Proyecto	**Servicios de Valor Añadido – Sistema de Intermediación Electrónica**
Título	**Política de Seguridad**

Realizado por	**InDenova**		
Documento	**DOC-200216.2093016**		
Fecha	**30/09/2020**	**Versión**	**1**

Dels Traginers, 14 - 2°B
Pol. Ind. Vara de Quart
46014 Valencia
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
indenova@indenova.com
http://www.indenova.com

Historia del documento

Revisión	Fecha	Motivo de la modificación	Responsable
1	30/09/2020	Creación del documento	Indenova S.L. - SBS

1 INTRODUCCIÓN

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

Como Prestador de Servicios de Valor añadido - SVA, INDENOVA S.L. 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, INDENOVA S.L. 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.

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.

2 OBJETIVO

Este documento tiene como objeto el establecimiento de directrices de protección de privacidad de datos personales para la gestión de los servicios de la SVA de INDENOVA, en el marco del cumplimiento de los requerimientos del "Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014" o también como es conocido "Reglamento eIDAS" establecida por el Parlamento Europeo y del Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

3 OBJETO DE LA ACREDITACIÓN

INDENOVA S.L. provee las herramientas de software, así como las políticas y procedimientos de gestión de los servicios y sistemas de certificación digital, no así la infraestructura de hardware y ambientes, como centros de datos y servidores. En este sentido, la Política de Seguridad establece los requerimientos que cumple el Sistema de Gestión de los Servicios de Valor Añadido sobre la base de la plataforma eSigna®.

Los clientes de INDENOVA S.L. 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. En este sentido al no brindar INDENOVA S.L. los servicios de alojamiento los siguientes aspectos serán a cargo del Cliente: Seguridad Física; Seguridad de Comunicaciones y redes; Mantenimiento del equipo y su dese cho; Control de cambios y su configuración; Auditorias y detección de intrusiones y Medios de almacenamiento.

4 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 el Organismo supervisor.
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 INDENOVA S.L. y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía:	Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas.

5 ALCANCE

La presente política es de cumplimiento obligatorio para el personal y terceros subcontratados por INDENOVA S.L. que participan de las operaciones críticas de los servicios de valor añadido conforme a las responsabilidades especificadas en las siguientes secciones.

6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los sistemas y aplicaciones de INDENOVA S.L. deben asegurar la integridad y autenticidad de los servicios de valor añadido, implementando herramientas de firma digital confiables y controles de acceso y auditoría conformes con la regulación vigente, dotando a las organizaciones cliente de las herramientas necesarias para proteger las transacciones de firma digital y la información procesada.

INDENOVA S.L. 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.

7 VERIFICACIÓN DE CERTIFICADOS

Antes de permitir la realización de los procesos de firma digital, autenticación o cifrado, las aplicaciones deben realizar de manera automática lo siguiente:

- Validar que el certificado no se encuentre revocado – mediante CRL u OCSP.

- Validar que la vigencia del certificado no haya expirado.
- Validar que el certificado se encuentre en la Lista de Prestadores de Servicios de Confianza.
- Validar que el certificado es aplicable para la transacción a realizar: firma digital, autenticación o cifrado.
    - Un certificado de cifrado no podrá ser usado para realizar firma digital o autenticación.

8 SELLO DE TIEMPO

Los servicios de INDENOVA S.L. permiten la conexión con una Autoridad Emisora de Sellos de Tiempo (TSA), conforme a la elección de la organización cliente.

Antes de agregar el sello de tiempo al documento, las aplicaciones deben realizar de manera automática lo siguiente:

- Validar que el certificado de la TSA no se encuentre revocado – mediante CRL.
- Validar que la vigencia del certificado de la TSA no haya expirado.
- Validar que el certificado de la TSA se encuentre en la Lista de Prestadores de Servicios de Confianza.
- Validar que el certificado es aplicable para la firma de sellos de tiempo.

Las aplicaciones validan el estado de vigencia, no revocación y confiabilidad de los certificados digitales de las TSA.

9 VERIFICACIÓN DE CERTIFICADOS POR PARTE DE LOS TERCEROS

Cada vez que se realiza una transacción de firma digital, las aplicaciones deben generar registros firmados digitalmente que puedan ser verificados por los terceros que confían:

- El certificado no se encuentra revocado.
- El certificado no se encuentra expirado.
- El certificado es confiable (está incluido en la TSL).
- Fecha y hora de la transacción.

10 DEFINICIÓN Y ADMINISTRACION DE ROLES

Los roles necesarios para la administración y operación de los sistemas de firma digital, autenticación y cifrado deben ser identificados, definidos y documentados. Los roles correspondientes al personal de INDENOVA S.L. deben ser asignados y esta asignación es documentada.

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

Las aplicaciones deben permitir la separación de los roles que son incompatibles, separando los derechos de acceso. La definición de roles debe incluir la determinación de roles incompatibles y el número de personas requeridas por labor.

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

El perfil de cada usuario debe incluir 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.

El administrador de la plataforma será el encargado de gestionar los usuarios, perfiles y SERVICIOS disponibles (como el eSigna© BPM, eSigna© Oficina de Atención al Ciudadano, eSigna© Portafirmas, etc.).

11 SEGURIDAD DEL PERSONAL

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

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

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

Las capacitaciones deben incluir los siguientes temas:

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

No se realiza rotación del personal en la operación y administración de la SVA de INDENOVA S.L.

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 deberá ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar. Dicha sanción deberá estar 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 VAPS, política de seguridad y otra documentación relevante, en relación con sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencias.

12 CONTROLES DE ACCESO

De acuerdo a los perfiles establecidos, las aplicaciones deben controlar el acceso a la información sensible. Se debe realizar el control de acceso a la plataforma, expedientes y documentos mediante perfiles, certificados digitales e identificación con usuario y contraseña, LDAP, o mediante usuario y contraseña.

La Plataforma web debe permitir el acceso unificado para todos los SERVICIOS.

Para asegurar la confidencialidad de las comunicaciones, deben realizarse sistemas de cifrado de información mediante certificados digitales.

En la Sede Electrónica debe de estar configurado el protocolo de conexión segura en Internet (SSL) con un Certificado digital apropiado, generado por una AC, proporcionado por la Administración, permitiendo disponer de una dirección "https://" para garantizar la integridad y veracidad de la información y, por tanto, brindar las máximas garantías de seguridad. Por otro lado, los servidores web a los que se accederá desde Internet deberán estar ubicados en la DMZ o zona aislada de la red interna del proveedor de servicios y se deberán conectar a los servidores internos, mediante conexiones seguras SSL y webservices seguros, para el intercambio y acceso a la información y documentación.

13 CONTROLES DE DESARROLLO

Se deben adoptar las prácticas del estándar conforme con la Norma ISO/IEC 33000 e ISO/IEC 12207, para la mejora y evaluación de los procesos de desarrollo y mantenimiento de los sistemas de información y software de la SVA (en la actualidad, estamos pendientes de recepción del certificado una vez completado el proceso de renovación y paso a nivel 3 con éxito).

14 GENERACIÓN DE REGISTROS

Se deben registrar 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 deben permitir 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 auditoría 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.

El sistema debe disponer de un motor de logs, basado en la plataforma LOG4J para la creación de logs personalizados, mediante la edición de un fichero TXT de recursos. A fin de lograr la creación de logs diferenciados con diferentes niveles de reporte de errores (ERROR, WARNING, INFO, APLICACIÓN, etc.).

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

15 EVALUACIÓN DE VULNERABILIDADES

Las versiones de las aplicaciones de la SVA de INDENOVA S.L. han sido sometidas a la evaluación Common Criteria EAL1. El certificado se encuentra publicado en la siguiente dirección:

https://www.indenova.com/

16 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

INDENOVA S.L. 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.

17 EVALUACIÓN DE RIESGOS

Definición del alcance del área o proceso a evaluar. Identificación y valoración de los activos que corresponden al alcance. Identificación de amenazas y vulnerabilidades de los activos críticos. Evaluación del impacto de los riesgos. Tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos que conforman los servicios de valor añadido del SVA.

INDENOVA S.L. realiza la evaluación de riesgos siguiendo el procedimiento interno *PR-038 Procedimiento de Análisis de riesgos de la seguridad de la información.* Este proceso está basado siguiendo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) en su versión 3.

18 AUDITORÍA

INDENOVA se debe someter a procesos de auditoría periódica por parte del organismo de evaluación de la conformidad para el mantenimiento de la acreditación de la SVA.

19 REVISIÓN, ACTUALIZACIÓN Y PUBLICACIÓN DEL PLAN

La Política de Seguridad, Política de Privacidad y el Plan de Privacidad serán revisados y actualizados al menos una vez por año.

Así mismo, se publicará en la web de INDENOVA dicho diagrama para conocimiento público (https://www.indenova.com/acreditaciones/eidas/).

20 RESPONSABILIDADES DE INDENOVA

El "*Responsable de Seguridad de la información y Privacidad de los Datos*" de INDENOVA S.L. gestiona la implementación y vela por el cumplimiento del presente plan, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

21 CONFORMIDAD

Este documento ha sido aprobado por el "*Responsable del Prestador de Servicios de Valor Añadido"* de INDENOVA S.L., y tiene carácter normativo sobre todos los servicios de valor añadido, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Dentro del organigrama, se define la estructura o comisión encargada de la implementación de la SVA.