| | |
|---|---|
| Proyecto | **Servicios de Valor Añadido (SVA) - Sistema de Intermediación Electrónica** |
| Título | **Declaración de Prácticas de Servicios de Valor Añadido (DPSVA)** |

| | | | |
|---|---|---|---|
| Realizado por | **LLEIDANET PKI SUCURSAL DE PERÚ** | | |
| Dirigido a | **Usuarios internos y externos** | | |
| Documento | **DOC-180219.1821910** | | |
| Fecha aprobación | **12/05/2025** | Revisión | **6** |

Firmado por: Sergio Belda Soler
Fecha firma: 16/05/2025 18:18:31 CEST

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

Avda. Santo Toribio Nº 143 Of. 38
San Isidro, Lima
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
**info@lleida.net**
**www.lleida.net**

# 1 DATOS DEL DOCUMENTO

| | |
|---|---|
| Proyecto | Servicios de Valor Añadido (SVA) - Sistema de Intermediación Electrónica |
| Título | Declaración de Prácticas de Servicios de Valor Añadido (DPSVA) |
| Código | DOC-180219.1821910 |
| Tipo de documento | DOC - Documento genérico |
| Clasificación del documento | Público |
| Realizado por | LLEIDANET PKI SUCURSAL DE PERÚ |
| Dirigido a | Usuarios internos y externos |
| Fecha aprobación | 12/05/2025 |
| Revisión | 6 |

# 2 HISTORIA DEL DOCUMENTO

| Revisión | Fecha | Motivo de la modificación | Responsable |
|---|---|---|---|
| 1 | 19/02/2018 | Creación del documento. | NG |
| 2 | 12/07/2018 | Modificación listado documentos | NG |
| 3 | 24/07/2018 | Modificación Servicio eSigna Firma Centralizada | NG |
| 4 | 20/07/2020 | Modificaciones menores | NG |
| 5 | 12/03/2024 | Actualización de funcionalidades | CJ |
| 6 | 12/05/2025 | Actualizar denominación a Lleidanet PKI Sucursal de Perú | Compliance (CJ) |

# 3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

| | |
|---|---|
| Elaborado por: | Nombre: Compliance (CJ)<br>Cargo: Responsable de Calidad<br>Fecha: 12/05/2025 |
| Revisado por: | Nombre: Lleidanet PKI (SB)<br>Cargo: Administrador del Servicio<br>Fecha: 12/05/2025 |
| Aprobado por: | Nombre: Lleidanet PKI (SB)<br>Cargo: Administrador del Servicio<br>Fecha: 12/05/2025 |

# 4 INTRODUCCIÓN

LLEIDANET PKI SUCURSAL DE PERÚ es una empresa trasnacional que nació con vocación de desarrollar, innovar y generar soluciones tecnológicas TIC en el ámbito empresarial e institucional. Está especializada en soluciones de firma electrónica, securización de archivos y comunicaciones y cifrado de datos, criptografía, movilidad, certificados digitales y procedimientos electrónico, invirtiendo en el desarrollo e implantación de las mismas el 95% de su actividad.

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

Junto a los servicios de valor añadido, LLEIDANET PKI SUCURSAL DE PERÚ brinda los servicios de certificación digital y registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales, al encontrarse acreditada como Entidad de Certificación y Entidad de Registro o Verificación.

El planteamiento es ofrecer una oferta diferenciada, generadora de soluciones y servicios innovadores, con el objetivo de crear valor. Para ello combinamos un alto grado de conocimiento de los directivos y profesionales, con su amplia experiencia en certificados digitales y firma electrónica para eCommerce y eAdministración y el uso de tecnología avanzada.

Nuestros SERVICIOS están dirigidos a la Administración Electrónica y Comercio electrónico y, en general, para proyectos de “oficina sin papeles”, tiene como componente central la Plataforma eSigna®, a partir del cual se apoyan el resto de nuestros productos y soluciones, entendidos como módulos independientes y a su vez interconectados, según las necesidades del proyecto a implantar.

# 5 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza LLEIDANET PKI SUCURSAL DE PERÚ para la administración de sus servicios como Prestador de Servicios de Valor Añadido – SVA, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI.

# 6 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación de LLEIDANET PKI SUCURSAL DE PERÚ cubre los sistemas de aplicaciones de software de trámite administrativo, el cual utiliza procesos de firma digital, autenticación y cifrado para resguardar la autenticidad, integridad y confidencialidad de las transacciones o trámites administrados: asimismo, la acreditación cubre las políticas y procedimientos necesarios para gestionar y proteger los servicios y sistemas de certificación digital.

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

Los clientes de LLEIDANET PKI SUCURSAL DE PERÚ que opten por obtener la solución acreditada deberán cumplir con los procedimientos y políticas normativas acreditadas que forman parte de su sistema de gestión y deberán ser sometidos a un proceso de actualización de acreditación. Serán los responsables de:

- Seguridad Física y del entorno.
- Manejo de medios y seguridad.
- Planificación de sistemas.
- Seguridad en redes.
- Monitoreo de sus servicios.

LLEIDANET PKI SUCURSAL DE PERÚ por su parte, realizará en este punto un monitoreo de que los clientes cumplen con las prácticas.

El Listado de las funcionalidades del Servicio de Valor Añadido que desea incluir en el alcance de la acreditación es el siguiente:

| Nº | Funcionalidad | Descripción | SI/NO |
|---|---|---|---|
| 1 | Notificaciones Electrónicas | Notificaciones Electrónicas. | SI |
| 2 | Carpeta Ciudadana | Domicilio Electrónico. | SI |
| 3 | Servicios de Sellado de tiempo | TSA | SI |
| 4 | eSigna RM | Archivo Electrónico. | SI |
| 5 | eSigna Batchserver | Solución automatizada masiva de firma electrónica de ficheros. | SI |
| 6 | eSigna Mobile | Servicio de movilidad. | SI |
| 7 | eSigna Viewer | Aplicación que le permite firmar y verificar cualquier tipo de edocumento | SI |
| 8 | eSigna Websecure | Servicio de identificación con certificados digitales en terceras plataformas. | SI |
| 9 | eSigna Website | API que permite integrar en terceras plataformas mecanismos de firma digital con certificados digitales. | SI |
| 10 | eSigna Printer | Servicio de Impresora virtual. | SI |
| 11 | eSigna BPM | Gestor de Expedientes. | SI |
| 12 | eSigna ECM | Gestor Documental (Plataforma). | SI |
| 13 | eSigna Designer | Diagramador de Procedimientos. | |
| 14 | Oficina de Atención al Ciudadano (OAC) | Oficina de Atención al Ciudadano (OAC). | SI |
| 15 | Oficina Virtual de Atención al Ciudadano (OVAC) | Oficina Virtual de Atención al Ciudadano (OVAC). | SI |
| 16 | eSigna Portafirmas | Portafirmas Electrónico. | SI |
| 17 | eSigna Portal Proveedor | Portal Proveedor: eFactura. | SI |
| 18 | eSigna Sede Electrónica | Sede Electrónica (Portal Ciudadano). | SI |
| 19 | Trámites | Sistema de Catalogación de trámites. | SI |
| 20 | eSigna DigitalScan | Digitalización Certificada de documentos. | SI |
| 21 | eSigna PKI | Plataforma PKI: emitir y gestionar los certificados de una organización. | SI |
| 22 | eSigna Firma Centralizada | Servicio de firma centralizada que permite almacenar los certificados de los usuarios en un servidor central HSM. | SI |
| 23 | eSigna Autoliquidaciones | Servicio para la generación de autoliquidaciones por parte del ciudadano y del personal de la organización | SI |
| 24 | eSignaBox | Plataforma en la nube para la firma e intercambio seguro de documentos y comunicaciones certificadas y/o cifradas. | SI |
| 25 | eSignaBox Mobile | Aplicación mobile en Android e iOS para el producto eSignaBox | SI |

| | | | |
|---|---|---|---|
| 26 | eSigna Maestros | Servicio que permite configurar los sistemas de información. | SI |
| 27 | eSigna Report | Servicio que permite asignar los diferentes informes de eSigna® Plataforma a los usuarios de la misma, además de publicarlos y visualizarlos | SI |
| 28 | Lleidanet Wallet | App móvil de gestión de identidades, passwords y firma electrónica | SI |

# 7 DEFINICIONES Y ABREVIACIONES

| | |
|---|---|
| Prestador de Servicios de Valor Añadido: | SVA: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE. |
| Servicios de valor añadido: | Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación. |
| Política de servicios de valor añadido: | Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida. |
| Suscriptor: | Entidad que requiere los servicios provistos por la SVA de LLEIDANET PKI SUCURSAL DE PERÚ y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento. |
| Tercero que confía: | Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas. |

# 8 PLATAFORMA ESIGNA®

La plataforma eSigna® es la base para la ejecución de los servicios de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ, contiene las librerías criptográficas que realizan los procesos autentificación, firma digital y cifrado, mediante el uso de certificados digitales de cualquier Entidad de Certificación, que utilice certificados digitales X.509.v3 y se encuentren publicados en la TSL del INDECOPI. Asimismo, realiza la respectiva verificación de estado de vigencia y confianza de cada certificado digital.

# 9 SERVICIOS DE VALOR AÑADIDO

LLEIDANET PKI SUCURSAL DE PERÚ implementa servicios de valor añadido dirigidos a la Administración Electrónica y, en general, para proyectos de "oficina sin papeles". Estos servicios se sostienen sobre aplicaciones de software y procesos de gestión diseñados para sustituir los procesos de trámite administrativo presencial por servicios que pueden ser atendidos en línea, tanto por parte de los clientes, ciudadanos, empleados, funcionarios y/o proveedores de una organización.

Las aplicaciones de software y los procesos de gestión son brindados a las personas jurídicas, en adelante organizaciones clientes, para ser utilizados en su operación administrativa diaria, en sus propias instalaciones y gestionados por su propio personal para atención de su propia comunidad de suscriptores. La base de estos servicios, es la utilización de la Plataforma eSigna® como componente central, a partir del cual se apoyan, a manera de módulos independientes y a su vez interconectados, según las necesidades del proyecto a implantar por cada organización cliente.

# 10 RESPONSABILIDADES DE LLEIDANET PKI SUCURSAL DE PERÚ

LLEIDANET PKI SUCURSAL DE PERÚ implementa las aplicaciones de software que sostienen los servicios de valor añadido, asimismo brinda directrices sobre la administración de estos servicios, los certificados digitales y los controles de seguridad que deben implementarse, así como las capacitaciones y asesoramiento requerido por cada cliente que debe adoptar los servicios de valor añadido dentro de su propia organización.

LLEIDANET PKI SUCURSAL DE PERÚ no proporciona la infraestructura de hardware, firmware, comunicaciones y ambiente donde deben ser ejecutadas las aplicaciones, estos deben ser provistos por cada organización cliente.

# 11 RESPONSABILIDADES DE LAS ORGANIZACIONES CLIENTES

Las organizaciones clientes deberán proveer toda la infraestructura de hardware, firmware, comunicaciones y entornos donde serán ejecutadas las aplicaciones que sostienen los servicios de valor añadido descritos en el presente documento. Asimismo, deberán cumplir con todas las directrices declaradas en el presente documento, respecto de la seguridad y adecuada gestión de los servicios y sus componentes. Cualquier cambio será comunicado al INDECOPI.

De igual modo, las organizaciones deberán someterse a la auditoría anual del INDECOPI, para la verificación del mantenimiento de la acreditación.

# 12 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE VAPS

LLEIDANET PKI SUCURSAL DE PERÚ administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la SVA.

Para cualquier consulta contactar:

- Dirección de correo electrónico: consultas@indenova.com

# 13 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Servicios de Valor Añadido de LLEIDANET PKI SUCURSAL DE PERÚ, la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección: http://www.indenova.com/acreditaciones/INDECOPI/SVA

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es autorizado y revisado por el Administrador de la SVA antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

# 14 SELLO DE TIEMPO

Los servicios de LLEIDANET PKI SUCURSAL DE PERÚ permiten la conexión con una Autoridad Emisora de Sellos de Tiempo (TSA), conforme a la elección de la organización cliente. Las aplicaciones validan el estado de vigencia, no revocación y confiabilidad de los certificados digitales de las TSA.

# 15 CONTROLES EN LAS INSTALACIONES, GESTIÓN Y OPERACIONALES

LLEIDANET PKI SUCURSAL DE PERÚ implementa en las aplicaciones los controles necesarios para garantizar la confiabilidad y autenticidad de la firma digital en los servicios de valor añadido. Esto implica controles de acceso a las aplicaciones, verificación de estado del certificado, generación de registros de eventos y transacciones, evaluación de vulnerabilidades de las aplicaciones y asimismo se somete ante el INDECOPI a auditorías periódicas

Corresponde a las organizaciones clientes, la implementación de los controles de seguridad de la infraestructura de hardware, firmware, comunicaciones, personal y ambiente.

Las medidas de seguridad adoptadas para proteger los servicios de valor añadido son señaladas en la Política de Seguridad de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ.

## 15.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

LLEIDANET PKI SUCURSAL DE PERÚ no proporciona los servicios de local o ambiente para brindar los servicios de valor añadido, éstos son implementados en el local de cada organización cliente.

Como parte de su papel de proveedor de servicios de valor añadido, LLEIDANET PKI SUCURSAL DE PERÚ establece políticas de seguridad física para proteger los sistemas donde se procesan los servicios de valor añadido.

Corresponde a las organizaciones clientes, la implementación de los controles de seguridad física.

## 15.2 ARCHIVO Y MEDIOS DE ALMACENAMIENTO

LLEIDANET PKI SUCURSAL DE PERÚ no proporciona los servicios de archivo para brindar los servicios de valor añadido, éstos son implementados en el local de cada organización cliente.

Como parte de su papel de proveedor de servicios de valor añadido, LLEIDANET PKI SUCURSAL DE PERÚ establece políticas de seguridad para proteger el archivo y los medios de almacenamiento donde se guarda la información generada en los servicios de valor añadido.

Corresponde a las organizaciones clientes, la implementación de los controles de seguridad del archivo y los medios de almacenamiento.

## 15.3 DEFINICIÓN Y ADMINISTRACION DE ROLES

Los roles necesarios para la administración y operación de los sistemas de firma digital, autenticación y cifrado son identificados, definidos y documentados. Los roles correspondientes al personal de LLEIDANET PKI SUCURSAL DE PERÚ son asignados y esta asignación es documentada.

Corresponde a las organizaciones clientes, la asignación de roles a su personal de confianza.

Las aplicaciones permiten separar los roles que son incompatibles, separando los derechos de acceso. La definición de roles incluye la determinación de roles incompatibles y el número de personas requeridas por labor.

Los roles que tienen acceso a información sensible son autenticados mediante el uso de certificados digitales de atributos, con credenciales de dominio o con usuario y contraseña.

El perfil de cada usuario incluye su identificación, el "mapa" de los SERVICIOS y las vistas que tiene asignadas y el trazado de su actividad en cuanto a uso y demanda de SERVICIOS, vistas y contenidos.

Existe la figura del administrador de la plataforma, el cual será el encargado de gestionar los usuarios, perfiles y SERVICIOS disponibles (como el Gestor de expedientes, Oficina de Atención al Ciudadano, Portafirmas, etc.).

## 15.4 SEGURIDAD DEL PERSONAL

El personal de LLEIDANET PKI SUCURSAL DE PERÚ está calificado respecto de conocimientos y experiencia de acuerdo a su rol. Asimismo, se realiza la verificación de no existencia de antecedentes criminales antes de tener acceso a los sistemas e información empresarial de los proyectos de las Organizaciones Clientes.

Los roles que tienen acceso a información sensible son conscientes de su responsabilidad y están comprometidos a su protección mediante convenios de confidencialidad con valor contractual.

Todos los empleados de LLEIDANET PKI SUCURSAL DE PERÚ que participan de la administración y desarrollo de los servicios de la SVA reciben capacitaciones periódicas sobre tecnología, políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Las capacitaciones incluyen los siguientes temas:

- El equipo y software requerido para operar.
- Requisitos legislativos en relación a sus funciones.
- Los aspectos de la CAPS, Política de Seguridad, Política de Privacidad y otra documentación relevante que afecte sus funciones.
- Sus roles en relación al plan de continuidad y recuperación de desastres.

No se realiza rotación del personal en la operación y administración de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ.

En el caso de una acción real o potencial no autorizada, que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona será inmediatamente suspendida de todo rol de confianza que pudiera desempeñar. Dicha sanción está establecida en el contrato de cada empleado y/o contratista que participa de la administración de la SVA.

El personal recibe periódicamente la documentación necesaria para el desempeño de sus funciones:

- Una declaración de funciones y autorizaciones.

- Manuales para los equipos de software que deben de operar.
- Aspectos de la CAPS, política de seguridad y otra documentación relevante en relación a sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencias.

## 15.5 GENERACIÓN DE REGISTROS

Se registran todos los eventos significativos de seguridad, incluyendo en cada registro la fecha y hora exacta de su realización, la cual no debe estar posibilitada de ser eliminada ni modificada del registro.

Los sistemas permiten la generación de los siguientes registros:

a) Intentos fallidos y exitosos de inicializar un usuario, renovar, habilitar, deshabilitar y actualizar o recuperar usuarios.
b) Intentos fallidos o exitosos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema, intentos de entrada y salida del sistema.
c) Intentos no autorizados de acceso a los registros o bases de datos del sistema.
d) Encendido y apagado del sistema principal.

El registro de auditoria de eventos debe registrar la hora, fecha e identificadores software y hardware.

Los registros generados durante la ejecución de los servicios, como son los cambios en la configuración, el personal e incidentes de acceso físico, deben ser gestionados por las organizaciones cliente que utiliza los sistemas de la SVA.

Compete a las organizaciones cliente la revisión, mantenimiento y protección del archivo de registros, así como los procesos de auditoría de estos registros.

## 15.6 EVALUACIÓN DE VULNERABILIDADES

Las versiones de las aplicaciones de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ han sido sometidas a la evaluación Common Criteria EAL1. El certificado y el informe correspondiente se encuentran publicados en la siguiente dirección:

http://www.indenova.com/

## 15.7 PROTECCIÓN DEL ARCHIVO

LLEIDANET PKI SUCURSAL DE PERÚ no proporciona los servicios de protección del archivo para brindar los servicios de valor añadido, éstos son implementados en el local de cada organización cliente.

Corresponde a las organizaciones clientes, la implementación de los controles de seguridad del archivo de documentos y evidencias generadas.

## 15.8 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

LLEIDANET PKI SUCURSAL DE PERÚ proporciona servicios de soporte de segundo nivel para la gestión de incidentes y recuperación de los sistemas de software que sustentan los servicios.

Corresponde a las organizaciones clientes, la implementación del Plan de Contingencias para el soporte del primer nivel y la recuperación en caso de incidentes en la infraestructura de hardware, firmware, comunicaciones y entorno.

# 16 GESTIÓN DE CICLO DE VIDA DE LAS CLAVES: (SISTEMAS AUTOMATIZADOS)

En relación a los controles de seguridad (generación e instalación de par de claves, protección de clave privada y controles de ingeniería de los módulos criptográficos, datos de activación, controles técnicos de ciclo de vida, ...) se encuentran ampliamente desarrollados en la Declaración de Prácticas de la EC acreditada por LLEIDANET PKI SUCURSAL DE PERÚ ante el INDECOPI.

## 16.1 GENERACIÓN DE LAS CLAVES

La Generación de las claves de firma del sistema automatizado deberá ser realizada en un ambiente asegurado físicamente, por personal que ocupa roles de confianza, bajo al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

La generación de la clave de firma del sistema automatizado deberá ser realizada en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

El algoritmo de generación, la longitud de la clave firma y el algoritmo de firma usado para firmar los sellos de tiempo deberán ser reconocidos por la IOFE.

## 16.2 PROTECCIÓN DE LA CLAVE PRIVADA

La clave privada de firma permanece confidencial y que se mantiene su integridad. La clave de firma del sistema automatizado estará protegida en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o,
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

Si se realiza un respaldo de la clave de firma, esta deberá ser copiada, almacenada y recuperada sólo por personal que ocupa roles de confianza, usando al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo.

## 16.3 DISTRIBUCIÓN DE LA CLAVE PUBLICA

La clave pública de firma debe ser disponible para los terceros que confían en un certificado de clave pública.

El certificado puede ser emitido por la misma entidad que opera el SVA o por otra EC reconocida por la IOFE.

El certificado debe ser emitido por una EC bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA.

Este certificado deberá ser reconocido por la IOFE.

## 16.4 RE-EMISIÓN DE LA CLAVE

El tiempo de vigencia del certificado no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento de la IOFE.

## 16.5 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA

Las claves privadas no pueden ser usadas tras la expiración de su ciclo de vida:

a. Se establecen procedimientos técnicos u operacionales para asegurar que son generadas y utilizadas nuevas claves.
b. La clave privada de firma, o cualquier parte de la clave será destruida de tal modo que no pueda ser recuperada.

c. El sistema de generación de sellos de tiempos debe rechazar cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado o se encuentra revocada.

## 16.6 CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

Durante la Gestión del ciclo de vida del módulo criptográfico se cumple que:

- El hardware del módulo criptográfico no debe ser manipulado durante su transporte.
- El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento.
- La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro.
- El hardware de firma de sellos de tiempo funciona correctamente.
- Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado.

# 17 AUTENTICACIÓN

Las funciones de validación de identidad de sus usuarios mediante un certificado digital son las siguientes:

- Validación de la confiabilidad de la raíz: El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.
- Validación del estado de revocación: El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.
- Validación del estado de vigencia: El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.
- Validación del propósito: El sistema deberá verificar que el certificado del usuario final tiene como propósito autenticación, conforme a la RFC 5280.

## 17.1 CERTIFICADOS DE AUTENTICACIÓN

La PSVA puede emitir certificados de autenticación para ser utilizados por sus usuarios en la operación de los servicios de valor añadido.

Para emitir los certificados, la PSVA debe utilizar los servicios de una EC acreditada o reconocida por la IOFE.

Las solicitudes de emisión, revocación, re-emisión, suspensión o modificación deben ser realizadas a través de una Entidad de Registro o de un Canal Seguro de Registro y Distribución de Certificados Digitales acreditados por la AAC.

Al retirarse una persona del campo de usuarios de los servicios de valor añadido, su certificado digital debe ser revocado o suspendido en función del periodo de tiempo definido para su retiro. Ninguna persona jurídica podrá guardar claves privadas de sus suscriptores, a menos que pueda garantizar que en ningún momento la clave privada podrá ser usada sin la autorización exclusiva del suscriptor. La persona jurídica no podrá guardar copias de las claves privadas de los suscriptores en formatos .PFX o PKCS#7.

# 18 CIFRADO

Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.

El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.

El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.

El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.

El sistema deberá verificar que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.

# 19 CANALES SSL

Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.

El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.

El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.

El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado. Así como que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.

# 20 CONTROL DE CAMBIOS

Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del SVA, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.

LLEIDANET PKI SUCURSAL DE PERÚ realiza la gestión de cambios siguiendo el procedimiento interno PR-032 Gestión de comunicaciones y operaciones. En este se describen los tipos de cambios, la gestión de los mismos y los controles a tener en cuenta.

# 21 POLÍTICA DE PRIVACIDAD

La SVA brinda sus servicios a personas jurídicas y no tiene acceso a la información personal proporcionada por los suscriptores de los servicios de valor añadido.

LLEIDANET PKI SUCURSAL DE PERÚ no se responsabiliza por la información que los suscriptores entregan a las organizaciones clientes. Corresponde a las organizaciones clientes, la implementación de controles para la protección de los datos personales de sus suscriptores.

# 22 CONFIDENCIALIDAD DE LA INFORMACIÓN DE NEGOCIO

Todo el personal de LLEIDANET PKI SUCURSAL DE PERÚ que participa de la administración de los sistemas de la SVA, ha firmado un Convenio de Confidencialidad para proteger la información confidencial de los proyectos de las organizaciones clientes.

La información crítica y sensible, que es archivada y protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizados.

En particular se protege la siguiente información:

- Material comercialmente reservado de la SVA, de las organizaciones cliente, incluyendo términos contractuales, planes de negocio y propiedad intelectual;

- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y/o terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los usuarios, titulares o terceros que confían.
- Información que pudiera perjudicar la normal realización de las operaciones de la SVA

# 23 DERECHOS DE PROPIEDAD INTELECTUAL

La totalidad de los componentes de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ, es decir, aplicaciones, políticas, procedimientos, sitios web, diagramas, textos, imágenes, ficheros, fotografías, logotipos, gráficos, marcas, iconos, combinaciones de colores, o cualquier otro elemento, su estructura y diseño, la selección y forma de presentación de los materiales, links y demás contenidos audiovisuales o sonoros, así como su diseño gráfico y códigos fuentes necesarios para su funcionamiento, acceso y utilización, están protegidos por derechos de propiedad industrial e intelectual, titularidad de LLEIDANET PKI SUCURSAL DE PERÚ, sin que puedan entenderse cedidos los derechos de explotación sobre los mismos más allá de lo estrictamente necesario para su correcto uso.

En particular, quedan prohibidas la reproducción, la transformación, distribución, comunicación pública, puesta a disposición del público y en general cualquier otra forma de explotación, por cualquier procedimiento, de todo o parte de los contenidos de los componentes de la SVA, así como de su diseño y la selección y forma de presentación de los materiales incluidos en la misma. Estos actos de explotación sólo podrán ser realizados si media la autorización expresa de LLEIDANET PKI SUCURSAL DE PERÚ.

Queda asimismo prohibido descompilar, desensamblar, realizar ingeniería inversa, sublicenciar o transmitir de cualquier modo, traducir o realizar obras derivadas de los programas de ordenador necesarios para el funcionamiento, acceso y utilización de las aplicaciones y de los servicios en él contenidos, así como realizar, respecto a todo o parte de tales programas, cualesquiera de los actos de explotación descritos en el párrafo anterior. El usuario del sitio web deberá abstenerse en todo caso de suprimir, alterar, eludir o manipular cualquier dispositivo de protección o sistemas de seguridad que puedan estar instalados en el mismo.

# 24 POLÍTICA DE REEMBOLSO

Las condiciones de reembolso serán definidas con cada organización cliente en los respectivos contratos con la SVA.

# 25 RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS

La cobertura de seguro, las provisiones de garantía y responsabilidad, así como las indemnizaciones son definidas en los contratos con las organizaciones clientes.

# 26 ENMENDADURAS

Los procedimientos para la resolución de enmendaduras serán definidas en los contratos con las organizaciones clientes.

# 27 RESOLUCIÓN DE DISPUTAS

Los procedimientos para la resolución de disputas serán definidas en los contratos con las organizaciones clientes.

# 28 ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad serán definidas en los contratos con las organizaciones clientes.

# 29 FUERZA MAYOR Y OTRAS PROVISIONES

Las cláusulas de fuerza mayor y otras provisiones aplicables a la entrega de los servicios de valor añadido serán definidas en los contratos con las organizaciones clientes.

# 30 TARIFAS

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

# 31 FINALIZACIÓN DE LA SVA

Antes de que la SVA termine sus servicios realizará las siguientes medidas:

- Con 30 días de anticipación se informará a todos las organizaciones clientes y suscriptores, la finalización de las operaciones de la SVA.
- Se pondrá a disponibilidad de todas las organizaciones cliente la información concerniente a su terminación y las limitaciones de responsabilidad
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre de la SVA
- Se mantendrán o transferirán a los terceros que confían sus obligaciones de verificar los documentos generados.
- Las claves privadas de la SVA, incluyendo copias, serán destruidas de manera segura de modo que no pueda ser recuperada
- Se tomarán medidas para que los certificados de la SVA sean revocados
- Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de las organizaciones cliente. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.

# 32 AUDITORÍA

LLEIDANET PKI SUCURSAL DE PERÚ se somete a servicios de auditoría periódica por parte del INDECOPI para el mantenimiento de la acreditación de la SVA. Se seleccionará a un auditor del listado proporcionado por el INDECOPI.

El auditor debe:

- Ser autorizado por la AAC.
- Ser independiente del PSVA, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.

Dentro de esta revisión anual se realizará un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del SVA, para asegurar que dichos requerimientos son considerados en los sistemas críticos.

# 33 CONFORMIDAD CON LA LEY APLICABLE

LLEIDANET PKI SUCURSAL DE PERÚ es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales, para el reconocimiento legal de los sellos de tiempo emitidos bajos las directrices definidas en el presente documento.

# 34 BIBLIOGRAFÍA


a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley N°27269 y sus modificaciones posteriores Ley N°27310.
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011