ECD_CO_1008.01_Política Servicio Estampado Cronológico (TSA)

Lleida SAS
Colombia - Bogotá

Control de documentación

Histórico de versiones

Versión	Fecha	Autor	Descripción
1	07/03/2022	Gloria Salvador	Versión inicial

Lista de distribución

Empresa
Lleida SAS

Clasificación y estatus

Clasificación	Estatus
Uso Interno	Aprobado

Documentos referenciados

Descripción

Tabla de contenido

1. Introducción

1.1 Objetivo

Dar a conocer al público en general los lineaminentos establecidos por Lleida SAS para prestar el servicio de Estampado Cronológico como ECD de acuerdo con los establecido en la Ley 527 de 1999, Ley 1437 de 2011 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia

1.2 Alcance

Todos los miembros de Lleida SAS, Entidad de Certificación Digital, así como todas las terceras partes identificadas en el alcance del Sistema de Gestión de la Entidad de Certificación Digital

1.3 Distribución

Aprobada por la Dirección de Lleida SAS, esta Política debe ser accesible a todas las personas incluidas en la lista de distribución especificada en el control documental, mediante los canales adecuados, establecidas en el procedimiento ECD_CO-3001 - Gestión del repositorio de documentación.

1.4 Revisión

La presente Política de Servicio será revisada y aprobada anualmente por parte del Comité de Seguridad de Lleida.net. No obstante, si tuvieran lugar cambios relevantes para la Organización, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento.

2. Consideraciones previas

Política de Servicio de Estampado Cronológico, en adelante *Política* es un documento elaborado por Lleida SAS (en adelante Lleida.net) que, actuando como una Entidad de Certificación Digital (en adelante ECD) contiene las normas, procedimientos que Lleida.net aplica como lineamiento para prestar el servicio de Estampado Cronológico de acuerdo a lo establecido en la Ley 527 de 1999, Ley 1437 de 2011 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia.

La Política está conforme con los siguientes lineamientos:

- Criterios específicos de Acreditración para las Entidades de Certificación Digital CEA 3.0-07 (en adelante CEA) que deben ser cumplidos para obtener la acreditación como ECD, ante el Organismo Nacional de Acreditación de Colombia (en adelante ONAC)
- Ley 527 de 1999
- Estándares y protocolos:

  CAdES (CMS Advanced Electronic Signatures). ETSI TS 101 733

  https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v02020p.pdf

  PAdES (PDF Advanced Electronic Signatures). ETSI TS 102 778

  https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

  RFC 5126 CMS Advanced Electronic Signatures (CAdES)

  https://datatracker.ietf.org/doc/html/rfc5126

  RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

  https://datatracker.ietf.org/doc/html/rfc3161

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

  RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

  https://datatracker.ietf.org/doc/html/rfc5905

  Protocolo ANSI ASC X9.95 ETSI TS 101 861 V1.2.1 Time stamping profile

  https://www.etsi.org/deliver/etsi_ts/101800_101899/101861/01.04.01_60/ts_101861v010401p.pdf

ISO/IEC 19005-3:2012 Document Management - Electronic document file format for long term preservation - Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

https://www.iso.org/standard/57229.html

DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN LEGAL

Razón social:	LLEIDA S.A.S.
N.I.T.	900571038-3
Dirección:	Calle 81 # 11 – 55 Oficina 903
Ciudad/País	Bogotá/Colombia
Teléfono:	+5713819903
Correo electrónico:	co@lleida.net
Página web:	www.lleida.net/co

DATOS DE LA ENTIDAD DE REGISTRO

La entidad de registro es la misma prestadora de servicios de certificación digital.

Peticiones, Quejas, Reclamos, Solicitudes y apelaciones

Las peticiones, quejas reclamos, solicitudes y apelaciones sobre los servicios prestados por Lleida SAS seran atendidas por varios mecanismos a disposición del subscriptor y seran resueltas por las personas pertinentes e imparciales.

- Por correo electrónico a clientes@lleida.net . Deberá adjuntarse la plantilla disponible en www.lleida.net/co ECD_CO 4501 Plantilla PQRSA Lleida SAS

- Por teléfono al +57 1 381 9903

En el plazo máximo de 15 días deberán ser resueltas y notificadas, previa radicación, análisis y redacción de reporte formal que será entregado al subscriptor.

DEFINICIONES

Tercero que confía Persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez de dicho sello provisto por la TSA de LLEIDA.NET

Suscriptor Persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está de acuerdo con los acuerdos y obligaciones descritos en la Declaración de Prácticas y la Política de Sellado de Tiempo.

Política de sellado de tiempo Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.

Sello de tiempo Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. El sello de tiempo incluye:

- La firma digital de la entidad de sellado de tiempo
- Identificador electrónico único del documento (HASH o resumen)
- Fecha y hora recogida de una fuente fiable de tiempo

Autoridad de Sellado de tiempo/Estampado Cronológico (TSA) Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.

Declaración de Prácticas Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.

Sistemas de la TSA Sistemas de tecnologías de la información que soportan la provisión de servicios de sellado de tiempo.

Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

Unidad de Sellado de tiempo Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

ABREVIACIONES

BIPM International Bureau of Weights and Measures (Bureau International Des Poids et Mesures

GMT Greenwich Mean Time

IERS International Earth Rotation Service

TAI International Atomic Time (Temps Atomique international)

TSA Time-Stamping Authority

TSU Time-Stamping Unit

UTC Coordinated Universal Time

PARTICIPANTES

AUTORIDAD DE SELLADO DE TIEMPO DE LLEIDA.NET (TSA LLEIDA.NET)

LLEIDA.NET., en su papel de Autoridad de Sellado de Tiempo, es la persona jurídica privada que presta indistintamente servicios de emisión de sellados de tiempo.

PROVEEDOR DEL CERTIFICADO DIGITAL (ECD LLEIDA.NET)

Los servicios de sellado de tiempo son provistos en la infraestructura y bajo la administración de LLEIDA.NET. El certificado digital es provisto por la EC LLEIDA.NET, es una Entidad de Certificación Digital autorizada por el Organismo supervisor. Como parte de la cobertura de seguridad del certificado digital de sellado de tiempo, LLEIDA.NET ampara las transacciones de sellado de tiempo mediante la cobertura del Seguro de Responsabilidad Civil.

3. Administración de políticas

La administración de las Políticas de Servicios están a cargo del proceso de Sistema Integrado de Gestión

Persona de contacto

Nombre: Eva Pané Vidal
Cargo: Supervisor de la ECD
Teléfono de contacto: +57 1 381 9903
Correo electrónico: compliance@lleida.net

Las políticas deben ser aprobadas por el Comité de Seguridad, una vez aprobadas es responsabilidad el Supervisor de la ECD la actualización en los portales web en su última versión.

3.1 POLÍTICA DE SELLADO DE TIEMPO

LLEIDA.NET gestiona las actividades de sellado de tiempo conforme con la RFC 3628.

3.2 IDENTIFICACIÓN

La Política de Sellado de Tiempo de LLEIDA.NET tiene como identificador único:

1.3.6.1.4.1.53589.1.1.5.3

3.2.1 CERTIFICADO SUBORDINADA SELLADO DE TIEMPO LLEIDA.NET

El DN del 'issuer name' del certificado de la subordinada de sellado de tiempo de LLEIDA.NET tiene las siguientes características:

CN = Certification Authority Root Lleida SAS

O = Lleida SAS

SERIALNUMBER = 9005710383

OU = Certification Authority Lleida SAS

L = BOGOTA

C = CO

En el DN del 'subject name' se incluyen los siguientes campos:

Description = Lleida SAS Timestamping Certificate 001

CN = Lleida SAS TSA 001

O = Lleida SAS

2.5.4.97 = VATCO-9005710383

SERIALNUMBER = 9005710383

OU = Trusted Timestamp Service Lleida SAS

T = Service Timestamping Lleida SAS

L = BOGOTA

C = CO

Número de serie = 55851d3283da

Huella digital = fd0c2775cf765897fa6d3c1837f1709d4b9a01eb

SHA-256 =
6161AC5B3AB0E37EE191E675E77076EFED2EB8C04C62DA936E08A67D0BF46DFB

3.2.2 CERTIFICADO TSU LLEIDA.NET

El DN del 'issuer name' del certificado de la TSU de LLEIDA.NET tiene las siguientes características:

Description = Lleida SAS Timestamping Certificate 001

CN = Lleida SAS TSA 001

O = Lleida SAS

2.5.4.97 = VATCO-9005710383

SERIALNUMBER = 9005710383

OU = Trusted Timestamp Service Lleida SAS

T = Service Timestamping Lleida SAS

L = BOGOTA

C = CO

En el DN del 'subject name' se incluyen los siguientes campos:

Description = Lleida SAS Timestamping Certificate 001

CN = Lleida SAS TSA 001

O = Lleida SAS

2.5.4.97 = VATCO-9005710383

SERIALNUMBER = 9005710383

OU = Trusted Timestamp Service Lleida SAS

T = Service Timestamping Lleida SAS

L = BOGOTA

C = CO

Número de serie = 0f722082701b

Huella digital = fefc64bf46cda1ca393d575450d9dc8b43c2ddf0

SHA-256 = 831CAD598471601847E62CDFE2488B916CB6EE6AD8873B502B6CC2B9185CE3B2

4. CICLO DE VIDA DE LA GESTIÓN DE LA CLAVE

4.1 GENERACIÓN DE LA CLAVE DE LA TSA

La generación de la clave privada del certificado digital con el cual se firman los sellos de tiempo es realizada en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628), por personal confiable (sección 7.4.3 de la RFC 3628) bajo, al menos, autorización de dos personas.

La generación de la clave privada se realiza en un módulo hardware de seguridad – HSM con certificaciones FIPS 140-2 nivel 3 o Common Criteria EAL 4+ y su administración es protegida por al menos dos personas.

4.2 CARACTERÍSTICAS TÉCNICAS DEL CERTIFICADO DIGITAL Y DE LOS ALGORITMOS UTILIZADOS

Las características del certificado digital y de los algoritmos utilizados en los servicios de sellado de tiempo son: SHA-1, SHA-256, SHA-384, SHA-512. Se desaconseja a sus subscriptores el uso de SHA-1 como algoritmo de resumen, que se mantiene por motivos de compatibilidad.

4.3 PROTECCIÓN DE LA CLAVE PRIVADA DE LA TSA

La clave privada del certificado de firma de cada sello de tiempo es resguardada durante su uso dentro de un módulo hardware criptográfico con certificación FIPS 140-2 nivel 2. Las copias de respaldo se almacenan en un módulo criptográfico del mismo nivel de seguridad.

4.4 DISTRIBUCIÓN DE LA CLAVE PÚBLICA TSU

La clave pública está contenida dentro de un certificado X.509 v3, firmada digitalmente por una Entidad de Certificación Digital de INDENOVA S.L. regulada por su Declaración de Prácticas.

4.5 RE-EMISIÓN DE LA CLAVE DEL TSU

La clave privada de la TSA será reemplazada antes de la expiración de su periodo de validez y en caso de obsolescencia o vulnerabilidad declarada del algoritmo, el tamaño de la clave u otra medida de seguridad relevante.

4.6 ALMACENAMIENTO DE LOS REGISTROS DE AUDITORÍA

Los registros concernientes a la operación del servicio de sellado de tiempo, incluyendo eventos relacionados a la sincronización del reloj con la fuente confiable de tiempo y la gestión de las claves de la TSA son salvaguardados contra modificación no autorizada.

Los registros son almacenados y protegidos por un periodo de 1 año adicional al periodo de vigencia del certificado digital con el que el sello de tiempo fue creado. En caso de que la clave privada de la TSA se vea comprometida, entonces el periodo de almacenamiento de registros será mayor que los sellos de tiempo más afectados.

4.7 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA DEL TSU

Las claves privadas con las cuales se firman los sellos de tiempo reconocidos por Lleida.net, no serán usadas luego de terminado su ciclo de vida sino que será emitida una nueva clave y puesta en operación, realizando el cambio de un certificado digital por otro, incluyendo la generación segura y la publicación del nuevo certificado.

La clave de la TSA que ha expirado o ha sido revocada o cualquier parte de ella, incluyendo cualquier copia será destruida de modo que no pueda ser recuperada.

5. GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO USADO PARA FIRMAR LOS SELLOS DE TIEMPO

Los módulos hardware criptográficos que se utilizan para almacenar y proteger las claves privadas con las cuales se firman los sellos de tiempo reconocidos por LLEIDA.NET, son protegidos contra manipulación no autorizada durante todo su ciclo de vida, incluyendo transporte, generación de la clave, uso y almacenamiento.

La instalación, activación y duplicación de las claves de la TSU en el hardware criptográfico sólo puede ser realizada por el personal que tiene asignado un rol de confianza, usando al menos un control dual en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628) con control de acceso físico de al menos dos personas.

Se monitoreará el funcionamiento correcto del hardware criptográfico.

En los casos que se decida desechar el equipo las claves privadas de la TSA serán borradas para evitar su uso no autorizado. Considerando el respaldo seguro de la clave si aún se encuentra vigente.

6. SELLO DE TIEMPO

Los sellos de tiempo cumplen lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161.
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA.
- Cada sello de tiempo tiene asignado un único identificador.
- El tiempo incluido en el sello de tiempo será sincronizado con la UTC dentro de la exactitud de +/- 1 segundo.
- El sello de tiempo incluye un resumen de los datos firmados (HASH).
- El sello de tiempo deberá ser firmado por una clave generada para este propósito, correspondiente a la TSA.
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada los sellos de tiempo no deben emitirse.

6.1 EMISIÓN DE SELLOS DE TIEMPOS

La emisión de sellos de la TSA de INDENOVA S.L. es conforme al protocolo y el perfil definido en la norma ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

6.2 PETICIÓN DE UN SELLO DE TIEMPO

El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161 [6].

El protocolo para el envío de la petición de sello de tiempo al servicio será HTTP o HTTPS de acuerdo con la definición del apartado 3.4 del RFC 3161 [6].

Los algoritmos de resumen criptográfico aceptados por la TSA de LLEIDA.NET son: SHA-256, SHA512 y SHA-1. LLEIDA.NET desaconseja a sus subscriptores el uso de SHA-1 como algoritmo de resumen, que mantiene por motivos de compatibilidad.

6.3 RESPUESTA A UNA PETICIÓN DE SELLO DE TIEMPO

Los sellos de tiempo generados por la TSA se adecuan al perfil definido en el apartado 5.2 de ETSI EN 319 422 [5].

El algoritmo de resumen de los sello de tiempo es SHA-256.

El algoritmo de firma del sello de tiempo es sha256WithRSAEncryption.

El sello de tiempo incluye una extensión del tipo qcStatements con la declaración esi4qtstStatement-1 de acuerdo el apartado 9.1 de ETSI EN 319 422 para indicar que el sello de tiempo es cualificado.

El sello de tiempo incluye el certificado electrónico de la clave pública de firma de la TSU.

6.4 PERFIL DEL CERTIFICADO

El certificado de la TSU está emitido por la entidad de certificación LLEIDA.NET.

La duración del certificado es de 6 años y el certificado contiene la extensión PrivateKey Usage Period para especificar el periodo de uso de la clave privada a 5 años.

7 TARIFAS

Las tarifas por los servicios serán definidas en los contratos con las organizaciones clientes.

8 SINCRONIZACIÓN DEL RELOJ CON LA UTC

LLEIDA.NET adopta medidas para asegurar que su reloj es sincronizado con la UTC dentro de la exactitud declarada:

- La calibración de los relojes será monitoreada y mantenida de modo que no se desvíen de la precisión de +/- 1 segundo. Protegiendo el reloj de la TSU contra amenazas que podrían provocar un cambio no detectable luego de la calibración. Y monitoreando la exactitud declarada, para detectar cualquier desviación.

- En caso de desviación los terceros que confían afectados serán informados mediante una publicación en la página web de LLEIDA.NET o mediante correo electrónico a todos los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.

- Cuando un cambio en el tiempo sea notificado por una autoridad competente, los respectivos cambios serán realizados el último minuto del día cuando el cambio en el tiempo haya sido planificado para ocurrir. En este escenario se mantendrá un registro del tiempo exacto (dentro de la exactitud declarada) y será notificado a los terceros que confían mediante una publicación en la página web de LLEIDA.NET o mediante correo electrónico a todos los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.

9 Políticas de seguridad del servicio

El servicio y el sistema que la gestiona atiendo a los distintos aspectos de seguridad:

- Seguro

El sistema no permite los accesos no autorizados a la información, a través de la plataforma y de ataques directos sobre los servidores sobre los que funciona.

- Trazable

Todas las acciones de los usuarios que implican una modificación en un documento se registran.
En algunos servicios la auditoría de eventos se firma y sella con TSA para asegurar su autenticidad.

- Fidedigno

No se modifican los originales de los documentos

- Integridad

Las evidencias periciales generadas, no se modifican.

- Buenas prácticas de Seguridad de la Información

El Sistema de Gestión de los Servicio de Correo electrónico certificado es auditado periódicamente según los estándares de ISO 27001.

- Auditado

Además ser realizan revisiones técnicas y de Ethical Hacking acorde con OWASP.

10 Obligaciones

16.1 Obligaciones de la ECD Lleida.net

Obligaciones de la ECD Lleida.net

Lleida.net como entidad de prestación de servicios de certificación está obligada según normativa vigente en lo dispuesto en las Políticas de Servicio y en la DPC a:

1. Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.
2. Publicar la DPC y cada una de las Políticas de Servicio en la página Web de Lleida.net
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificado.
4. Mantener la DPC y Políticas de Servicio con su última versión publicadas en la página Web de Lleida.net.
5. Emitir el servicio conforme a las Políticas de Servicio y a los estándares definidos

16.2 OBLIGACIONES DE LOS SUSCRIPTORES

Es responsabilidad de los suscriptores utilizar una aplicación de software, que realice las peticiones e interprete las respuestas conforme al formato establecido en la RFC 3161, las verificaciones del estado del certificado, así como realizar la correcta configuración de la hora local en estas aplicaciones.
La emisión de sellos de la TSA es conforme al protocolo y el perfil definido en la norma ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
Petición de un sello de tiempo El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161.
El protocolo para el envío de la petición de sello de tiempo al servicio será HTTP o HTTPS de acuerdo con la definición del apartado 3.4 del RFC 3161.

16.3 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían son responsables de verificar que los documentos sean firmados con un sello de tiempo, con un certificado digital reconocido por LLEIDA.NET y que estos sellos tengan como parte de su número de identificación el OID.
Asimismo, deben verificar que el certificado de sello de tiempo se encuentra firmado y que la clave privada no estuvo comprometida en el momento en el que se realizó el sellado de tiempo.

17 Mapa de controles

Norma	Apartado
CEA- 3.0-07	10.11