10011
110000011
001011
010110110
1010001
010

inDenova

Portafirmas electrónico
Sede electrónica
Gestión de expedientes
Portal del proveedor

Movilidad con firma electrónica
Facturación electrónica
Gestión documental
Digitalización certificada

Proyecto	**Servicios Cualificados de Validación de Firmas y Sellos Electrónicos**
Título	**Declaración de Practicas SVA - Servicios Cualificados de Validación de Firmas y Sellos Electrónicos (DPSVA)**

Realizado por	**INDENOVA S.L.**		
Documento	**DOC-200216.2140915**		
Fecha	**31/05/2021**	Versión	**2**

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-1140/2011

AENOR ER Madurez Software 3 ISO/IEC 33000 NMS-0009/2012

AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0024/2013

CERTIFIED IQNet MANAGEMENT SYSTEM ES-1140/2011

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	09/04/2021	Creación del documento.	Indenova S.L.
2	31/05/2021	Nueva ceremonia de claves de la PKI	Indenova S.L.

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 electrónicos, 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 REFERENCIAS

[DPSVA] - Declaración de Practicas SVA - Servicios Cualificados de Validación de Firmas y Sellos Electrónicos (DPSVA) (https://www.indenova.com/acreditaciones/eidas/)

[ETSI EN 319 401] - General Policy Requirements for Trust Service Providers

[ETSI EN 319 411-1] - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI TS 119 431-1] - TSP service components operating a remote QSCD / SCDev

[ETSI TS 119 441] - Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

[CEN EN 419 241-1]: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 733, v.1.6.3, v1.7.4 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

- Anexo A de la ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

- ETSI TS 102 778, v 1.2.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic - Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation.

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

- ETSI TS 101 861 V1.3.1 Time stamping profile.

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).

ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

3 DEFINICIONES Y ABREVIACIONES

A las definiciones dispuestas en la DPSVA, para la interpretación del presente documento se añaden los siguientes términos y abreviaturas tal y como se definen en ETSI TS 119 431-1:

- 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
- Identificación electrónica (eid): 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.
- Referencia a medios de identificación electrónica: datos usados en el ssasc como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.
- Servicio de confianza: servicio electrónico consistente en la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo, servicios de entrega electrónica certificada y certificados de estos servicios; o la creación, verificación y validación de certificados para la autenticación de sitios web; o la preservación de firmas, sellos o certificados electrónicos.
- Proveedor de servicios de confianza (TSP): entidad que provee de servicios de confianza.
- Dispositivo cualificado de creación de firma / sello electrónico (qscd): dispositivo de creación de firma que cumple con los requisitos del anexo ii del reglamento(eu) no 910/2014.
- Dispositivo remoto de creación de firma: dispositivo de creación de firma utilizado a distancia por el firmante y operado en su nombre bajo su control exclusivo de uso.
- Proveedor del servicio de validación de firma (SVSP): TSP que opera un SVS.
- SVS: Servicio de Validación de Firmas.
- Proveedor del Servicio Cualificado de Validación de Firma (QSVSP): TSP que opera un SVS.
- Dispositivo de creación de firma (SCDev o SCD): un equipo o programa informático configurado que se utiliza para crear una firma electrónica.
- SAD Signature Activation Data SAM Signature Activation Module SAML Security Access Markup Language SCA Signature Creation Application SCAL Sole Control Assurance Level SCAL1 Sole Control Assurance Level 1
- SCASC Signature Creation Application Service Component SCDev Signature Creation Device SCS Signature Creation Service SCSP Signature Creation Service Provider SD Signer's Document SDO Signed Data Object
- SSA Server Signing Application SSASC Server Signing Application Service Component TSP Trust Service Provider

4 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza INDENOVA S.L. para la administración de sus servicios como Prestador Cualificado de Servicios de Confianza, 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.

5 OBJETO

INDENOVA S.L., es un Prestador cualificado de Servicios de Confianza de conformidad con el Reglamento (UE) No 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 eIDAS).

Este documento contiene la Política y Declaración Prácticas Servicios Cualificados de Validación de Firmas y Sellos Electrónicos.

- La validación de firmas electrónicas y sellos cualificados en concordancia con la Regulación 910/2014, permitiendo asegurar la validación a largo plazo de las firmas electrónicas incrustadas en el documento, según la especificación EN 319 102-1 y ETSI TS 119 101 Este documento define los formatos de las firmas/sellos electrónicos admitidos, los protocolos e interfaces del servicio y la relación con servicios cualificados externos como CRL, OCSP, TSA). Este servicio valida los aspectos técnicos de la firma/sello electrónico cualificado recibido, pero no su aplicabilidad para diferentes propósitos de negocio (como por ejemplo legalidad de la firma para el acto realizado, apoderamiento de la persona).

El presente documento es un documento público que su contenido es de acuerdo a la especificación técnica de la ETSI TS 119 441 (y en concreto en el Anexo A) y define las políticas y prácticas en la provisión de los servicios de validación de firmas/sellos electrónicos cualificados.

6 RELACIÓN ENTRE EL TSP Y EL SERVICIO DE VALIDACIÓN DE FIRMA Y SELLOS ELECTRÓNICOS

INDENOVA SL es un proveedor de servicios de confianza cualificado que emite certificados y sellos electrónicos cualificados de acuerdo con la legislación vigente.

El servicio de SVS forma parte de los servicios operados por INDENOVA SL y permite prestar el servicio de validación de firma y sellos electrónicos a los firmantes que cuentan con un certificado electrónico definido en la Declaración de Prácticas de Certificación.

En el presente documento INDENOVA SL es identificado como el QSVSP.

7 DISPOSICIONES GENERALES DE LA POLÍTICA Y DE LA DECLARACIÓN DE PRÁCTICAS

INDENOVA S.L. en la prestación de su servicio de validación de firma y sellos electrónicos emplea dispositivos criptográficos de creación y protección de firmas catalogados como cualificados (QSCD) de conformidad con el Reglamento (UE) No 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 eIDAS).

Los HSM son operados de acuerdo con su certificación FIPS 140-2 y/o Common Criteria EAL 4+ y la solución SSASC empleada está alineada con los requisitos de seguridad definidos en la norma EN 419 241-1 para poder actuar como un Trustworthy System Supporting Server Signing (TW4S) con Sole Control Level 2 (SCAL2).

8 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

INDENOVA S.L. administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la SVA.

Para cualquier consulta contactar:

Nombre: INDENOVA S.L.
Dirección: Carrer Dels Traginers, 14 - 2° B C.P 46014, Valencia, España
Tel: (+34) 96 381 99 47
Correo electrónico: consultas@indenova.com
Página Web: www.indenova.com

9 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Este documento es la "Política y Declaración Prácticas Servicios Cualificados de Validación de Firmas y Sellos Electrónicos" de INDENOVA S.L.

1. En concordancia con ETSI EN 319 441 el servicio validación de firmas electrónicas tiene asignado el OID 1.3.6.1.4.1.49959.1.5.2, siguiendo lo indicado para servicios cualificados de validación de firmas electrónicas y sellos electrónicos tal como se define en los artículos 32 y 33 del Reglamento UE 910/2014 (EIDAS), con el OID OID 0.4.0.19441.1.2. Lo cual significa que este servicio cumple con el documento ETSI TS 119 441 y que el servicio es cualificado.

INDENOVA S.L. revisa periódicamente la conformidad de sus políticas con respecto a la especificación ETSI TS 119 431-1 y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 de dicha especificación.

La Declaración de Prácticas de Servicios de Valor Añadido de INDENOVA S.L., la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección: https://www.indenova.com/acreditaciones/eidas/

Los miembros de la Comunidad Electrónica y los Usuarios de los servicios tienen la obligación comprobar regularmente los documentos declarativos correspondientes (Políticas y/o Prácticas de Certificación de aplicación), solicitando cuanta información consideren oportuna a INDENOVA S.L.

No obstante, de cara a facilitar a los Usuarios destinatarios (Entidad usuaria y Suscriptor) el conocimiento de la existencia de novedades, cuando las modificaciones practicadas en cualquiera de las Declaraciones de Prácticas de Certificación y Políticas de Certificación afecten directamente a los derechos y obligaciones de las partes integrantes de la Comunidad Electrónica, o bien restrinjan el ámbito de aplicación de los Certificados, INDENOVA S.L. notificará a los interesados con una antelación mínima de treinta (30) días a la entrada en vigor de los cambios, con la finalidad que los miembros de la Comunidad Electrónica adopten la decisión que a su derecho convenga. INDENOVA S.L. no asumirá ningún compromiso indemnizatorio por las modificaciones o supresiones operadas en la Declaración en el ejercicio de sus derechos como Prestador de Servicios Certificación.

Las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por la Comisión de Seguridad de la SVA de INDENOVA S.L. antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores de INDENOVA S.L., así como la Declaración de Prácticas de la SVA con las que tiene filiación serán accesibles también para las personas con discapacidad y estos serán publicados en la siguiente dirección:

https://www.indenova.com/acreditaciones/eidas/

10 PKI PARTICIPANTES

10.1 ENTIDAD DE CERTIFICACIÓN INDENOVA S.L. (EC INDENOVA S.L.)

INDENOVA S.L., en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

10.2 ENTIDAD DE REGISTRO INDENOVA S.L. (ER INDENOVA S.L.)

INDENOVA S.L., brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

Las funciones de ER podrán ser tercerizadas. En este caso la ER de INDENOVA S.L. evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento a dicho tercero.

La ER puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la ER, siempre que se asegure la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión (lo cual se realiza a través de nuestra plataforma de PKI. Sin embargo, la responsabilidad legal frente al Organismo de supervisión, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. El tercero debe garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión, durante la ejecución de las actividades de tercerización, quedando claro que ante el Organismo de supervisión el responsable ante terceros es la ER.

Cabe indicar que INDENOVA S.L. suministra al tercero la Plataforma de ER para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma eSignaPKI con el certificado digital del operador.

10.3 PROVEEDOR DE SERVICIO CUALIFICADO DE VALIDACIÓN DE FIRMAS Y SELLOS (INDENOVA S.L.)

INDENOVA S.L. actúa como proveedor del servicio de validación de firmas y sellos electrónicos y no delega ninguna parte del servicio a entidades terceras.

10.3.1 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en la DPC de INDENOVA S.L.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por INDENOVA S.L. conforme lo establecido en la Política de Certificación.

10.3.2 SUSCRIPTOR

El Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

10.3.3 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la DPC de INDENOVA S.L.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

10.3.4 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación INDENOVA S.L. a un titular. El Tercero que confía, a su vez puede ser o no titular.

10.3.5 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

10.3.6 OTROS PARTICIPANTES

10.3.6.1 EL COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación INDENOVA S.L., conformado por el Directora de RRHH y Organización, Director de Operaciones, Coordinador Técnico, Responsable del SGSI y el Administrador del Sistema y tiene entre otras

funciones la aprobación de la DPC como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la DPC aprobada y autorizar su publicación. El Comité de Seguridad es el responsable de integrar la DPC, a la DPC de terceros prestadores de servicios de certificación.

11 PRÁCTICAS DEL PROVEEDOR DE SERVICIOS CUALIFICADOS DE VALIDACIÓN DE FIRMAS Y SELLOS ELECTRÓNICOS

La Plataforma de Validación de firmas y sellos electrónicos de INDENOVA S.L. responde al Servicio Cualificado de validación de Firmas electrónicas y sellos electrónicos, certificado bajo reglamento eIDAS, que permite generar las correspondientes evidencias de validación de certificados cualificados, firmas y sellos electrónicos. El servicio, trabaja teniendo en cuenta las publicaciones de la Comisión Europea, por lo que su uso y servicio atiende a todos los países de la UE.

El Servicio Cualificado de validación de Firmas electrónicas genera evidencias, teniendo en cuenta las normas y estándares fijados por la normativa legal vigente de la UE, Reglamento eIDAS. Se realizan comprobaciones del estado de calificación del certificado en el momento, día y hora de su emisión. En caso de existir Sello de Tiempo electrónico, se realiza también su comprobación. De igual manera, se realiza comprobación del estado del certificado en el momento de la firma. De todos los procesos, se generan las correspondientes evidencias.

Permite que el consumidor tenga pleno conocimiento sobre la validez, vigencia y cumplimiento normativo de la firma sometida a validación y le permite establecer políticas internas para blindarse frente a documentos o archivos firmados por clientes, proveedores o trabajadores que no cumplan con lo dispuesto en la normativa.

Características de la plataforma de validación:

- Validación de certificados bajo el reglamento eIDAS.

- Validación de confianza, caducidad y revocación de los certificados

- Validación de todos los certificados recogidos por la TSL: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- Extracción de información de los certificados (identificación de personas físicas y jurídicas).

- En el caso de certificados de personas físicas extracción de CIF y nombre y apellidos.

- En el caso de certificados de sello extracción de CIF y razón social

- En el caso de certificados de representante extracción de CIF y nombre y apellidos del representante y CIF y razón social de la empresa.

- Extracción de información de si el certificado es cualificado o no.

- Sellos de tiempo.

- Periodo de validez de los Sellos de Tiempo. Mínimo 15 años.

- La emisión de las evidencias de validación de certificados de firma electrónica será realizada en conformidad con las normas ETSI aprobadas en el marco de la regulación eIDAS.

- La emisión de las evidencias de validación de certificados de sello electrónico será realizada en conformidad con las normas ETSI aprobadas en el marco de la regulación eIDAS.

- La verificación de los sellos de tiempo que puedan ser recibidos para verificación, así como los certificados electrónicos a validar, deberán cumplir las normas del Reglamento eIDAS.

- Generación y emisión de evidencias.

Además de los servicios de validación de firmas electrónicas, se proporciona a las aplicaciones integradas la capacidad de extender las firmas electrónicas tanto ASN.1 como XML y PDF a formatos longevos. El Servicio recupera las evidencias de validación necesarias para la extensión al formato longevo deseado, y construye la firma resultante.

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que, si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas existe un servicio que mantiene dichas evidencias, y realiza la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

Los pasos que realiza el servicio son:

1. En primer lugar, se verifica la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.

2. Se realiza un proceso de completado de la firma electrónica, consistente en lo siguiente:

    a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.
    b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.

3. Se sellan las referencias a los certificados y a las informaciones de estado.

El almacenamiento de los certificados y las informaciones de estado se realiza dentro del documento resultante de la firma electrónica, siguiendo las modalidades de firmas AdES – X o -A.

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010, de 8 de enero).

11.1 FORMATOS ADMITIDOS DE FIRMA EN EL SERVICIO DE VALIDACIÓN Y POLÍTICAS

Actualmente se consideran formatos admitidos:

- **Formato XAdES (XML Advanced Electronic Signatures)**, según especificación técnica ETSI TS 101 903, versión 1.2.2, versión 1.3.2. y versión 1.4.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- **Formato CAdES (CMS Advanced Electronic Signatures),** según especificación técnica ETSI TS 101 733, versión 1.6.3, versión 1.7 y versión 1.8.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- **Formato PAdES (PDF Advanced Electronic Signatures),** según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

INDENOVA S.L., de conformidad con el Reglamento 910/2014, aprueba las siguientes firmas / sellos avanzados en formatos CADES, XADES y PADES en los niveles de cumplimiento B, T y LT, los cuales se encuentran reconocidos por los Estados miembros.

INDENOVA S.L. aprueba las condiciones y políticas bajo las cuales se confirma la validez de una firma / sello electrónico avanzado, siguiendo lo indicado en ETSI TS 119 101:

(1) el certificado que respalda la firma electrónica avanzada era válido en el momento de la firma, y cuando la firma electrónica avanzada está respaldada por un certificado cualificado, el certificado cualificado que respalda la firma electrónica avanzada era, en el momento de la firma, un certificado cualificado de firma electrónica que cumple con el Anexo I del Reglamento (UE) No 910/2014 y que fue emitido por un proveedor de servicios de confianza cualificado;

(2) los datos de validación de la firma corresponden a los datos proporcionados a la parte que confía;

(3) el conjunto único de datos que representa al usuario se proporciona correctamente a la parte que confía;

(4) el uso de cualquier seudónimo se indica claramente a la parte que confía si se usó un seudónimo en el momento de la firma;

(5) cuando la firma electrónica avanzada es creada por un dispositivo de creación de firma electrónica cualificado, el uso de dicho dispositivo se indica claramente a la parte que confía;

(6) la integridad de los datos firmados no se ha visto comprometida;

(7) en el momento de la firma se cumplían los requisitos establecidos en el artículo 36 del Reglamento (UE) no 910/2014;

(8) el sistema utilizado para validar la firma electrónica avanzada proporciona, a la parte que confía, el resultado correcto del proceso de validación y permite que la parte que confía detecte cualquier problema de seguridad relevante.

11.2 MODELO DE VALIDACIÓN

Según ETSI EN 319 102-1, el modelo conceptual de validación de QES / QESeal o AdES_QC / AdESeal_QC, se presenta en la Ilustración 1.

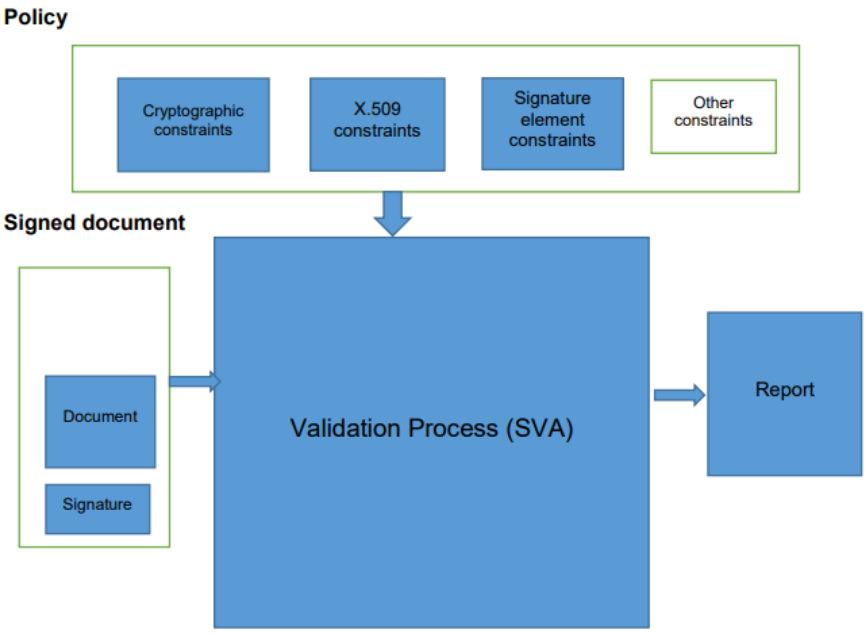

Ilustración 1: Modelo conceptual de validación

En el modelo, el componente SVA recibe la firma/sello y, de acuerdo con la Política de Validación (conjunto de restricciones), valida y genera un indicador de estado y un informe de validación que es interpretado por un usuario (parte de confianza) para la aplicabilidad de la firma/sello.

Para validar el formato de firma/sello, se ejecutan varios subprocesos dentro del proceso SVA (proceso de validación para el formato/nivel seleccionado): verificación de formato, verificación de control de calidad, verificación criptográfica, etc. el proceso es APROBADO, FALLIDO o INDETERMINADO.

Los estados que proporciona el proceso SVA después de validar el formato/nivel particular de acuerdo con la Política de Validación son:

- APROBADO: las verificaciones de todas las características/parámetros criptográficos de la firma/sello son exitosas de acuerdo con la Política; Cabe indicar que el servicio indica que la firma/sello es técnicamente válido, pero esto no significa que sea aplicable al propósito comercial particular;
- FALLIDO: las comprobaciones de todas las características/parámetros criptográficos de la firma/sello no son satisfactorias, la firma/sello se creó después de la revocación del control de calidad, o el formato no coincidía con uno de los formatos de referencia especificados en la sección 11.1 Formatos admitidos de firma en el servicio de validación;
- INDETERMINADO: los resultados de las comprobaciones individuales no permiten que la firma/sello se evalúe como APROBADO o FALLIDO; la aceptación de la firma/sello es prerrogativa del usuario/parte que Confía.

Para cada nivel/formato de firma electrónica/sello electrónico, la SVA realiza una secuencia lógica de subprocesos que comprenden los siguientes procesos de validación:

- Proceso de validación para formato básico de firma/sello - BASELINE_B. La SVA realiza este proceso si el tiempo de validación está dentro del período de validez del QC y no se revoca, o el tiempo de validación está fuera del período de validez del QC y la CA ha proporcionado información sobre su revocación / cancelación;
- Proceso de validación para el nivel básico de firma / sello BASELINE_T y BASELINE_LT - la SVA realiza este proceso de validación de firma básica de una firma / sello con tiempo certificado (_T) y de firma / sello con tiempo certificado y estado de un QC (_LT);
- Proceso de validación para el nivel de firma / sello BASELINE_LTA - la SVA realiza este proceso de validación de firma básica de una firma / sello con tiempo certificado (_T), de firma / sello con tiempo certificado y estado de un QC (_LT) y de una firma / sello con material de archivo (LTA);

11.3 PROCESO DE VALIDACIÓN

EL proceso que sigue el SVA sigue es:

(1) Si la firma/sello para la validación es:
- con perfil BASELINE_B - el SVA deberá realizar (4)
- con perfil BASELINE_T o BASELINE_LT - el SVA deberá realizar (3)
- con perfil BASELINE_LTA: el SVA deberá realizar (2)

(2) Si el SVA no admite la validación de firma/sello con el perfil BASELINE_LTA, el SVA deberá realizar (3); de lo contrario, la SVA realizará un proceso de validación de firma/sello con perfil BASELINE_LTA y pasará a (5);

(3) Si el SVA no admite la validación de firma/sello con los perfiles BASELINE_LTA, BASELINE_T y BASELINE_LT, el SVA deberá realizar (4); de lo contrario, la SVA realizará un proceso de validación de firma/sello con el perfil BASELINE_T y BASELINE_LT y pasará a (5);

(4) La SVA realizará un proceso de validación de sello/firma de formato básico (perfil BASELINE_B) y pasará a (5);

(5) Cuando el estado de validación del proceso de validación seleccionado sea APROBADO, la SVA devolverá un indicador de estado TOTAL PASSED y un informe de validación en formato XML como respuesta del servicio web;

(6) Cuando el estado de validación del proceso de validación seleccionado es FALLIDO, el SVA devolverá un indicador de estado TOTAL-FALLIDO y un informe de validación en formato XML como respuesta del servicio web;

(7) En otro caso, el SVA devolverá el indicador de estado INDETERMINADO y un informe de validación en formato XML como respuesta del servicio web.

Las solicitudes de validación de firmas/sellos y las respuestas a estas solicitudes utilizan el canal de comunicación seguro entre Cliente y Servidor. El intercambio está protegido por el soporte de la autenticación del servidor y se puede mantener la autenticación del cliente. El protocolo de validación (solicitudes y respuestas) cumple con ETSI EN 119 442.

De acuerdo con ETSI TS 319 172-1, el SVA realiza el proceso de validación en los siguientes pasos:

Paso 1: El Cliente genera y envía una solicitud de validación que contiene los documento (si la firma/sello está envuelto o envuelto); Las restricciones de validación son establecidas implícitamente por el software SVA y el proceso de validación las ejecuta de acuerdo con el formato de la firma/sello entregado en la solicitud.

Paso 2: El SVA realiza la validación de firma/sello; la implementación de este paso implica el uso de servicios de confianza internos adicionales de INDENOVA S.L. (CRL/OCSP,) o, si es necesario, de otros proveedores externos.

Paso 3: El SVA genera, prepara y envía una respuesta XML como informe de validación en respuesta a una solicitud de validación de firma/sello; el informe de validación detallado contiene el indicador de estado (SI/NO) de la validación de cada restricción y sus efectos en función del proceso de validación seleccionado del SVA, cumple con la especificación técnica ETSI TS 119 102-2.

Paso 4: Sobre la base de la respuesta XML del informe de validación, el Usuario/Confianza acepta o rechaza la validez técnica de la firma/sello.

El servicio realiza los siguientes procesos de validación, dependiendo del perfil de la firma/sello presentado:

- Proceso de validación de firma/sello con perfil BASELINE_B;
- Proceso de validación del sello de tiempo;
- Proceso de validación de firma/sello con perfiles BASELINE_T y BASELINE_LT; este proceso es el mismo para ambos perfiles;
- Proceso de validación de firma/sello con perfil BASELINE_LTA.

La elección del proceso de validación del SVA sigue las instrucciones de la sección 12.2del modelo de validación y el proceso seleccionado realiza los pasos anteriores, incluidos los procedimientos funcionales básicos (subprocesos), que construyen la secuencia lógica de verificaciones en el marco del proceso de validación de la firma/sello.

11.4 RESULTADO DE LA VALIDACIÓN

El proceso de validación de firma / sello finaliza con:

- Indicador de estado de validación (APROBADO, FALLIDO, INDETERMINADO);
- Identificador de la política de validación (o descripción de las limitaciones);
- Fecha y hora de validación y datos de validación (firma / certificado de sello;
- El proceso de validación seleccionado (según el perfil de firma / sello);
- Informe de validación.

11.5 INTERFACES AND VALIDATION PROTOCOL

INDENOVA S.L. opera y respalda el SERVICIO como un servicio web al que se accede a través de:

- API Servicio calificado de validación de firmas o sellos electrónicos: https://app.swaggerhub.com/apis/eSignaBox/circuits-api/2.0.3#/Signatures/checkSignatures

La interfaz utiliza un canal de transporte / comunicación seguro que admite la autenticación del cliente.

EL SERVICIO se autentica mediante el uso de tokens y protocolos Open ID Connect:

- Autorización API: https://app.swaggerhub.com/apis/eSignaBox/authorization-api/2.0.1

11.6 CONSULTA DE INFORMACIÓN DE FUENTES EXTERNAS

En ciertos casos, el SERVICIO requiere acceso a fuentes externas de certificados relacionados con el proceso de validación de firma/sello a un documento firmado/sellado. Dichos participantes externos (indirectos) en el proceso de validación son:

- Depósitos de certificados mantenidos por otros QTSP: registros públicos, fuentes CRL/OCSP; autoridades certificadoras de sellado de tiempo;
- Lista de confianza nacional, listas de confianza (TL) externas (Estados miembros);
- Lista de listas de confianza (LoTL).

EL SERVICIO utiliza interfaces de software estandarizadas para acceder a estas fuentes externas de certificados calificados, que verifica durante el proceso de validación de QES/QESeal y/o AdES/AdESeal_QC.

La LoTL es una publicación de la Comisión Europea. Este archivo XML contiene las Listas de confianza de los Estados miembros, incluida la Lista de confianza nacional.

Puede encontrar información sobre quién firma y publica LoTL en: http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015XC1224(01)&from=EN.

El formato de firma de la LoTL y la TL nacional es XAdES BASELINE_B. El SERVICIO confía en LoTL verificando la firma a través del certificado publicado en la dirección anterior.

12 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Véase punto 5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIÓN de la DPC.

12.1 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.

12.2 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

Véase apartado 5.4 PROCEDIMIENTO DE REGISTRO DE EVENTOS de la DPC. Además, en particular, en la prestación del servicio de firma electrónica en servidor:

1. El SSA guarda registro, al menos, de los siguientes eventos: - Inicialización de sistema, arranque, parada y cambios de configuración. - Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción) - Uso de claves de los firmantes. - Autenticación de los firmantes (incluyendo intentos fallidos). - Gestión de los datos de activación de firma del firmante (cambios de PIN/contraseña) - Accesos al sistema por parte de los usuarios administradores.
2. El SSA genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores. 61. El SSA protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior.
3. Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información: - Fecha y hora del evento. - Tipo de evento. - Identidad de la entidad (firmante, administrador o proceso) responsable de la acción. - Resultado del evento (éxito o error)
4. El SSA comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema.
5. Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización.

12.3 ARCHIVO DE REGISTROS

Véase apartado 5.4 PROCEDIMIENTO DE REGISTRO DE EVENTOS de la DPC.

12.4 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.

13 CONTROLES DE SEGURIDAD TÉCNICA

13.1 GESTIÓN DE LOS SISTEMAS DE LA SEGURIDAD

El SSA implementa los siguientes roles de gestión:

- Responsable de seguridad (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- Administrador del sistema (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- Operador del sistema (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- Auditor del sistema (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

INDENOVA S.L. asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1. 6.5.2.

13.2 OPERACIONES Y SISTEMAS

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC.

El componte software SSA y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos su certificación como dispositivo QSCD.

13.3 CONTROLES DE SEGURIDAD INFORMÁTICA.

Véase apartado de la DPC

14 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 DPC

14.1 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 Common Criteria EAL 4+
- 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 el Organismo supervisor.

14.2 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 Common Criteria EAL 4+,
- 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.

14.3 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 el Organismo supervisor.

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 el Organismo supervisor.

14.4 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 del Organismo supervisor.

14.5 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.

14.6 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.

15 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.

INDENOVA S.L. 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.

16 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. INDENOVA S.L. 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.

17 CONFIDENCIALIDAD DE LA INFORMACIÓN DE NEGOCIO

Todo el personal de INDENOVA S.L. 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

18 DERECHOS DE PROPIEDAD INTELECTUAL

La totalidad de los componentes de la SVA de INDENOVA S.L., 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 INDENOVA S.L., 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 INDENOVA S.L.

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.

19 POLÍTICA DE REEMBOLSO

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

20 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.

21 ENMENDADURAS

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

22 RESOLUCIÓN DE DISPUTAS

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

23 ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

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

24 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.

25 TARIFAS

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

26 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.

27 AUDITORÍA

INDENOVA S.L. se somete a servicios de auditoría periódica por parte del Organismo de evaluación de la conformidad para el mantenimiento de la acreditación de la SVA.

El auditor debe:

- Ser autorizado por el Organismo supervisor.
- 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.

28 CONFORMIDAD CON LA LEY APLICABLE

INDENOVA S.L. es afecta y cumple con las obligaciones establecidas por el Organismo supervisor, 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 a la Ley de Firmas Electrónica, para el reconocimiento legal de los sellos de tiempo emitidos bajos las directrices definidas en el presente documento.

29 BIBLIOGRAFÍA

(1) REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 (Reglamento eIDAS)
(2) Reglamento (UE) 2016/679 (Reglamento general de protección de datos)
(3) Ley 59/2003, de 19 de diciembre, de firma electrónica.
(4) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
(5) 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 y por el que se deroga la Directiva 95/46/CE.
(6) Real Decreto 505/2007, de 20 de abril, por el que se aprueban las condiciones básicas de accesibilidad y no discriminación de las personas con discapacidad para el acceso y utilización de los espacios públicos urbanizados y edificaciones.