEIDANET PKI S.L. mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

El plan asegura que los servicios de registro para los procesos de emisión y revocación puedan ser reasumidos dentro de un plazo máximo de 48 horas.

Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, juntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

La recuperación de los sistemas administrados por la EC, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC. En esos casos, la ER de LLEIDANET PKI S.L. informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

10.6.2 Compromiso de la clave privada

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

10.7 CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER

10.7.1 Información considerada confidencial

La ER de LLEIDANET PKI S.L. mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;

- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

10.7.2 Información que puede ser publicada

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.
- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

10.8 DERECHOS DE PROPIEDAD INTELECTUAL

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

10.9 RESPONSABILIDADES

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

10.10 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.