DECLARACIÓN DE POLÍTICAS Y PRÁCTICAS DE LOS SERVICIOS DE FIRMA ELECTRÓNICA AVANZADA
Y
CERTIFICACIÓN DE COMUNICACIONES ELECTRÓNICAS CERTIFICADAS

AES-RECA-PPS 01.00.00|

Versión 2.0

2022 – Enero – 03

LLEIDA.NET
PCiTAL · Edificio H1, 2a planta B, 25003 Lleida (SPAIN)

Control de documentación

Descripción

Este documento y sus disposiciones describen las políticas y las prácticas de Lleida Networks Serveis Telemàtics respecto a sus servicios de firma electrónica avanzada y a los aspectos técnicos del servicio de entrega certificada. En cuanto a su finalidad y contenido, la presente Política se rige por lo dispuesto en el artículo 26 y 43 del Reglamento eIDAS (UE 910/2014); en el estándar técnico definido en el ETSI EN 319 401 "General policy requirements for trusted service providers" ("Requisitos de política general para prestadores de servicios de confianza"), y en la norma ISO/IEC 29115:2013 *"Information Technology - Security Techniques - Entity Authentication Guarantee Framework" ("Tecnologías de la información - Técnicas de seguridad - Marco de Garantía de Autenticación de Entidades"),* y por otras normativas de jurisdicciones concretas incluidas en los suplementos de esta Política.

Se tienen en cuenta las directrices sobre identificación electrónica que se derivan del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Asimismo, se tienen en cuenta la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

Historial del documento

Versión	Fecha	Autor	Descripción
1	2019-10-31	MG, IM, JR, EP, ES	AES + ERDS
2	2022-01-03	BP	Adaptación a la nueva Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Clasificación y estado del documento

Clasificación del documento	
Estado	

Documentos relacionados

Descripción

Índice

1 INTRODUCCIÓN

LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A. (en lo sucesivo, Lleida.net o LLEIDA.NET) es una operadora de telecomunicaciones autorizada por las autoridades españolas y prestador cualificado de servicios de confianza que opera según lo dispuesto por el Reglamento europeo (UE) 910/2014 (conocido como Reglamento eIDAS). Ofrece servicios relacionados con la confianza en todo el mundo.

LLEIDA.NET ha recibido autorización para distintos servicios de telecomunicaciones a lo largo de su desarrollo:

- De la Comisión del Mercado de Telecomunicaciones para la prestación de servicios de transmisión de datos - proveedor de acceso a Internet (10/12/1998);
- Para servicios fijos de telefonía (11/05/2005); transmisión de datos - almacenamiento y reenvío de mensajes (23/4/2008), y
- Operador virtual - de servicios móviles totales (5/12/2008).

Actualmente, presta varios servicios de evidencias electrónicas como prestador de servicios de confianza para garantizar el valor probatorio de los documentos jurídicos digitales en internet así como servicios cualificados de entrega certificada, correo certificado, SMS certificado y otros servicios de comunicación certificada.

A este efecto, la empresa actúa como prestador cualificado de servicios de confianza bajo el nombre de "Lleida.net Prestador de Servicios de Confianza" (en lo sucesivo, LLEIDA.NETPSC) en virtud de lo dispuesto por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza cualificados (TSL) , y en el Reglamento (UE) 910/2014 (en lo sucesivo, Reglamento eIDAS) del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Se tiene en cuenta la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

La estructura y contenidos de la presente Política se han definido de acuerdo con el estándar técnico ETSI EN 319 401 (*"General Policy Requirements for Trust Service Providers"*, "Requisitos de política general para prestadores de servicios de confianza"); la ISO/IEC 29115:2013 (*"Information Technology - Security Techniques - Entity Authentication Guarantee Framework"*, "Tecnologías de la información - Técnicas de seguridad - Marco de Garantía de Autenticación de Entidades"), y por otras normativas de jurisdicciones concretas incluidas en los suplementos de esta Política.

También tiene en cuenta las directrices sobre identificación electrónica que se derivan del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas.

1.1 Perspectiva general

En esta Política se describe:

- A los participantes y sus funciones.
- Cómo se verifica la identificación del firmante y la identidad declarada en cada uno de los servicios y sus distintas modalidades.
- Cómo se genera la firma que vincula al firmante con el documento firmado.
- La gestión de las instalaciones (seguridad física, personal, auditorías, etc.).
- Los procedimientos de auditoría.
- Otros asuntos jurídicos y comerciales.

Lleida.net expedirá certificados de acreditación de los servicios de firma electrónica avanzada (incluido el consentimiento electrónico para la creación de contratos) y de las comunicaciones electrónicas certificadas.

El presente documento de Declaración de Políticas y Prácticas indica las funciones, responsabilidades y prácticas de todas las entidades implicadas en el ciclo de vida, uso, fiabilidad y gestión de las credenciales de firma electrónica y de los certificados para comunicaciones electrónicas certificadas. Las disposiciones de este documento en relación con las prácticas, niveles de servicio, responsabilidades y obligaciones vinculan a todas las partes implicadas, incluida Lleida.net, las AR (autoridades de registro) que esta designe, los suscriptores y las partes que confían. Algunas disposiciones podrían también ser de aplicación a otras entidades, como prestadores de servicios de certificación, proveedores de aplicaciones, etc.

El presente documento de Declaración de Políticas y Prácticas describe los requisitos para expedir, gestionar y utilizar las credenciales de firma electrónica y de los certificados de acreditación de comunicaciones electrónicas certificadas expedidos por Lleida.net.

Cualquier suscriptor o parte que confía de un servicio de firma electrónica o de un certificado de acreditación de comunicaciones electrónicas certificadas de Lleida.net debe consultar la Declaración de Políticas y Prácticas de Lleida.net para establecer la debida confianza.

1.2 Nombre e identificación de documentos

De acuerdo con el Reglamento eIDAS y dentro del alcance de esta Declaración de Políticas y Prácticas de los servicios de firma electrónica avanzada y de certificación de comunicaciones electrónicas certificadas, los servicios que ofrece LLEIDA.NET se definen de la siguiente forma:

Tabla 1. Identificador de objeto digital (OID) de la política

Name	Policy OID
Electronic Signature/Seal & Electronic Contract Offer and Confirmation	
Signature	1.3.6.1.4.1.52376.2.5.0
Seal	1.3.6.1.4.1.52376.2.5.1
Simple Signature	1.3.6.1.4.1.52376.2.5.0.0
Advanced signature -no certificate	1.3.6.1.4.1.52376.2.5.0.1
Advanced signature -with certificate	1.3.6.1.4.1.52376.2.5.0.2
Simple Seal	1.3.6.1.4.1.52376.2.5.1.0
Advanced seal -no certificate	1.3.6.1.4.1.52376.2.5.1.1
Advanced seal -with certificate	1.3.6.1.4.1.52376.2.5.1.2
Advanced signature- non qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.0
Advanced signature- qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.1
Advanced seal- non qualified certificate	1.3.6.1.4.1.52376.2.5.1.2.0
Advanced seal- qualified certificate	1.3.6.1.4.1.52376.2.5.1.2.1
Advanced signature- qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.0.2.1.0
Advanced signature-qualified certificate-qualified device	1.3.6.1.4.1.52376.2.5.0.2.1.1
Advanced seal- qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.1.2.1.0
Advanced seal-qualified certificate-qualified device	1.3.6.1.4.1.52376.2.5.1.2.1.1
Advanced signature on server -non qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.0.1
Advanced signature on server- with qualified certificate	1.3.6.1.4.1.52376.2.5.0.2.1.1
Advanced signature on server- with qualified certificate-nonqualified device	1.3.6.1.4.1.52376.2.5.0.2.1.0.1
Advanced signature on server- with certificate -qualified device	1.3.6.1.4.1.52376.2.5.0.2.1.1.1
Electronic Delivery	
Electronic comunication atesttations	1.3.6.1.4.1.52376.2.4.0
Registered email	1.3.6.1.4.1.52376.2.4.1
Registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2
Registered email	1.3.6.1.4.1.52376.2.4.1.0
Qualified registered email	1.3.6.1.4.1.52376.2.4.1.1
Registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2.0
Qualified registered electronic delivery (non email)	1.3.6.1.4.1.52376.2.4.2.1

El presente documento de Declaración de Políticas y Prácticas está disponible en internet, en el apartado https://lleida.net/policies.

1.3 Funciones y entidades intervinientes

Esta Política establece las reglas y prácticas generales para la prestación de servicios de firma electrónica avanzada y de acreditación de comunicaciones electrónicas certificadas por parte de Lleida.net. Estas reglas y prácticas generales son aplicables a todas las personas y entidades que intervengan en dichos servicios, incluidas las partes que sean usuarias de los servicios y las partes que confían en el servicio.

Todas las partes intervinientes deben conocer el contenido de este documento para comprender cómo se gestionan las evidencias y la acreditación y cuáles son los mecanismos que protegen la confianza en las firmas electrónicas avanzadas y en la acreditación del consentimiento de contacto electrónico, tal como las proporciona LLEIDA.NET.

Además, este documento puede ser utilizado por terceros u otras entidades independientes para comprobar, verificar y certificar que Lleida.net actúa de acuerdo con su Declaración de Políticas y Prácticas.

Para los firmantes y ordenantes (personas físicas), este documento entra en vigor y es vinculante desde el momento en que se acepta cualquier solicitud de contrato o firma y se sigue adelante con el proceso de firma. Para las entidades y ordenantes contratantes (personas jurídicas), existen unos “términos y condiciones” específicos relativos, entre otras cuestiones, a la identificación de los firmantes y para la identificación del destinatario de la comunicación electrónica.

En cuanto a las partes que confían, este documento pasa a ser vinculante simplemente al enviar una solicitud de verificación de firma de un documento expedido por Lleida.net. El acuerdo de suscriptor pierde el consentimiento de la parte usuaria en relación con la aceptación de las condiciones expuestas en este documento.

1.3.1 Validador de identidad o autoridad de registro

El validador de la identidad ejerce las mismas funciones que una autoridad de registro (AR) en el marco de un servicio de expedición de certificados. Por lo tanto, al ser un término creado dentro del sector de los servicios de confianza, el encargado de verificar una identidad se denominará en este documento "autoridad de registro" o "AR".

LLEIDA.NET, como prestador de servicios de confianza, puede ofrecer su servicio de firma electrónica avanzada y de comunicación electrónica certificada directamente, mediante su propio servicio de autoridad de registro, para validar la identidad declarada por el firmante o el destinatario; o bien, en algunos casos, puede llevar a cabo la validación de la identidad la entidad que ofrece el contrato o documento a firmar, a través de un servicio de firma electrónica avanzada, o bien la entidad que envía una comunicación electrónica certificada. En ambos casos, el término "autoridad de registro" o "AR" describe el papel y los procedimientos para identificar debidamente al firmante o destinatario.

Dicho de otro modo, las funciones de la AR pueden ser realizadas por la entidad que ofrece al firmante el documento a firmar, mediante el servicio de firma electrónica avanzada de LLEIDA.NET, o bien la que envía una comunicación electrónica certificada. Esta entidad puede ser denominada "oferente" u "ordenante".

En el caso de instituciones financieras y otras entidades que tengan que cumplir con la normativa de prevención del blanqueo de capitales y de financiación del terrorismo (PBC-FT), LLEIDA.NET entiende que actuarán de conformidad con las prácticas de diligencia debida y los procedimientos del buen conocimiento de la clientela ("KYC" o "know your customer") para identificar y verificar la identidad de sus clientes.

El organismo de evaluación de la Conformidad Trust Conformity Assessment Body S.L.U. (TCAB) ha evaluado el Servicio de Firma Electrónica Avanzada Remota prestado por Lleidanetworks Serveis Telemàtics SA de acuerdo con la normativa y normas técnicas aplicables y ha comprobado que el servicio prestado cumple con el artículo 26 del Reglamento EIDAS [Reglamento (UE) No 910/2014).

La acreditación muestra que el servicio de Firma Electrónica Avanzada Remota, prestado por Lleidanetworks Serveis Telemàtics SA, cumple con los estándares ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 403 v2.2.2 y la Commission Implementing Regulation (EU) 2015/1502

Asimismo el organismo de evaluación de la Conformidad Trust Conformity Assessment Body S.L.U. (TCAB) ha evaluado el Servicio de Identificación Remota restado por Lleidanetworks Serveis Telemàtics SA de acuerdo con la normativa y normas técnicas aplicables y ha comprobado que el servicio prestado cumple con los requisitos y normas establecidos por el Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior (eIDAS) y cumple todos los requisitos pertinentes definidos en las normas y el reglamento: Reglamento de Ejecución (UE) 2015/1502 de la Comisión, ETSI EN 319401, ETSI 319 411-1, Ley Nacional 10/2010, Real Decreto 304/2014 y autorización de video-identificación española publicada por SEPBLAC.

Las entidades que ejerzan como AR quedan obligadas por esta Declaración de Políticas y Prácticas, junto con la relación contractual que establezcan con Lleida.net.

Cualquier AR está sujeta, entre otras, a las siguientes obligaciones:

- Identificar y autenticar a los firmantes y ordenantes.
- Establecer una relación contractual con los firmantes o con las entidades a las que representen dichos firmantes, y con los ordenantes o las entidades a las que representen esos ordenantes.
- Iniciar el procedimiento de firma electrónica avanzada una vez que se haya validado la identidad del firmante, a través de los medios electrónicos ofrecidos por el servicio de firma electrónica avanzada de LLEIDA.NET.
- Iniciar la comunicación electrónica certificada una vez que se haya validado la identidad del ordenante, a través de los medios electrónicos ofrecidos por el servicio de acreditación de comunicaciones electrónicas certificadas de LLEIDA.NET.
- Registrar, conservar, archivar y custodiar cualquier documentación relevante relacionada con la identidad del firmante u ordenante por tanto tiempo como lo estipule la normativa sobre PBC-FT.
- Cumplir con las normativas aplicables de protección de datos personales.
- Proporcionar cualquier información que requiera Lleida.net en relación con los procedimientos de validación de identidad en cualquier momento, especialmente durante la evaluación anual de cumplimiento de la Declaración de Políticas y Prácticas.

- Autorizar a Lleida.net a realizar y gestionar la generación y conservación de entregas electrónicas y registros electrónicos en nombre de la AR y a representar a la AR en relación con la generación y custodia de dichas entregas electrónicas y registros electrónicos.

Según las normativas de los servicios de confianza, los documentos relacionados con la validación de la identidad se archivarán durante 15 años excepto en los casos en los que las normativas locales aplicables ordenen un periodo distinto.

Las AR que ejerzan como tal en el servicio de firma electrónica avanzada y de acreditación de comunicaciones electrónicas certificadas de Lleida.net, están obligadas al cumplimiento de esta Declaración de Políticas y Prácticas, así como a superar cualquier evaluación de cumplimiento de la Declaración de Políticas y Prácticas que lleve a cabo Lleida.net u otro organismo de evaluación de la conformidad que Lleida.net designe.

1.3.2 Proveedor de testigos digitales y de acreditaciones de comunicaciones electrónicas:

Función ejercida por LLEIDA.NET como tercero de confianza que acredita quiénes son los participantes en una comunicación de documentos o contenidos o en una firma, así como el contenido de los documentos firmados, junto con otras evidencias electrónicas. Esta acreditación incluye información importante como las direcciones IP, las direcciones electrónicas, los números de teléfono móvil, la localización geográfica y la fecha, así como evidencias de que los procedimientos subyacentes cumplen con los requisitos definidos en los artículos 26 y 43 del Reglamento eIDAS (UE) u otros requisitos nacionales relevantes.

1.3.3 Entidad oferente u ordenante

Entidad que ofrece el contrato o documento a firmar mediante el servicio de firma electrónica avanzada de LLEIDA.NET, o que envía una comunicación electrónica que será acreditada mediante el servicio de acreditación de comunicación electrónica certificada de Lleida.net. En algunos casos, la misma entidad puede también realizar las funciones de AR identificando al firmante o al destinatario antes de la firma del contrato o del procedimiento de entrega de la comunicación electrónica.

1.3.4 Firmante

Persona física que firma un documento mediante el servicio de firma electrónica avanzada de LLEIDA.NET. Se trata habitualmente de la persona que expresa el consentimiento a las cláusulas de un documento y que completa la formalización del contrato ofrecido por el ordenante.

1.3.5 Destinatario

Persona física o jurídica a la que se envía la comunicación electrónica certificada mediante el servicio de acreditación de comunicación electrónica certificada de Lleida.net. Por lo general, es identificada por el ordenante a través de una dirección electrónica, un número de teléfono móvil o un certificado digital, y firma un documento mediante el servicio de firma electrónica avanzada de LLEIDA.NET.

1.3.6 Parte que confía

Persona o entidad que comprende y acepta la certificación de Lleida.net como prueba de la formalización de un contrato, de la firma de un documento o de una entrega electrónica certificada, mediante su servicio de firma electrónica avanzada o su servicio de acreditación de entregas electrónicas certificadas.

Las partes que confían deben conocer y cumplir las garantías, límites y responsabilidades descritas en esta Política.

1.3.7 Autoridad de verificación de AR

Función ejercida por Lleida.net a la hora de verificar la identidad de una AR, registrarla y proporcionarle las credenciales para que actúe como AR.

Esta función puede delegarse a una autoridad delegada de verificación de AR.

1.3.8 Autoridad delegada de verificación de AR

Función ejercida por algunos socios comerciales de Lleida.net y que les permite realizar, en nombre de Lleida.net, las funciones de una autoridad de verificación de AR.

Esta función no se puede delegar, externalizar o subcontratar y está sujeta a unos términos y condiciones contractuales específicos acordados entre Lleida.net y su socio comercial.

1.4 Administración de políticas

La Autoridad de Gestión de Políticas de Lleida.net es la que gestiona esta Declaración de Políticas y Prácticas. Lleida.net registra e interpreta esta Declaración de Políticas y Prácticas, y procura que se cumplan sus procedimientos.

1.4.1 Ámbito

Lleida.net podrá realizar revisiones y actualizaciones de sus políticas según lo crea conveniente o si resulta necesario en función de las circunstancias. Dichas actualizaciones serán vinculantes para todas las credenciales expedidas o que se expidan inmediatamente después de la fecha de publicación de la versión actualizada de la Declaración de Políticas y Prácticas.

Independientemente de las disposiciones sobre cambios en la Declaración de Políticas y Prácticas, y en el supuesto de que Lleida.net suspendiera sus actividades, este documento seguirá siendo válido durante un periodo de tiempo indefinido.

La invalidez de una o más disposiciones de esta Declaración de Políticas y Prácticas no afectará en modo alguno al resto del documento y, en ese caso, se actuará como si dichas disposiciones no se hubieran incluido en ella.

1.4.2 Autoridad de Gestión de Políticas

Las nuevas versiones y las actualizaciones publicitadas de las políticas de Lleida.net reciben la aprobación de la Autoridad de Gestión de Políticas de Lleida.net. Esta autoridad, en su actual estructura organizativa, consta de los miembros que se indican a continuación:

- Comité Directivo de la ISO 27001 de Lleida.net
- Comités de aprobación, según se definen en la ISO 27001 de Lleida.net

Solo la Autoridad de Gestión de Políticas tiene la capacidad de aprobar la Declaración de Políticas y Prácticas de Lleida.net. Dicha aprobación debe quedar registrada de forma explícita.

1.4.3 Cambios

Después de que la Autoridad de Gestión de Políticas de Lleida.net apruebe la actualización de una política, esa Declaración de Políticas y Prácticas se publica en el repositorio online de Lleida.net identificado en el apartado “Nombre e identificación de documentos”.

La versión actualizada es vinculante para todos los suscriptores actuales y futuros a no ser que se reciba una notificación de un suscriptor en un plazo de 30 días tras la publicación de la Declaración de Políticas y Prácticas. Pasado dicho periodo, la versión actualizada de la Declaración de Políticas y Prácticas resulta vinculante para todas las partes, incluidos los suscriptores y partes que confían, en relación con las credenciales de firma electrónica avanzada y los certificados de acreditación de comunicaciones electrónicas certificadas que hayan sido expedidos bajo la versión anterior de la Declaración de Políticas y Prácticas de Lleida.net.

Se considerará que ha habido un cambio de versión cuando, a criterio de la Autoridad de Gestión de Políticas de Lleida.net, los cambios puedan afectar a la aceptabilidad de los servicios de

Lleida.net. Si no es el caso, la nueva redacción de la misma versión se considerará únicamente como una modificación menor.

1.4.4 Gestión de versiones e indicación de cambios

Los cambios se indicarán mediante un nuevo número de versión de la Declaración de Políticas y Prácticas.

Las nuevas versiones se señalarán con un número entero seguido de un decimal que será cero.

Los cambios menores se señalarán mediante un número decimal mayor que cero. En estos cambios menores se incluyen, entre otros:

- correcciones de texto menores
- cambios en los datos de contacto.

1.4.5 Publicación

La Declaración de Políticas y Prácticas de Lleida.net se publicará inmediatamente tras su aprobación inicial y, según corresponda, tras cada modificación. La dirección web (URL) para su publicación se encuentra en el apartado “Nombre e identificación de documentos”.

1.4.6 Contacto

Prestador de servicios	LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A.
Dirección	PCiTAL, Edificio H1, 2a planta B, 25003, Lleida (SPAIN)
Dirección electrónica	compliance@lleida.net
Teléfono	(+34) 973 282 300

1.5 Definiciones, acrónimos y referencias

1.5.1 Definiciones

- «identificación electrónica», el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;
- «medios de identificación electrónica», una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea;
- «datos de identificación de la persona», un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica;
- «autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico;
- «parte usuaria», la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza;
- «organismo del sector público», las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad;
- «organismo de Derecho público», el definido en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo (1);
- «firmante», una persona física que crea una firma electrónica;
- «firma electrónica», los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar;
- «firma electrónica avanzada», la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento UE 910/2014 (eIDAS);
- «firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica;
- «datos de creación de la firma electrónica», los datos únicos que utiliza el firmante para crear una firma electrónica;
- «certificado de firma electrónica», una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona;
- «certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE 910/2014 (eIDAS);
- «servicio de confianza», el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
b) la creación, verificación y validación de certificados para la autenticación de sitios web, o
c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

- «servicio de confianza cualificado», un servicio de confianza que cumple los requisitos aplicables establecidos en el presente Reglamento;
- «sistema de identificación electrónica», un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica;
- «organismo de evaluación de conformidad», un organismo definido en el punto 13 del artículo 2 del Reglamento (CE) no 765/2008 cuya competencia para realizar una evaluación de conformidad de un prestador cualificado de servicios de confianza y de los servicios de confianza cualificados que este presta esté acreditada en virtud de dicho Reglamento;
- «prestador de servicios de confianza», una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas;
- «prestador cualificado de servicios de confianza», un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación;
- «producto», un equipo o programa informático, o los componentes pertinentes del mismo, destinado a ser utilizado para la prestación de servicios de confianza;
- «dispositivo de creación de firma electrónica», un equipo o programa informático configurado que se utiliza para crear una firma electrónica;
- «dispositivo cualificado de creación de firma electrónica», un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II;
- «creador de un sello», una persona jurídica que crea un sello electrónico;
- «sello electrónico», datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos;
- «sello electrónico avanzado», un sello electrónico que cumple los requisitos contemplados en el artículo 36 del Reglamento UE 910/2014 (eIDAS);
- «sello electrónico cualificado», un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico;
- «datos de creación del sello electrónico», los datos únicos que utiliza el creador del sello electrónico para crearlo;
- «certificado de sello electrónico», una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona;
- «certificado cualificado de sello electrónico», un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que

cumple los requisitos establecidos en el anexo III del Reglamento UE 910/2014 (eIDAS);

- «dispositivo de creación de sello electrónico», un equipo o programa informático configurado que se utiliza para crear un sello electrónico;
- «dispositivo cualificado de creación de sello electrónico», un dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II;
- «sello de tiempo electrónico», datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;
- «sello cualificado de tiempo electrónico», un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del Reglamento UE 910/2014 (eIDAS);
- «documento electrónico», todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual;
- «servicio de entrega electrónica certificada», un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada;
- «servicio cualificado de entrega electrónica certificada», un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44 del Reglamento UE 910/2014 (eIDAS);
- «certificado de autenticación de sitio web», una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado;
- «certificado cualificado de autenticación de sitio web», un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV del Reglamento UE 910/2014 (eIDAS);
- «datos de validación», los datos utilizados para validar una firma electrónica o un sello electrónico;
- «validación», el proceso de verificar y confirmar la validez de una firma o sello electrónicos.

1.5.2 Acrónimos

- AR: autoridad de registro
- FEA: firma electrónica avanzada
- DP: Declaración de Prácticas
- IETF: Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force)
- ISO: Organización Internacional de Normalización (International Organization for Standardization)
- ITU: Unión Internacional de Telecomunicaciones (International Telecommunications Union)
- RFC: "Request for Comments" (publicaciones del IETF)
- SSCD: dispositivo seguro de creación de firma (Secure Signature Creation Device)

1.5.3 Referencias jurídicas

Reglamentos europeos

- 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.
- Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Normativa técnica internacional

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ("Firmas electrónicas e infraestructuras (ESI); Requisitos de política general para prestadores de servicios de confianza")
- ISO/IEC 29115:2013 “Information Technology - Security Techniques - Entity Authentication Guarantee Framework” (“Tecnologías de la información - Técnicas de seguridad - Marco de Garantía de Autenticación de Entidades”; (ITU X.1254: Entity authentication assurance framework).

Normativa nacional española

- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Normativa nacional de Sudáfrica

- Ley de Comunicaciones Electrónicas n.º 25 de 2002

- Ley de Comunicaciones y Transacciones Electrónicas n.º 36 de 2005
- Ley de Crédito Nacional n.º 35 de 2005
- Protection of Personal Information Act (POPI Act)

Normativa de los Emiratos Árabes Unidos

- Ley Federal n.º 1 de 2006 sobre comercio electrónico y transacciones electrónicas
- Ley Federal n.º 10 de 1992 sobre pruebas en transacciones civiles y comerciales (modificada por la Ley Federal n.º 36 de 2006)
- Ley Federal n.º 11 de 1992 de emisión de la Ley de Procedimiento Civil
- Ley Federal n.º (5) de 2017 sobre el uso de las tecnologías de la comunicación remotas en procedimientos penales
- Resolución Ministerial n.º (259) de 2019 sobre el Manual de procedimientos de regulación de litigios mediante el uso de tecnologías de la comunicación electrónicas y remotas en procedimientos penales
- Decreto-ley Federal n.º 20 de 2018 sobre prevención del blanqueo de capitales y lucha contra la financiación del terrorismo y financiación de organizaciones ilegales
- Decisión Ministerial n.º 10 de 2019 sobre la implementación del Decreto-ley n.º 20 de 2018 sobre prevención del blanqueo de capitales y lucha contra la financiación del terrorismo y financiación de organizaciones ilegales
- Resolución del Gabinete de los EAU 57/2018 sobre el Reglamento Ejecutivo de la Ley de Procedimiento Civil n.º 11 de 1992
- Resolución Ministerial de los EAU n.º (259) y (260) de 2019 sobre el Manual de procedimientos de regulación de litigios mediante el uso de tecnologías de la comunicación electrónicas y remotas en procedimientos penales y procedimientos civiles, respectivamente
- El Decreto-Ley Federal No.45 de 2021 en materia de Protección de Datos Personales (“PDPL”)
- El Decreto-Ley Federal de los EAU n. ° 44 de 2021 de creación de la Oficina de Datos de los UAE

Normativa del Reino de Arabia Saudita

- Decisión del Consejo de Ministros n.º 80 de 7/3/1428H, aprobada por el Real Decreto n.º M/18 de 8/3/1428H sobre transacciones electrónicas

Normativa del Líbano

- Ley n.º 81 de 2018 relativa a las transacciones electrónicas y los datos personales

Normativa del Reino de Baréin

- Decreto Legislativo n.º 54 de 2018 de promulgación de la Ley de Comunicaciones y Transacciones Electrónicas.

Normativa de Kuwait

- Ley 20 de 2014 sobre Transacciones Electrónicas

Normativa de la República Islámica de Irán

- Ley del Comercio Electrónico de la Asamblea Consultiva Islámica de 17/10/1382, ratificada por el Consejo Guardián de la Constitución el 24/10/1382

Sultanato de Omán

- Decreto del Sultán 69/2008, Ley de Transacciones Electrónicas

Normativa de India

- Ley de Tecnologías de la Información del 2000
- Enmiendas a la Ley India de Pruebas de 1872, el Código Penal indio de 1860 y la Ley de Pruebas del Registro Bancario de 1891 para respaldar la admisibilidad de las pruebas digitales como pruebas documentales

2 UTILIZACIÓN DE LAS CREDENCIALES

2.1 Usos permitidos/adecuados de las credenciales de firma electrónica

Firma electrónica: el objeto principal de las credenciales de firma electrónica de Lleida.net es garantizar que actúan como factor para probar la identidad declarada del firmante, además de como garantía de que esas credenciales solo pueden utilizarse bajo el control exclusivo del firmante y como voluntad explícita de ejecutar la firma por parte del titular de las credenciales.

Las credenciales de firma electrónica también garantizan que la firma generada está vinculada de manera única al documento o a los contenidos que se firman.

Autenticación de usuarios: las credenciales de firma electrónica de Lleida.net pueden utilizarse para transacciones concretas de autenticación electrónica que operan con sitios web de acceso u otros contenidos en línea. La función de autenticación de las credenciales de firma electrónica de Lleida.net puede determinarse en cualquier contexto de transacción con el fin de autenticar al suscriptor usuario final de un servicio de Lleida.net Service. Las credenciales de firma electrónica de Lleida.net son adecuadas para la autenticación de usuarios.

2.2 Usos adecuados/permitidos de las credenciales del servicio de certificación de comunicaciones electrónicas certificadas

Envío de comunicaciones electrónicas certificadas: el objetivo principal de las credenciales del servicio de certificación de comunicaciones electrónicas certificadas de Lleida.net es garantizar que actúan como factor de identidad del remitente, además de garantizar que dichas credenciales pueden utilizarse únicamente bajo el control exclusivo del ordenante y como voluntad explícita de realizar una comunicación electrónica certificada por parte del titular de las credenciales.

El uso más adecuado del servicio de certificación de comunicaciones electrónicas certificadas es la generación de pruebas y evidencias documentales que demuestren el envío, por parte de Lleida.net o un tercero, y la recepción, por los correspondientes destinatarios, de una determinada comunicación electrónica, así como el momento en el que ambas acciones han tenido lugar, el contenido de la comunicación y, si corresponde, el acceso a la documentación adjunta o su descarga, con el objetivo principal de que pueda utilizarse esa información en contextos jurídicos.

Autenticación de usuarios: las credenciales del servicio de certificación de comunicaciones electrónicas certificadas de Lleida.net pueden utilizarse para transacciones concretas de autenticación electrónica que operen con sitios web de acceso u otros contenidos en línea. La función de autenticación de las credenciales de firma electrónica de Lleida.net puede determinarse en cualquier contexto de transacción con el fin de autenticar al suscriptor usuario final de un servicio de Lleida.net o la identidad del destinatario de una comunicación electrónica certificada. Las credenciales de firma electrónica de Lleida.net son adecuadas para la autenticación de usuarios.

3 PROCEDIMIENTO RELATIVO A LA AUTORIDAD DE VERIFICACIÓN DE AR

3.1 Quién puede realizar el registro y procedimiento de verificación de AR

Solo Lleida.net, como autoridad de verificación de AR, o bien los socios comerciales de Lleida.net que hayan sido designados, mediante una relación contractual con Lleida.net, como autoridades delegadas de verificación de AR, pueden efectuar la verificación y el registro de la identidad de una AR.

3.2 Verificación de la identidad de una AR (persona jurídica)

Una autoridad de verificación de AR o una autoridad delegada de verificación de AR identificará a la AR y formalizará una relación contractual válida con dicha AR en la que se definan las funciones, obligaciones y responsabilidades de la AR, antes de registrar a dicha AR.

El nivel de seguridad exigido para las pruebas y la verificación de la identidad de una AR es el que se describe en el apartado 2.1.3 del Anexo del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, como “nivel de seguridad sustancial”, aunque se recomienda utilizar el nivel recogido en el mismo apartado como “nivel de seguridad alto”.

3.3 Vinculación de la verificación de la identidad entre una AR (persona jurídica), sus representantes (personas físicas) y la expedición de las credenciales de la AR.

Una persona física será siempre la “representante” de la AR.

Esta representante es la que, una vez que se haya verificado su identidad como representante válida de la AR, recibirá las credenciales de AR y podrá delegar el ejercicio de la vinculación a otras personas físicas de su propia AR, las cuales también recibirán sus respectivas credenciales de AR.

La vinculación debe realizarse según lo descrito en el apartado 2.1.4 del Anexo del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, como “nivel de seguridad sustancial”, aunque se recomienda utilizar el nivel recogido en el mismo apartado como “nivel de seguridad alto”.

4 PROCEDIMIENTO DE FIRMA AVANZADA

4.1 Identificación de firmantes

La AR identificará a los firmantes antes de iniciar el procedimiento de firma.

El conjunto mínimo de datos de identificación necesarios se describe en el artículo 11 y en los Anexos del Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n.º 910/2014.

El detalle de las obligaciones de la AR para la verificación de la identidad de los firmantes se establece en una relación contractual entre la AR y Lleida.net (como autoridad de verificación de identidad de AR) o entre la AR y una autoridad delegada por Lleida.net para la verificación de identidad de AR.

4.2 Vinculación del firmante al documento firmado

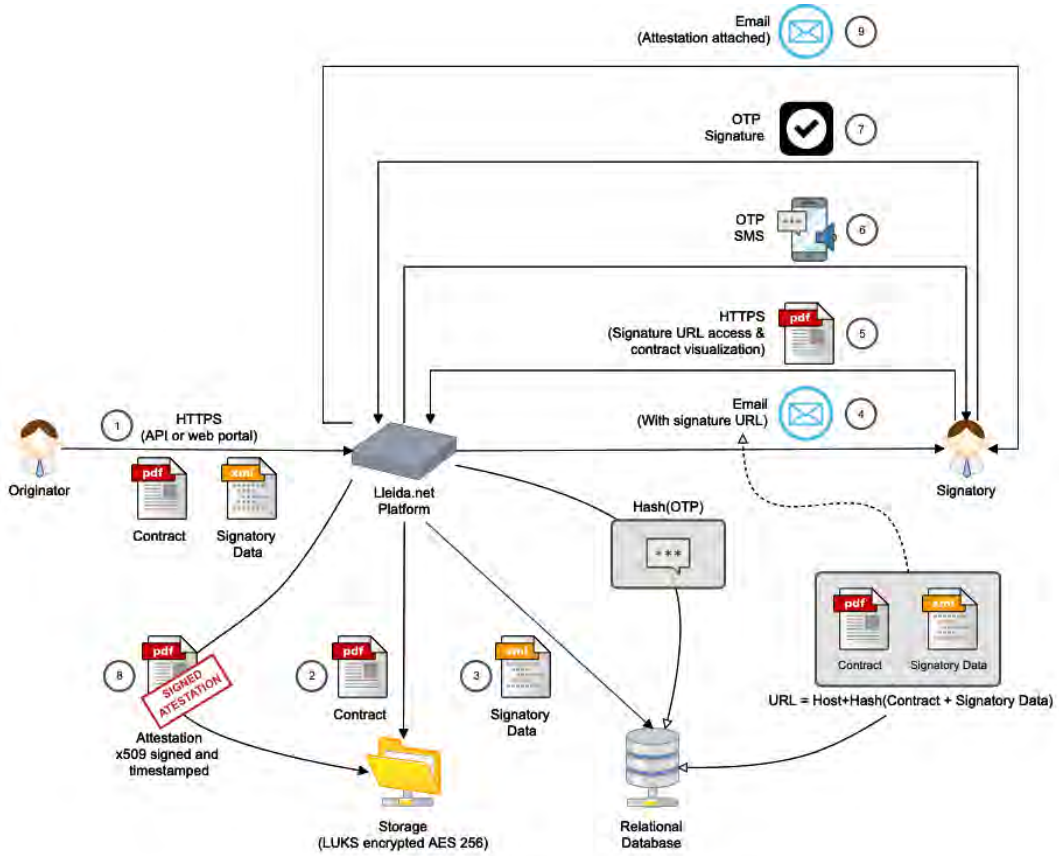
El ordenante utiliza medios electrónicos para proporcionar a LLEIDA.NET el contenido del contrato y los pertinentes identificadores de contacto electrónico, como el MSISDN (número de teléfono móvil) y/o la dirección electrónica, recopilados en el proceso de identificación.

Una funcionalidad de seguridad separa la generación de los datos de creación de una firma con OTP (contraseña de un solo uso), al mismo tiempo que se envía al firmante el mensaje que contiene la URL que permite iniciar el procedimiento de firma.

El código OTP no se almacena como texto normal en ningún momento antes de que el signatario lo utilice para expresar su consentimiento introduciendo el código en la forma presentada en el punto final de la firma, produciendo así la firma electrónica, de manera que la OTP queda bajo el control exclusivo del firmante. Cuando el sistema de Lleida.net genera la OTP, se guarda un hash de la OTP. Cuando el firmante introduce la OTP, se calcula su hash y se compara con el hash almacenado en el sistema de Lleida.net.

Una vez generada la firma, los datos de creación de la firma OTP se almacenarán en texto normal en la acreditación, como prueba para que el firmante reconozca la firma y como evidencia jurídica para el ordenante y las partes que confían.

El algoritmo utilizado para generar el hash de la página de aterrizaje (identificación única de URL del punto final del servicio que gestiona la firma avanzada) tiene en cuenta el valor del hash de los distintos documentos que van a firmarse así como los datos identificadores del firmante, lo que hace que los datos de la firma sean únicos y garantiza la integridad de los datos que van a validarse, así como la vinculación del documento con el firmante.



El procedimiento de inicio de firma de Lleida.net validará y garantizará que todos los datos recibidos tengan el formato correcto y autorizará la operación, procediendo a guardar los documentos en un almacenamiento cifrado y en una base de datos.

Durante la operación de almacenamiento de los documentos electrónicos, se calculará su valor de hash (sin los metadatos del certificado en PDF, para ser compatible con una firma biométrica manuscrita, otro servicio de Lleida.net) y se guardará en una tabla, junto con el resto de datos relevantes que identifican de forma única el documento.

La URL del servicio de firma incluirá una dirección de dominio con un prefijo que identificará el servicio de Lleida.net (por ejemplo, https://sign.clickandsign.eu/h/) y una parte calculada para identificar al firmante y el documento a firmar: esta parte única, denominada aquí “landing_hash”, se calculará a partir de los datos personales del firmante recibidos por el servicio de firma de Lleida.net, y el valor del hash del documento o documentos.

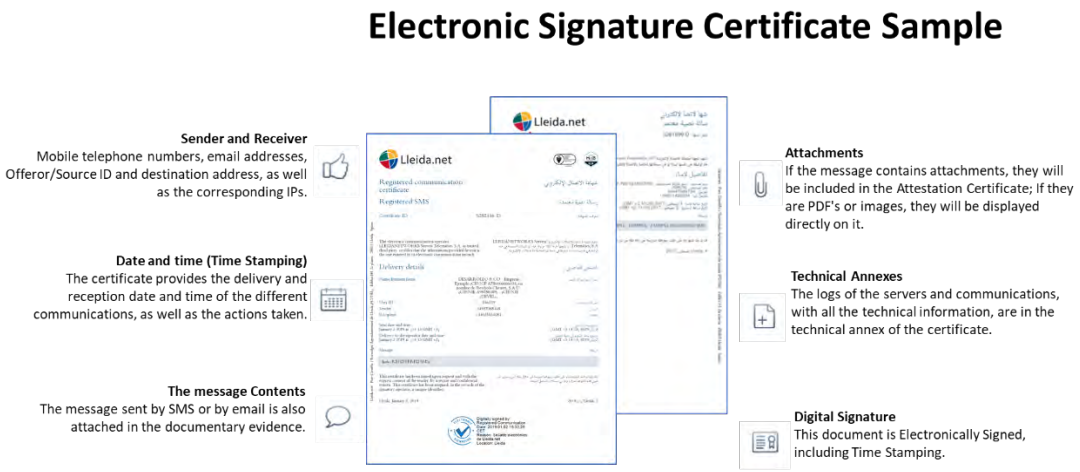
La pantalla del servicio de firma que aparece cuando se accede a la URL muestra un mensaje de descargo de responsabilidad que indica que la firma se aplicará a todos los documentos mostrados en la página de aterrizaje del servicio de firma. Esta pantalla también incluye información sobre los términos y condiciones del propio servicio de firma avanzada y de los aspectos destacados del documento subyacente que va a firmarse y que son relevantes para la formalización del consentimiento.

El “landing_hash” se calcula mediante un algoritmo SHA256 con los datos siguientes:

- Se calculará un document_hash para cada documento a firmar. Cada document_hash estará relacionado con un identificador único de los ficheros de la tabla.
- Una cadena formada por el conjunto de datos asociado al firmante en formato de cadena JSON. Suele incluir el número de teléfono, la dirección electrónica, el nombre y apellido, el documento de identidad, etc., entre otros datos. El ordenante/oferente es quien proporciona estos datos en el momento de iniciar el proceso de solicitud de firma y será responsabilidad suya, como AR, vincularlos a la identificación del firmante.
- contract_id: identificador único del oferente que identifica el proceso de firma.
- La fecha de registro de la solicitud para iniciar el proceso de firma en formato de sello de tiempo UNIX.
- Identificador único del firmante, signatory_id.
- Identificador único de la multifirma, signature_id. Identifica de forma única un proceso de firma (puede haber varios firmantes en el mismo proceso de firma).

4.3 Finalización de la firma del documento

Una vez firmado el documento, el firmante (mediante SMS o mensaje de correo electrónico) y el ordenante/oferente (por medios electrónicos que permitan la comunicación entre el solicitante y LLEIDA.NET) reciben la copia del certificado de acreditación (por correo electrónico) o una URL que dirija al certificado de acreditación de la firma, que incluye todas las evidencias electrónicas y un sello y una marca de tiempo electrónicos realizados por LLEIDA.NET, así como un número de identificación único del certificado de acreditación.



4.4 Recomendaciones operativas

Los certificados de acreditación de firma electrónica avanzada de Lleida.net llevan un sello y una marca de tiempo que se calcula mediante el hash del documento y se cifra con una clave privada asociada a un certificado RSA X.509 versión 3. LLEIDA.NET posee un certificado cualificado de persona jurídica expedido por un prestador cualificado de la UE de servicios de firma electrónica y también podría utilizar a otros prestadores de servicios de certificación válidos en otros países y jurisdicciones si fuera necesario.

Todas las partes que confían en los certificados de acreditación de LLEIDA.NET deben verificar que llevan incluido un sello electrónico y que son válidos según las normas de validación, lo que incluye la verificación de la cadena de confianza, las Listas de servicios de confianza y servicios de validación como OCSP o CRL.

5 PROCEDIMIENTOS DE CERTIFICACIÓN DE ENTREGA ELECTRÓNICA CERTIFICADA

5.1 Identificación del destinatario

La AR identificará al destinatario antes de iniciar el procedimiento de certificación de una comunicación electrónica certificada.

Los datos mínimos de identificación necesarios son la dirección electrónica o el teléfono móvil del destinatario, que deberán vincularse a la persona física o jurídica identificada como destinatario por la AR.

5.2 Autorización a Lleida.net por parte de la AR o el ordenante

El ordenante de una comunicación electrónica a través del servicio de certificación de comunicaciones electrónicas certificadas de Lleida.net concede a Lleida.net autorización plena para entregar, en nombre del ordenante, el mensaje de datos al destinatario indicado por el ordenante, así como para generar y mantener certificados de acreditación y registros certificados y firmados electrónicamente de dicha comunicación electrónica, así como para enviar la comunicación a los números de MSISDN (teléfono móvil) o direcciones electrónicas indicadas por el ordenante y recopiladas durante el proceso de identificación del destinatario.

Esta autorización es otorgada por el ordenante simplemente mediante el uso del servicio de certificación de comunicaciones electrónicas certificadas de Lleida.net en cualquier de sus formas (correo electrónico certificado, SMS certificado o entrega electrónica por internet - Openum).

5.3 Envío y recepción de comunicaciones electrónicas

Lleida.net considera que una comunicación o un mensaje de datos se ha enviado cuando el mensaje ha salido del último sistema controlado por el ordenante del mensaje o del último sistema controlado por Lleida.net, en caso de que Lleida.net realice las tareas de comunicación y registro electrónico en nombre del ordenante del mensaje de datos.

Lleida.net considera que una comunicación o mensaje de datos ha sido recibido por el destinatario cuando ese mensaje ha sido recibido en el primer sistema controlado por el destinatario (incluido el terminal del teléfono móvil o el primer MTA del destinatario); en los casos en los que se utiliza un servidor o sistema web de Lleida.net para la entrega de una comunicación electrónica web, consideramos que el mensaje se ha recibido cuando el destinatario accede al mensaje de datos o lo descarga del sistema o servidor web de Lleida.net.

5.4 Utilización del servicio de certificación de comunicaciones electrónicas certificadas

El ordenante utiliza medios electrónicos para proporcionar a LLEIDA.NET el contenido del contrato y los pertinentes identificadores de contacto electrónico, como el MSISDN (número de teléfono móvil) o la dirección electrónica, recopilados en el proceso de identificación.

Lleida.net pondrá a disposición del ordenante varios mecanismos para procesar las solicitudes para que Lleida.net realice la comunicación electrónica certificada que desea el ordenante y para que acredite esa comunicación, genere los registros electrónicos que correspondan a la comunicación, mantenga esos registros disponibles para consultas futuras, y expida los pertinentes certificados de acreditación de la comunicación electrónica certificada.

Comunicación SMS certificada: Lleida.net pondrá a disposición del ordenante una interfaz web y, si corresponde, las pertinentes API del servicio, de forma que el ordenante podrá crear un mensaje, indicar un destinatario en forma de MSISDN (número de teléfono móvil) y solicitar que Lleida.net inicie el envío del mensaje de SMS certificado en nombre del ordenante.

Lleida.net SMSC (el centro de mensajes SMS), conectado directa o indirectamente a redes móviles de operadores de telecomunicaciones, enviará el mensaje al destinatario indicado y controlará y guardará las evidencias del contenido del mensaje, la fecha y hora de envío y el destinatario.

El operador de telecomunicaciones que proporcione el servicio de SMS al destinatario (servicios de terminación de SMS) procesará la solicitud de entrega del mensaje y proporcionará a Lleida.net SMSC los datos de la entrega en el terminal del destinatario (teléfono móvil), tanto si es una entrega satisfactoria como fallida, con la fecha y la hora de la entrega.

Los sistemas de Lleida.net registrarán la respuesta del proveedor de servicios del destinatario.

Lleida.net firmará electrónicamente, mediante un certificado cualificado tipo eIDAS u otro certificado X.509 válido en otras jurisdicciones ("certificado de acreditación de SMS certificado") que identifique los siguientes elementos:

- El identificador único de la transacción de la comunicación certificada
- El ordenante del mensaje de SMS de acuerdo con los registros de verificación de la identidad de la AR
- La fecha y hora de envío del mensaje de SMS
- El MSISDN (número de teléfono móvil) del destinatario
- La fecha y hora de la recepción del mensaje en el terminal (teléfono móvil) del destinatario
- El contenido del mensaje de SMS transmitido

Este certificado de acreditación de SMS certificado se almacenará cifrado en un medio de almacenamiento cifrado y estará disponible para futuras consultas.

Comunicación de correo electrónico certificada: Lleida.net habilitará la dirección electrónica del ordenante, de acuerdo con los registros de verificación de identidad de AR, para que envíe mensajes al sistema de servicios de correo electrónico certificado de Lleida.net.

Mediante cualquier aplicación de correo electrónico o que soporte SMTP, el ordenante proporcionará a Lleida.net:

- El contenido del mensaje de correo electrónico y los adjuntos que haya que entregar al destinatario
- La dirección electrónica del destinatario

Estos datos se entregarán de una de las tres siguientes maneras:

- Enviando un mensaje al destinatario y enviando al sistema de correo electrónico certificado de Lleida.net una copia del mensaje.
- Enviando el mensaje a Lleida.net y añadiendo la dirección electrónica del destinatario al inicio del "Asunto" del mensaje de correo electrónico que haya que enviar.

- Utilizando la interfaz web de Lleida.net (sistema de software de correo electrónico de Lleida.net o sistema Openum de Lleida.net) para crear un mensaje de correo electrónico e indicar sus destinatarios.

Cuando el sistema de servicio de correo electrónico certificado de Lleida.net recibe ese mensaje, los sistemas de Lleida.net lo procesan como una solicitud de envío de correo electrónico certificado y crean y entregan un mensaje de correo electrónico con los siguientes elementos:

- Remitente: el identificador único del ordenante creado mediante el sistema de correo electrónico certificado de Lleida.net para el ordenante en el sistema de correo electrónico certificado de Lleida.net.
- Destinatario: la dirección electrónica indicada por el ordenante.
- Mensaje electrónico y adjuntos: los que determine el ordenante en su solicitud de correo electrónico.

Lleida.net registrará todos los datos del mensaje que vaya a enviarse en nombre del ordenante, así como la fecha y hora de envío.

El MTA (servidor de correo) de Lleida.net enviará el mensaje y recibirá una respuesta del MTA del destinatario con información sobre la aceptación o rechazo del mensaje.

Los sistemas de Lleida.net registrarán la respuesta del MTA del destinatario.

Lleida.net firmará electrónicamente, mediante un certificado cualificado tipo eIDAS u otro certificado X.509 válido en otras jurisdicciones ("certificado de acreditación de correo electrónico certificado") que identifique los siguientes elementos:

- El identificador único de la transacción de la comunicación certificada
- El ordenante del mensaje de correo electrónico de acuerdo con los registros de verificación de la identidad de la AR
- La fecha y hora de envío del mensaje de correo electrónico
- La dirección electrónica del destinatario
- La fecha y hora de la recepción del mensaje en el MTA del destinatario (buzón)
- El contenido del mensaje de correo electrónico transmitido, incluido el mensaje en sí y todos sus adjuntos

Este certificado de acreditación de correo electrónico certificado se almacenará cifrado en un medio de almacenamiento cifrado y estará disponible para futuras consultas.

Comunicación web certificada (Openum): El ordenante de la comunicación certificada utilizará sus credenciales de ordenante para acceder al servicio de comunicaciones web certificadas de Lleida.net (Openum).

Desde esta interfaz web, el ordenante realizará las acciones siguientes en el servicio de Lleida.net:

- Indicará el mecanismo para notificar al destinatario que hay una nueva comunicación web a su disposición (correo electrónico o SMS).
- Configurará un mensaje para el destinatario.
- Determinará la fecha de vencimiento de la comunicación certificada; la comunicación estará disponible para el destinatario solo hasta esa fecha.

- Cargará todos los documentos en PDF que deban transmitirse al destinatario.
- Indicará los datos de contacto del destinatario en formato MSISDN (número de teléfono móvil) o la dirección electrónica, o ambos.
- Indicará el secreto compartido o certificado digital X.509 opcional que tiene que presentar el destinatario para obtener acceso al mensaje de la comunicación certificada (por ejemplo, Openum eIDAS de Lleida.net).

Entonces, el servicio de Lleida.net:

- Enviará un correo electrónico o mensaje SMS (según haya indicado el ordenante) al destinatario, tal como lo haya configurado el ordenante, incluyendo un enlace para acceder a los documentos en PDF que se hayan adjuntado.
- En el momento en que el destinatario acceda al enlace indicado, si el ordenante ha solicitado un secreto compartido o un certificado digital X.509 opcional, el destinatario tendrá que proporcionar los datos solicitados para obtener acceso a los documentos en PDF proporcionados por el ordenante. Si no se ha solicitado, el destinatario podrá acceder a los documentos en PDF cargados por el ordenante y descargarlos.
- Lleida.net realizará el registro y el seguimiento:
    - Del mensaje configurado por el ordenante, los documentos cargados y el destinatario indicados.
    - De la notificación por SMS o correo electrónico enviada al destinatario.
    - De la fecha y hora del envío del SMS o correo electrónico al destinatario.
    - Del MSISDN (número de teléfono móvil) o dirección electrónica del destinatario.
    - De la dirección IP del destinatario desde la cual se accedió a los documentos en PDF.
    - De los resultados del secreto compartido o del certificado X.509 para acceder a los documentos en PDF, si es el caso.
    - De la fecha y hora en la que el destinatario accedió a los documentos en PDF.
    - Del contenido de los documentos en PDF a los que accedió el destinatario.

Lleida.net firmará electrónicamente, mediante un certificado cualificado tipo eIDAS u otro certificado X.509 válido en otras jurisdicciones (“certificado de acreditación de comunicación web certificada (Openum)”) que identifique los siguientes elementos:

- El identificador único de la transacción de la comunicación certificada
- El ordenante de la notificación de acuerdo con los registros de verificación de identidad de la AR
- La fecha y hora de envío del mensaje de notificación
- La dirección electrónica o el MSISDN (número de teléfono móvil) del destinatario
- La fecha y hora de acceso del destinatario a los contenidos de la comunicación
- El contenido de la comunicación, incluidos los mensajes y los documentos en PDF.

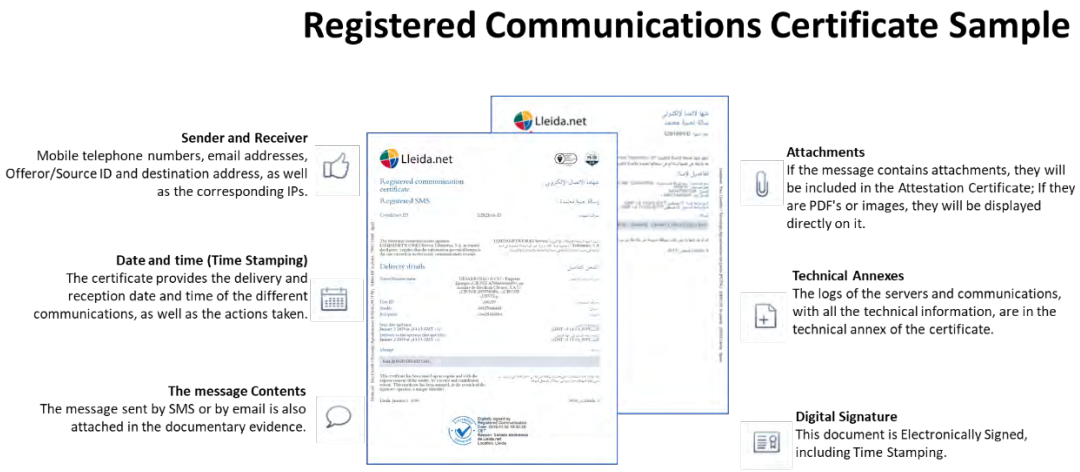
Este certificado de acreditación de correo electrónico certificado se almacenará cifrado en un medio de almacenamiento cifrado y estará disponible para futuras consultas.

La URL de enlace del servicio de comunicación web incluirá una dirección de dominio con un prefijo que identificará el servicio de Lleida.net (por ejemplo, https://openum.ae/h/) y una parte calculada para identificar al destinatario y los documentos a los que se accederá; esta parte

única, denominada aquí "landing_hash", se calculará a partir de los datos personales del destinatario recibidos por el ordenante, y del valor del hash del documento.

5.5 Finalización del proceso de acreditación de la comunicación electrónica certificada

Una vez finalizada la comunicación (enviada y recibida) o bien a su vencimiento (enviada sin recepción por parte del destinatario), el ordenante (a través de un mensaje de correo electrónico) y, según el criterio de este último, también el destinatario (por medios electrónicos que permitan la comunicación entre el destinatario y LLEIDA.NET) recibirán el documento del certificado de acreditación correspondiente a la comunicación certificada, que incluye todas las evidencias electrónicas y lleva un sello electrónico de LLEIDA.NET.



5.6 Recomendaciones operativas

Los certificados de acreditación de comunicaciones electrónicas certificadas de Lleida.net llevan un sello y una marca de tiempo que se calcula mediante el hash del documento y se cifra con una clave privada asociada a un certificado RSA X.509 versión 3. Lleida.net posee un certificado cualificado de persona jurídica expedido por un prestador cualificado de la UE de servicios de firma electrónica y también podría utilizar a otros prestadores de servicios de certificación válidos en otros países y jurisdicciones si fuera necesario.

Todas las partes que confían en los certificados de acreditación de LLEIDA.NET deben verificar que llevan incluido un sello electrónico y que son válidos según las normas de validación, lo que incluye la verificación de la cadena de confianza, las Listas de servicios de confianza y servicios de validación como OCSP o CRL.

6 CONTROL DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONES

6.1 Controles de la seguridad física

Lleida.net ha implantado un sistema de gestión de la seguridad de la información (ISMS, por sus siglas en inglés) certificado, de conformidad con la norma ISO/IEC 27001, que cubre los servicios de confianza que son objeto de esta política.

Así, Lleida.net ha documentado, adoptado e implantado una política de seguridad, una organización de seguridad y también los controles de seguridad necesarios tras realizar un análisis de riesgos y con el objetivo de reducir los posibles riesgos detectados en los ámbitos siguientes:

1. Adopción de una política de seguridad que incluya las directrices del Departamento de Seguridad de la Información y un conjunto de políticas de seguridad de la información, así como su revisión.

2. Implantación de controles organizativos relativos a la seguridad de la información, con la asignación de responsabilidades en seguridad, la puesta en marcha de la segregación de tareas, la seguridad de la información en la gestión de proyectos, y la concienciación, formación y capacitación en seguridad de la información.

3. La implantación de procesos para la gestión de activos, estableciendo un inventario de los mismos con una indicación sobre su uso aceptable, de acuerdo con la clasificación de la información procesada o almacenada fuera de las instalaciones de la empresa, y la seguridad del equipo y los activos que estén fuera a dichas instalaciones.

4. Implantación de la gestión del control de acceso físico y de software; control de redes y del acceso a los servicios asociados; gestión del acceso por parte de los usuarios; gestión de los registros y eliminaciones de los usuarios; gestión de los derechos de acceso concedidos a los usuarios, y gestión de los derechos de acceso con privilegios especiales.

5. Gestión de la información confidencial para la autenticación de usuarios, y la revisión, retirada o adaptación de los derechos de acceso de los usuarios, así como el uso de la información confidencial para la autenticación.

6. Control del acceso a sistemas y aplicaciones con controles de restricción de acceso a la información, procedimientos seguros de inicio de sesión, gestión de contraseñas de usuario, uso de herramientas de administración del sistema y control del acceso al código fuente de los programas.

7. Implantación de medidas físicas y ambientales que establezcan un perímetro de seguridad física, controles de entrada física, seguridad para oficinas y recursos, así como protección contra amenazas externas y ambientales.

8. Medidas de control de la seguridad de los equipos, implantación de controles de ubicación y protección para los equipos, sistemas de suministros, seguridad de cables,

mantenimiento de los equipos, así como procedimientos para sacar los activos de una empresa, además de la seguridad del equipo.

9. Establecimiento de responsabilidades operativas, documentación y procedimientos, gestión de cambios, gestión de capacidades, separación de entornos de desarrollo, pruebas y producción, protección contra malware.

10. Políticas de copias de seguridad, registros de actividad y supervisión, registro y gestión de eventos de actividades.

11. Gestión de vulnerabilidades técnicas y gestión de incidentes y mejoras en materia de seguridad de la información, respuestas a incidentes de seguridad de la información y planificación de la continuidad de la seguridad de la información.

Los procedimientos mencionados más arriba se detallan en la documentación interna confidencial sobre gestión de servicios y seguridad.

6.2 Controles de personal

En Lleida.net se han establecido los siguientes procedimientos de seguridad de las personas de acuerdo con las normas siguientes:

Antes de la contratación:

Tiene que realizarse una verificación que tenga en cuenta, siempre que esté permitido, lo siguiente:

- disponibilidad de unas referencias satisfactorias en cuanto a carácter;
- la verificación del currículum vitae de la persona solicitante;
- la confirmación de las cualificaciones académicas y profesionales declaradas;
- una verificación independiente de la identidad, y
- la comprobación de los antecedentes penales.

Las obligaciones contractuales para empleados y contratistas reflejan las políticas de la empresa sobre seguridad de la información, además de aclarar y declarar:

1. que todos los empleados y contratistas que poseen acceso a información confidencial firman un acuerdo de confidencialidad o no revelación antes de que se les conceda el acceso a instalaciones donde se trate información;

2. las responsabilidades legales y derechos del empleado o contratista;

3. las medidas que se emprenderán si el empleado o contratista ignora los requisitos de seguridad de la empresa que determine Lleida.net.

Cuando se contrata a una persona para un cargo concreto relativo a la seguridad de la información, Lleida.net tiene que asegurarse de que:

a) la persona candidata posee las competencias necesarias para ejercer ese cargo de seguridad, y
b) puede confiarse en ella para asumir ese cargo.

Durante el ejercicio del cargo:

La Dirección exige que los empleados comprendan las responsabilidades en materia de seguridad de la información, así como el cumplimiento de las políticas de seguridad.

Se establece un programa de formación para concienciar en materia de seguridad. Este programa de concienciación se actualiza periódicamente.

Existe un proceso disciplinario formal y debidamente comunicado para tomar medidas respecto a los empleados que cometan una violación de la seguridad de la información:

1. Se verifica debidamente que se ha cometido una violación de la seguridad de la información, y

2. Las medidas están proporcionadas a la gravedad de los hechos.

Cese

En caso de cese o de cambio de puesto de trabajo, las responsabilidades en materia de seguridad de la información continúan vigentes tras el cese o cambio y se indica debidamente cuál es el periodo de confidencialidad.

6.3 Procedimientos de auditoría de seguridad

Se han establecido unos procedimientos de auditoría de seguridad de acuerdo con las normas siguientes:

Se realizan pruebas periódicas de penetración en los sistemas para detectar posibles vulnerabilidades.

Se crean registros de eventos de las actividades de los usuarios, se conservan y se revisan periódicamente.

Como registros de eventos, se incluyen, según corresponda, los siguientes:

- identificaciones de usuario;
- actividades del sistema;
- fechas, horas y detalles de eventos clave (p. ej., entradas y salidas del sistema);
- registros de intentos de acceder al sistema aceptados y rechazados;
- registros de intentos aceptados y rechazados de acceder a datos y a otros recursos;
- cambios en la configuración de los sistemas;
- uso de privilegios;

- uso de las prestaciones y aplicaciones de los sistemas;
- archivos a los que se accede y tipo de acceso;
- activación y desactivación de los sistemas de protección.

6.4 Análisis de vulnerabilidades

Se toman las medidas oportunas como respuesta a la detección de posibles vulnerabilidades técnicas. Se siguen las normas siguientes para establecer un proceso de gestión eficaz ante vulnerabilidades técnicas:

a) se establecen las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluida la monitorización de las vulnerabilidades, la evaluación de riesgos de vulnerabilidad, los parches, el seguimiento de los activos y cualquier responsabilidad de coordinación necesaria;
b) se definen unos plazos para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente importantes;
c) se prueban y evalúan los parches antes de su instalación. Si no hay parches disponibles, se valorará el uso de otros controles, como, por ejemplo:
   - apagado de los servicios o prestaciones relacionados con la vulnerabilidad;
   - adaptación o incorporación de controles de acceso;
   - aumento de la monitorización para detectar ataques reales;
   - información para concienciar sobre la vulnerabilidad en cuestión;
d) mantenimiento de un registro de auditoría de todos los procedimientos realizados.

6.5 Archivo de registros

Los registros de auditoría se utilizan para reconstruir los eventos significativos registrados en el software de la autoridad de registro o de Lleida.net, y el usuario o evento que dio origen al registro. Los registros también se utilizan en el marco de litigios o resolución de disputas para solucionar cualquier posible conflicto comprobando la validez de una firma en un momento determinado.

6.5.1 Tipos de eventos archivados

Lleida.net registra y almacena los registros de auditoría de todos los eventos relacionados con el sistema de seguridad del servicio de firma electrónica avanzada. Se registrarán los eventos siguientes:

- El apagado o encendido del sistema.
- Intentos de crear, eliminar, establecer contraseñas o modificar privilegios.
- Intentos de inicio o cierre de sesión.
- Intentos de acceso no autorizado al sistema a través de la red.
- Intentos de acceso no autorizado al sistema de ficheros.
- Acceso físico a las pistas de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones que operan con el servicio.

- Encendido y apagado de la aplicación que opera con el servicio.
- Cambios en los datos de las claves.
- Registros de solicitudes de expedición o revocación de las credenciales de firma.
- Registros de la expedición o revocación de las credenciales de firma.
- Eventos relacionados con el ciclo de vida del servicio.

Además, Lleida.net conserva, mediante un procedimiento no automático o electrónico, la información siguiente:

- Registros de accesos físicos.
- Cambios en el mantenimiento y la configuración del sistema.
- Informes sobre compromisos y discrepancias.

6.5.2 Plazo de archivo de los registros

Lleida.net almacena información de las pistas de auditoría durante un plazo mínimo de 10 años. Los documentos relativos a la identidad se almacenan durante 15 años.

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

No es posible la eliminación o modificación no autorizada de una entrada de registro de auditoría mediante registros de auditoría escritos.

Los procedimientos y pruebas de auditoría se conservan en medios que no permiten su reescritura o eliminación sin ser detectadas. Este control se garantiza mediante un sistema de hashes en cadenado y de firma digital. En el caso del libro de registros (en papel), se emplean copias de seguridad periódicas y técnicas que limitan la posibilidad de manipular o eliminar la información.

6.6 Recuperación en caso de desastre natural o catástrofe

6.6.1 Procedimiento de gestión de incidentes y vulnerabilidades

Se establecen responsabilidades de gestión y procedimientos para garantizar una respuesta rápida, eficaz y ordenada a cualquier incidente de seguridad de la información. Se tienen en cuenta las directrices siguientes:

1. Se establecen responsabilidades de gestión para garantizar que se llevan a cabo y se transmiten adecuadamente dentro de la organización los siguientes procedimientos:
    - procedimientos de planificación y preparación de respuestas a incidentes;
    - procedimientos de monitorización, detección, análisis y creación de informes de eventos e incidentes sobre seguridad de la información;
    - procedimientos de registro de actividades de gestión de incidentes;
    - procedimientos de manejo de pruebas forenses;
    - procedimientos para realizar evaluaciones y tomar decisiones sobre eventos de seguridad de la información, y para la evaluación de debilidades en la seguridad de la información;

- procedimientos de respuesta, incluidos los de derivación de problemas, recuperación controlada de un incidente y comunicación a personas u organizaciones internas o externas;

2. Los procedimientos establecidos garantizan que:
   - el personal competente maneja las cuestiones relacionadas con los incidentes de seguridad de la información dentro de la organización;
   - se implanta un punto de contacto para la detección e información de los incidentes de seguridad;
   - se mantienen los contactos pertinentes con las autoridades y con grupos o foros de interés externos que manejan cuestiones relacionadas con incidentes de seguridad de la información.

6.6.2 Continuidad del negocio tras un desastre natural o catástrofe

Lleida.net establece, documenta, implanta y mantiene procesos, procedimientos y controles para garantizar el nivel exigido de continuidad de la seguridad de la información durante una situación adversa, y se asegura de que:

1. existe una estructura de gestión adecuada para prepararse, paliar y responder a un evento perjudicial mediante personal con la autoridad, la experiencia y la competencia necesarias;
2. se elaboran y aprueban planes documentados y procedimientos de respuesta y recuperación que detallen cómo gestionará la organización un evento perjudicial;

De acuerdo con los requisitos de continuidad de la seguridad de la información, Lleida.net establece, documenta, implanta y mantiene:

1. controles de seguridad de la información dentro de los planes de continuidad del negocio y de recuperación de desastres;
2. procesos, procedimientos y cambios de implantación para mantener los controles actuales de seguridad de la información durante esa situación adversa;
3. controles que compensen los controles de seguridad de la información que no puedan mantenerse durante la situación adversa.

6.7 Fin del servicio

En el caso de que Lleida.net deje de prestar los servicios descritos en esta política, se lo notificará a la correspondiente autoridad supervisora, a la entidad de certificación/evaluación que haya elaborado su última evaluación de la conformidad, así como a todos sus clientes actuales y a los que lo hayan sido en los últimos cinco años, con un mínimo de cuarenta y cinco (45) días naturales de antelación respecto al final del servicio.

En este periodo de aviso, los suscriptores podrán solicitar, a sus expensas, acceso a las evidencias generadas en sus transacciones con Lleida.net, la cual se las entregará en un formato legible. En cualquier caso, a efectos legales, y a partir del vencimiento del periodo de aviso, Lleida.net procederá a archivar las pruebas en formato PDF de acuerdo con sus procedimientos internos vigentes de generación y conservación de evidencias.

Dada la naturaleza de las propias evidencias generadas y el envío a los clientes y el mantenimiento de la clave pública utilizada para firmar las evidencias por parte del proveedor

de la firma electrónica, no se requiere al servicio que transfiera los derechos y obligaciones del servicio a un tercero en caso del cese de Lleida.net como entidad jurídica.

Las medidas que habrá que tomar para ejecutar el cese serán las siguientes:

- Notificación a los suscriptores actuales y a los que lo hayan sido en los últimos cinco años, con un plazo mínimo de cuarenta y cinco (45) días naturales antes del fin del servicio.
- Notificación a los proveedores de servicios.
- Notificación al Ministerio de Industria o a otras autoridades relevantes.
- Eliminación de la clave privada utilizada para la firma de evidencias de Lleida.net.

7 CONTROLES DE SEGURIDAD TÉCNICA

7.1 Controles de seguridad informática y de ordenadores

7.1.1 Requisitos técnicos específicos de seguridad

Existen una serie de controles sobre los distintos componentes que forman el sistema del servicio.

Controles operativos

- Todos los procedimientos operativos están debidamente documentados en los correspondientes manuales de operaciones. Lleida.net mantiene un plan de contingencia.
- Se han implantado herramientas para la protección contra virus y códigos maliciosos.
- Se realiza un mantenimiento continuo del equipo para garantizar que no se interrumpe su disponibilidad e integridad.
- Existe un procedimiento para almacenar, borrar y eliminar de forma segura de los equipos de almacenamiento de medios, los medios extraíbles y los equipos obsoletos.

Intercambio de datos. Los siguientes intercambios de datos se realizan de forma cifrada para garantizar su confidencialidad:

- Transmisión de los datos de registro entre la AR y la base de datos de registro.
- Transmisión de los datos pre-registro.
- Comunicaciones entre las AR y Lleida.net.

Control del acceso

- Se utilizan identificaciones únicas de usuario de modo que los usuarios son
- y pueden considerarse responsables de sus actos.
- Los derechos se conceden de acuerdo con la norma de proporcionar a los usuarios la mínima cantidad de información y
- solo la cantidad de privilegios de sistema que necesiten para realizar su trabajo.
- Los derechos de acceso se cancelan inmediatamente en el momento en el que los usuarios cambian de puesto de trabajo o dejan la organización.
- El nivel de acceso asignado a los usuarios se revisa cada tres meses.
- Los privilegios de sistema se conceden dependiendo de cada caso y terminan una vez que el motivo por el que se concedieron deja de ser válido.
- Lleida.net mantiene unas directrices de calidad respecto a las contraseñas.

Evaluación de la seguridad informática

Lleida.net realiza varias auditorías respecto al mantenimiento del certificado ISO 27001 y a su estatus como prestador cualificado de servicios de confianza de la Lista de confianza de la Comisión Europea.

7.2 Controles de seguridad del ciclo de vida

7.2.1 Controles de desarrollo de sistemas

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

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

- Existe un procedimiento de autorización formal para la actualización de las bibliotecas de software (incluidos los parches) en producción. La autorización se otorga solo tras asegurarse de que funciona adecuadamente.
- El sistema de comprobación se mantiene separado del sistema de producción para garantizar que funciona adecuadamente antes de entrar en producción.
- Se mantiene un fichero de registro en todas las actualizaciones de bibliotecas.
- Se conservan las versiones anteriores del software.
- El software adquirido se mantiene según el nivel de soporte del vendedor.
- Existen procedimientos para incluir ampliaciones del código fuente.

7.2.2 Controles de seguridad del ciclo de vida

Para realizar pruebas, se requiere de un gran volumen de datos que sean lo más parecidos posible a los datos de producción. Lleida.net evita el uso de bases de datos de producción con información personal.

7.2.3 Controles de seguridad de la red

Todas las medidas y controles de seguridad especificados para el resto de sistemas se aplican también a los dispositivos de red. La política de seguridad para el uso de redes y servicios de red se describe en la política de seguridad de redes. Los usuarios solo pueden acceder a los servicios para los cuales tienen autorización.

7.2.4 Fuentes para las horas

Cuando se incluya alguna información sobre la hora, se utilizará como referencia la hora oficial proporcionada por el ROA (Real Observatorio de la Armada). Los sistemas de Lleida.net se sincronizarán mediante NTP con los servidores del ROA o bien podrán obtener la información del tiempo universal coordinado del sistema de satélites GPS, que tiene una precisión de más de 100 nanosegundos con respecto a todos los laboratorios nacionales de metrología, incluido el ROA y el USNO (Observatorio Naval de Estados Unidos, por sus siglas en inglés).

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

LLEIDA.NET ha realizado varias auditorías a su **Sistema de Gestión Integrada** en relación con varias normativas. En este momento, cuenta con las certificaciones de las normas siguientes:

- ISO 27001
- EIDAS QERDS (Qualified Electronic Registered Delivery Service)

Lleida.net realizará auditorías del rendimiento de su servicio de firma electrónica avanzada y de su servicio de certificación de comunicaciones electrónicas certificadas. Dichas auditorías serán realizadas por un auditor independiente. También se llevarán a cabo auditorías en todos los servicios de confianza de Lleida.net cada dos (2) años, a no ser que exista alguna disposición que exija una evaluación anual.

Todas las auditorías verificarán, como mínimo, que las prácticas de Lleida.net se llevan a cabo en cumplimiento de esta Declaración de Políticas y Prácticas, de los mandatos vigentes de las autoridades pertinentes y de las normativas aplicables, así como que existe una metodología para garantizar la calidad de los servicios prestados.

9 OTRAS CUESTIONES JURÍDICAS Y SOBRE LA ACTIVIDAD DE LLEIDA.NET

9.1 Honorarios

Los honorarios son los establecidos en la página web de Lleida.net (www.lleida.net) o en los acuerdos concretos firmados entre Lleida.net y sus suscriptores o entre Lleida.net y las AR designadas, o entre la AR designada por Lleida.net y sus suscriptores, según corresponda de acuerdo con el contrato del suscriptor.

Lleida.net publicará los honorarios aplicados a la prestación de cada uno de sus servicios en su sitio web, y podrá actualizarlos cada cierto tiempo.

Lleida.net no cobrará ningún honorario por el acceso a la información necesaria para verificar la validez de una prueba expedida o a esta Declaración de Políticas y Prácticas, ni a ninguna información que deba hacerse pública en virtud de las disposiciones de dicha Declaración.

9.2 Responsabilidad económica

Lleida.net solo será responsable del incumplimiento de las obligaciones previstas en la legislación aplicable y en esta Declaración de Políticas y Prácticas.

Lleida.net no será de ningún modo responsable respecto al uso de la prueba expedida con fines no autorizados por esta Declaración de Políticas y Prácticas.

Lleida.net no es responsable del contenido de los documentos y datos para los cuales se utilizan sus servicios y, por tanto, no será responsable de los posibles daños causados por las transacciones en las que se utilicen dichos servicios.

Lleida.net no representa en modo alguno a los firmantes, creadores de documentos, partes que confían o personas usuarias de los servicios o de la prueba o evidencia expedida.

Lleida.net no proporciona garantía alguna ni asume responsabilidad de ningún tipo hacia los titulares de los certificados u otras pruebas expedidas ni hacia los usuarios de los mismos, excepto en lo que dispone esta Declaración de Políticas y Prácticas.

Lleida.net y sus filiales están aseguradas bajo la Póliza de Indemnización Profesional con una cobertura de siete millones de euros (7.000.000,00 €).

9.3 Confidencialidad de la información

Se considerará como información confidencial cualquier información que se revele verbalmente o por escrito, o por cualquier otro medio tangible o intangible, de una forma conocida actualmente o facilitada por alguna tecnología futura, que se intercambie como consecuencia de la prestación del servicio y que una de las partes indique o describa a la otra como confidencial. Las partes se comprometen a adoptar las medidas adecuadas para garantizar el tratamiento confidencial de dicha información, medidas que no serán de nivel inferior a las medidas que ellas mismas aplican para su propia información confidencial, asumiendo además las siguientes obligaciones:

- Utilizar la información confidencial solo para el uso propio para el que está destinada.

- Permitir el acceso a la información confidencial solo a las personas físicas o jurídicas que, en ambos casos, en la prestación de sus servicios, necesiten la información para realizar tareas en las cuales el uso de esa información sea estrictamente necesario.

A este respecto, la parte que recibe la información advertirá a dichas personas físicas o jurídicas de sus obligaciones con respecto a la confidencialidad y se asegurará de que las cumplen.

- Comunicar a la otra parte cualquier violación de la información que conozcan o de la cual entren en conocimiento, que resulte del incumplimiento de esta condición o de la deslealtad de las personas que hayan accedido a la información confidencial, entendiendo que dicha comunicación en ningún caso exime de su responsabilidad a la parte que ha incumplido el compromiso de confidencialidad, excepto si el incumplimiento diera lugar a responsabilidades derivadas de dicha omisión en concreto.

- Limitar el uso de la información confidencial intercambiada por las partes a lo estrictamente necesario para el cumplimiento del objeto de este acuerdo, de manera que la parte que reciba la información confidencial asumirá la responsabilidad por cualquier uso distinto de ese objeto, realizado por esa parte o por las personas físicas o jurídicas a las que haya permitido acceder a la información confidencial.

- No revelar la información de la otra parte a terceros a no ser que se cuente con la autorización previa por escrito de esa otra parte.

Sin perjuicio de las obligaciones impuestas por la legislación nacional y/o asumidas por la parte que recibe la información confidencial, las obligaciones de confidencialidad incluidas en esta disposición no se aplicarán a la información respecto de la cual la parte receptora pueda demostrar que:

- Era de dominio público en el momento en el que se le reveló.
- Tras serle revelada, fue publicada o pasó a ser de dominio público de otro modo, sin que mediara incumplimiento de la obligación de confidencialidad de la parte que recibió la información.
- En el momento de serle revelada, la parte que la recibió ya la conocía por medios legales, o bien tenía acceso legal a la misma.
- Tenía el consentimiento previo por escrito de la otra parte para revelar la información.
- Se le ha solicitado la revelación por parte de una autoridad administrativa o judicial competente que deba pronunciarse sobre todos o algunos de sus aspectos, en cuyo caso la parte que deba realizar la revelación debe comunicárselo a la otra parte con anterioridad a que tenga lugar dicha revelación.

9.4 Protección de datos personales

Como consecuencia de la prestación de los servicios, es posible que LLEIDA.NET tenga acceso a datos personales de los que el ordenante sea responsable.

LLEIDA.NET informa al firmante y al ordenante del tratamiento de los datos personales recopilados en cada contrato y de los que puedan obtenerse durante su vigencia, con el fin de prestar el servicio solicitado y facturarlo. La base legal del tratamiento de los datos es el contrato entre el ordenante y LLEIDA.NET. Los datos proporcionados se conservarán durante tanto tiempo como se mantenga la relación comercial o durante los años como sea necesario para

cumplir con las obligaciones legales. Los datos no podrán transferirse a terceros excepto en aquellos casos en los que exista una obligación legal. El firmante tiene el derecho de obtener una confirmación sobre si LLEIDA.NET está tratando sus datos personales y, por tanto, tiene derecho a acceder a ellos, a rectificar los que sean inexactos o a solicitar su eliminación cuando los datos ya no sean necesarios, tras demostrar su identidad e interés en la realización de esas acciones. Los datos personales no se transferirán a un tercer país. El firmante tiene derecho a presentar una queja a la autoridad encargada de cuestiones de privacidad (en España, la AEPD) o a otras autoridades competentes en otras jurisdicciones, en el caso de que considere que se están infringiendo sus derechos a la protección de datos (Reglamento UE 2016/679, de 27 de abril de 2016).

9.5 Derechos de propiedad intelectual

La totalidad de las aplicaciones o programas informáticos que hacen posible la prestación de los servicios, incluido el diseño de la plataforma, sus bases de datos, su estructura de navegación y los textos, imágenes, animaciones, logotipos o nombres, son propiedad de LLEIDA.NET o, cuando así se indique, corresponden a terceros que han autorizado su uso e incorporación a la plataforma, y están protegidos por las leyes y tratados sobre propiedad intelectual e industrial.

Queda prohibida la reproducción, transformación y distribución de estos contenidos, así como cualquier acto de descompilación o ingeniería inversa distinto de la visualización, reproducción o edición de documentos dentro de la propia plataforma de LLEIDA.NET. Bajo ninguna circunstancia se permitirá la extracción, reutilización y/o explotación de dichos contenidos cuando impliquen la realización de actos contrarios a la explotación normal de los mismos, especialmente su uso con finalidades comerciales o publicitarias, fuera del servicio o bien que perjudiquen los derechos morales o de explotación de los clientes de LLEIDA.NET. El ordenante, como cliente de LLEIDA.NET, no llevará a cabo ni permitirá que otros lleven a cabo ningún acto que pueda de alguna forma socavar o menospreciar el valor o la validez de los derechos de propiedad intelectual o industrial de LLEIDA.NET.

9.6 Obligaciones

El ordenante tendrá derecho a utilizar solo los servicios estrictamente contratados y asumirá la responsabilidad sobre el contenido de la información que se transfiera a través de ellos.

Términos de la licencia del programa Tools (www.tools.LLEIDA.NET) y de otras herramientas proporcionadas por LLEIDA.NET a los ordenantes: LLEIDA.NET otorga a los ordenantes una licencia no exclusiva para usar estas aplicaciones para las finalidades propias del CLIENTE y durante toda la vigencia del contrato. El ordenante no podrá distribuir comercialmente, sublicenciar, revender o transferir en ningún caso, sin el consentimiento previo por escrito de LLEIDA.NET, ni reproducir para esos propósitos los programas o cualquier modificación o derivación de los mismos, ya sea por separado o conjuntamente con cualquier otro producto o programa. Además, los ordenantes no podrán modificar los programas excepto para su uso personal y para finalidades comerciales internas.

Ley de Comercio Electrónico. Los ordenantes aceptan, de conformidad con lo previsto en los artículos 21 y 22 de la LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO

ELECTRÓNICO (LSSICE, Ley 34/2002, de 11 de julio, BOE de 12 de julio de 2002) que no podrán utilizar los servicios para enviar mensajes masivos (correo basura, publicidad, mensajes promocionales o comerciales) sin el consentimiento o autorización expresos de cada uno de los destinatarios, a no ser que se trate de excepciones previstas por la ley, ni tampoco para el envío de mensajes cuyo propósito o contenido pueda considerarse contrario a la legalidad, la moralidad o las buenas costumbres o que constituyan un delito o falta, ni aquellos que puedan perjudicar los derechos o la imagen de LLEIDA.NET o de terceros.

Los ordenantes deben mantener en secreto los códigos de acceso a los servicios y cambiarlos si sospechan que otros terceros los conocen o pueden llegar a conocerlos de forma indebida.

Si el ordenante no cumple con alguna de estas obligaciones legales o contractuales, LLEIDA.NET se reserva el derecho de interrumpir los servicios de forma inmediata, informando a su CLIENTE de que dicho incumplimiento debe subsanarse para que puedan restablecerse los servicios. El hecho de que el ordenante no subsane el incumplimiento en un plazo de cinco (5) días a partir de la fecha en que LLEIDA.NET se lo comunique, podrá acarrear la rescisión del contrato, teniendo el ordenante la obligación de compensar por los daños provocados como resultado del incumplimiento.

Se prohíbe la redistribución de los servicios a terceros sin el consentimiento previo por escrito de LLEIDA.NET.

9.7 Renuncia de responsabilidad

LLEIDA.NET no será responsable de las infracciones de la legislación vigente que puedan cometer los ordenantes como resultado del uso indebido de los servicios. En el caso de que LLEIDA.NET detecte la existencia de alguna irregularidad en el uso de los servicios, podrá terminar el contrato sin aviso previo al CLIENTE.

La responsabilidad de LLEIDA.NET en cualquiera de los casos de incumplimiento que le sean atribuibles se limitará a la cantidad de servicios prestados objeto de la reclamación.

Puesto que LLEIDA.NET depende de los servicios de terceros para la adecuada prestación de sus propios servicios, LLEIDA.NET declina cualquier responsabilidad por daños provocados por la falta de dichos servicios, aceptando únicamente los causados por una deficiencia en los medios telemáticos de apoyo o por una negligencia de LLEIDA.NET y sus empleados, teniendo que quedar estas debidamente acreditadas.

Puesto que la mayoría de las instalaciones necesarias para el funcionamiento adecuado de la red dependen de empresas terceras, LLEIDA.NET no será responsable del resultado del servicio. Esto incluye errores de direccionamiento, pérdida de información o datos, retrasos de entrega o interrupciones no previstas de los servicios.

LLEIDA.NET declina toda responsabilidad en relación con la calidad, exactitud, fiabilidad y corrección de los datos, programas e informaciones de cualquier tipo que circulen por sus redes. El contenido de dicha información es responsabilidad única de las partes que la intercambian (remitente y destinatarios).

LLEIDA.NET no será considerada responsable en caso de uso no autorizado de los servicios por terceros.

9.8 Responsabilidades

Lleida.net será responsable de los daños causados al firmante o a terceros de buena fe cuando incumpla las obligaciones que le impone el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 julio de 2014 y la legislación nacional de los correspondientes mercados aplicable a este servicio.

La responsabilidad del prestador de servicios de confianza regulada por ley será ejecutable de conformidad con las reglas generales sobre dolo contractual o no contractual, según sea el caso, pero será el prestador de servicios de confianza el que deberá demostrar que ha actuado con la diligencia profesional que se le exige haciéndose responsable de los daños causados intencionadamente o por negligencia a cualquier persona física o jurídica a la que haya delegado este servicio.

Cuando Lleida.net, como prestador de servicios de confianza, debidamente y por adelantado informe a los solicitantes, firmantes y otros suscriptores del servicio sobre las limitaciones de uso de los servicios que presta y esas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los daños causados por un uso de los servicios que se exceda de las limitaciones indicadas.

Lleida.net, como prestador de servicios de firma electrónica avanzada, asumirá la responsabilidad ante terceros por las acciones de personas que deleguen la ejecución de una o más de las funciones necesarias para la prestación de servicios fiables.

Autoridad de registro

La autoridad de registro asumirá toda la responsabilidad respecto a la identificación correcta de los solicitantes y firmantes de datos y a la verificación de sus datos, con las mismas limitaciones que las establecidas para Lleida.net.

9.9 Renuncias a pérdidas

Lleida.net no asume responsabilidad alguna por los daños causados en las siguientes circunstancias:

- En caso de guerra, catástrofes naturales o cualquier otro acontecimiento fortuito o de fuerza mayor: disturbios de orden público, huelgas de transporte, cortes del suministro eléctrico o de teléfono, virus informáticos, deficiencias en los servicios de telecomunicaciones o el uso del compromiso del servicio de firma electrónica avanzada derivado de un riesgo tecnológico impredecible.
- Cuando lo cause el uso no autorizado de las credenciales de firma del firmante, o la superación de los límites establecidos en esta política.
- Cuando lo cause el uso inadecuado o fraudulento de las credenciales de firma expedidas por Lleida.net.
- Lleida.net no será responsable del contenido de los documentos firmados electrónicamente ni de ninguna otra información utilizada en un proceso de autenticación en el que se incluya una firma electrónica avanzada expedida por Lleida.net.

9.10 Periodo de validez de los documentos de la Política

El presente documento constituye la actual Declaración de Políticas y Prácticas de los servicios de firma electrónica avanzada y de certificación de comunicaciones electrónicas certificadas, relativa a los servicios de firma electrónica avanzada y de certificación de comunicaciones electrónicas ofrecidos por Lleida.net. Cualquier modificación de este documento tiene que ser aprobada por el pertinente organismo de gestión y aprobación de políticas.

Dichas modificaciones se incluirán en un documento que actualiza esta Declaración de Políticas y Prácticas, cuyo mantenimiento queda garantizado por Lleida.net.

Las versiones actualizadas de este documento, junto con la lista de modificaciones realizadas, pueden consultarse en la dirección web (URL) que se encuentra en el apartado “Nombre e identificación de documentos”.

Lleida.net podrá modificar este documento y para hacerlo actuará de conformidad con el siguiente procedimiento:

- La corrección tendrá una justificación técnica, jurídica o comercial.
- Se revisarán todas las repercusiones técnicas y jurídicas de la nueva versión de las especificaciones.
- Se establecerá un control de las modificaciones para garantizar que las especificaciones resultantes
- cumplen los requisitos que tienen que cumplir y que motivaron el cambio.
- Se valorarán las repercusiones que puede tener sobre los usuarios el cambio de especificaciones,
- en caso de que tengan que ser informados del cambio.

En la fase de preparación de las auditorías, Lleida.net revisará este documento para asegurarse de que se mantiene al día en relación con los cambios que tengan lugar en los ámbitos siguientes.

- Implementación del marco legislativo.
- Publicación de estándares.
- Mejoras o faltas de conformidad detectadas en las auditorías.
- Mejoras realizadas en los servicios o lanzamiento de nuevos servicios.
- Adopción de productos o servicios de terceros que se integren con los que ya ofrece Lleida.net.

Lleida.net podrá efectuar en el documento, sin aviso previo a los usuarios, cambios como:

- Correcciones de errores tipográficos en el documento
- Cambios en la información de contacto.
- Cambios en las especificaciones o condiciones de los servicios.

9.11 Notificaciones individuales y comunicaciones con Lleida.net

Cualquier notificación a Lleida.net se realizará por correo electrónico a la dirección info@lleida.net o bien por correo postal a la dirección Lleidanetworks Serveis Telemàtics, S.A., PARC CIENTÍFIC I TECNOLÒGIC AGROALIMENTARI, ED. H1 PL. 2 - 25003 LLEIDA (ESPAÑA).

Cualquier comunicación no certificada se considerará efectuada a partir de la fecha en la que Lleida.net proporcione un acuse de recibo al remitente.

9.12 Reclamaciones y jurisdicción y ley aplicable

Cuando un usuario desee presentar una reclamación respecto a los servicios de Lleida.net, esta debe comunicarse a través de cualquiera de los medios de contacto indicados en el apartado anterior. Lleida.net responderá a la reclamación en un periodo máximo de una semana.

Excepto cuando existan suplementos nacionales específicos a esta Declaración de Políticas y Prácticas, los ordenantes, los firmantes y las partes que confían aceptan por la presente quedar sujetos a la jurisdicción de los tribunales de Madrid (España) para cualquier controversia que se derive de la prestación de los servicios por parte de Lleida.net, y renuncian expresamente a cualquier otra jurisdicción que pudiera corresponderles. Si el firmante es un consumidor, se le aplican las disposiciones de tratados y convenciones internacionales. En cualquier caso, siempre se preferirá la resolución amistosa de cualquier controversia.

Excepto cuando existan suplementos nacionales específicos a esta Declaración de Políticas y Prácticas, los actuales términos y condiciones se aplicarán e interpretarán de acuerdo con la legislación española.

9.13 Otras disposiciones

Los servicios de firma electrónica avanzada y de certificación de comunicaciones electrónicas certificadas se basan, en la mayoría de casos, en servicios de AR gestionados por los ordenantes. Sin embargo, pueden contratarse los servicios de AR proporcionados por LLEIDA.NET, que podrán asociarse a los servicios de firma electrónica avanzada y de certificación de comunicaciones electrónicas certificadas.

En el caso de entidades supeditadas a los reglamentos de PBC-FT y los grupos de trabajo FATF o MENA-FATF, el ejercicio de las actividades de diligencia debida exige la obligación de realizar una identificación previa.

En otros contextos de comercio electrónico y contratación a distancia, la generación de evidencias permite su presentación ante un tribunal, pero depende de la confirmación de la identidad, en caso de que se ponga en cuestión.

Cuando se usan certificaciones en un contexto para confirmar la formalización de un contrato, la realización de una firma electrónica avanzada no basada en un certificado o el envío y recepción de comunicaciones electrónicas, se incorporan todas las evidencias electrónicas posibles de la transacción, como, por ejemplo:

- la IP desde la cual se accedió,
- el sistema operativo utilizado por el usuario,

- el navegador utilizado por el usuario,
- las características técnicas de la comunicación, y
- otra información complementaria, como el número de teléfono móvil vinculado a la operación, cuando se usen técnicas de autenticación de factor doble.

Debe tenerse en cuenta que la asociación de un número de teléfono móvil con una persona concreta, incluso en terminales de prepago, exige, en la mayoría de las jurisdicciones, que se verifique la identidad a través de los puntos de venta de teléfonos móviles y tarjetas SIM.