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	**Entidad de Certificación**
Título	**Política de Seguridad**

Realizado por	**INDENOVA S.L.**		
Documento	**DOC-200216.20A2615**		
Fecha	**26/10/2020**	Versión	**1**

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 - 2ºB
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	26/10/2020	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 Entidad Certificación (EC), INDENOVA S.L. provee los servicios de emisión, re-emisión, distribución y revocación de certificados digitales, provistos por la EC de INDENOVA S.L.

Junto a los servicios de certificación digital, INDENOVA S.L. brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales.

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 VISIÓN GENERAL

El alcance de la acreditación cubre la infraestructura y sistemas de registro que utiliza INDENOVA S.L. en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación INDENOVA S.L.

3 OBJETO DE LA ACREDITACIÓN

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza INDENOVA S.L. para la administración de sus servicios como Entidad de Certificación Digital – EC, 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.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación – EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la legislación vigente.

Entidad de Registro – ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y registro de los solicitantes del certificado.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC 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 firmado digitalmente, y que confía en la validez de las transacciones realizadas.

4.1 PKI PARTICIPANTES

4.1.1 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.

4.1.2 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. L 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 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.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (INDENOVA S.L.)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación INDENOVA S.L., cuando la entidad de certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece INDENOVA son provistos por la Entidad de Certificación INDENOVA S.L.

4.1.4 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 y publicados en esta CPS.

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

4.1.5 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.

4.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo esta CPS. En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

4.1.7 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.

4.1.8 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.

4.1.9 OTROS PARTICIPANTES

4.1.9.1 EL COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación INDENOVA S.L., conformado por el Gerente, el Administrador del Sistema, Jefe de Operaciones y el Auditor del Ciclo de Certificación y tiene entre otras funciones la aprobación de la CPS como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la CPS aprobada y autorizar su publicación. El comité de Seguridad es el responsable de integrar la CPS, a la CPS de terceros prestadores de servicios de certificación.

5 RESPONSABILIDADES DE INDENOVA S.L.

INDENOVA S.L. establece la Política de Seguridad que los proveedores de servicios de certificación digital deben cumplir.

En caso de incidentes que puedan afectar la seguridad de los servicios contratados a INDENOVA S.L., las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por INDENOVA S.L., de acuerdo con su documento Declaración de Prácticas de Certificación, publicado en:

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

INDENOVA S.L. brinda los servicios de registro o verificación conforme a la normativa de aplicación vigente, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por INDENOVA S.L. a través de la Entidad de Certificación son recibidas directamente por INDENOVA S.L. como prestador de Servicios Digitales o a través de nuestra Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone INDENOVA S.L. es permanente.

6 ALCANCE

La presente política es de cumplimiento obligatorio por los proveedores de servicios de certificación digital contratados por INDENOVA S.L.

7 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La EC de INDENOVA S.L. tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de certificación, asegurando que los proveedores de servicios de certificación digital cumplan con lo establecido en la presente política.

7.1 ORGANIZACIÓN

El Responsable de la EC de INDENOVA S.L. y el Responsable de Seguridad son los encargados de velar por el cumplimiento de lo establecido en la presente política.

7.2 GESTIÓN DE RIESGOS

El servicio adquirido a los proveedores de servicios de Certificación Digital incluye la administración de los riesgos relacionados con dicha infraestructura física y de comunicaciones.

7.3 GESTIÓN DE ACTIVOS

El servicio adquirido a los proveedores de servicios de Certificación Digital protege los activos entregados por INDENOVA S.L., de acuerdo a la clasificación y controles especificados por el Responsable de Seguridad de la EC.

7.4 SEGURIDAD FÍSICA

7.4.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la infraestructura de los proveedores de servicios de certificación digital debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre.

7.4.2 SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

Se deben implementar controles para proteger al personal y el equipamiento contra daño físico.

7.4.3 PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas donde se procesan los sistemas de información críticos de la EC deben estar protegidas constantemente contra acceso no autorizado.

7.4.4 PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA

Las instalaciones deben estar protegidas contra exposición al agua o humedad.

7.4.5 PROTECCIÓN CONTRA INCENDIOS

Las instalaciones deben poseer medidas para la prevención y protección contra incendios.

7.4.6 ARCHIVO DE MATERIAL

Los archivos tanto electrónicos como de papel relacionados a la gestión de certificados digitales deben estar protegidos en las áreas de archivo, en contenedores de protección contra fuegos y deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación. Y deben ser conservados por un periodo de 15 años.

7.4.7 GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos como de papel que contengan información crítica de la EC que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

7.5 GESTIÓN DE ROLES

7.5.1 ROLES DE CONFIANZA

Los proveedores de servicios de certificación digital deben tener definidos y establecidos los roles que realizan funciones críticas.

La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.

7.5.2 NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los accesos físicos y lógicos a los sistemas que protegen las claves de la EC deben requerir la autenticación de al menos 2 personas.

7.5.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza se deben emplear controles de acceso físico para el acceso a las áreas críticas, así como lógicos para las funciones de administración con la EC.

7.5.4 AUDITORÍA

El auditor asignado por el organismo de evaluación de la conformidad deberá ser siempre una persona independiente de las operaciones de registro.

7.6 GESTIÓN DEL PERSONAL

7.6.1 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de certificación digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos.

Asimismo, deben tener experiencia relacionada a los temas de certificación digital.

7.6.2 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de certificación.

7.6.3 REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de certificación deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

7.6.4 FRECUENCIA DE LAS CAPACITACIONES

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

7.6.5 SANCIONES POR ACCIONES NO AUTORIZADAS

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

7.6.6 REQUERIMIENTOS DE LOS CONTRATISTAS

El personal contratado para fines específicos dentro de las operaciones de la EC será evaluado respecto de sus conocimientos y experiencia.

7.7 PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

7.7.1 TIPOS DE EVENTOS REGISTRADOS

Se deben registrar los eventos críticos relacionados al procesamiento de los sistemas de la Entidad de Certificación.

7.7.2 FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría deben ser procesados y revisados con periodicidad con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

7.7.3 PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro deben conservarse por un periodo de quince (15) años.

7.7.4 PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Los logs de auditoria forman parte del respaldo diario del sistema de información y se conservan de igual manera manteniendo una copia en el sitio y otra copia fuera de las instalaciones.

7.7.5 COPIA DE RESPALDO

Las copias de respaldo deberán ser protegidas contra modificación no autorizada.

7.7.6 AUDITORÍA

Los proveedores de servicios de certificación digital deberán someterse a la evaluación realizada por los auditores autorizados por el Organismo de supervisión, conforme a la frecuencia establecida por dicha autoridad.

Asimismo, los proveedores de servicios de certificación digital deberán cumplir y mantener vigente la certificación internacional ISO 27001.

7.8 ARCHIVO

7.8.1 PROTECCIÓN DEL ARCHIVO

El archivo debe estar protegido con controles de acceso físico para impedir el acceso a personas no autorizadas.

7.9 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

7.9.1 PLAN DE CONTINGENCIAS

El proveedor de servicios de certificación digital debe mantener un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

El plan debe asegurar que los servicios de registro para los procesos de emisión y revocación, puedan ser reasumidos dentro de un plazo máximo de 48 horas.

Los planes deben ser evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, conjuntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

La recuperación debe incluir los sistemas administrados por la EC y los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC.

7.9.2 COMPROMISO DE LA CLAVE PRIVADA

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

7.10 CONFIDENCIALIDAD DE INFORMACIÓN

7.10.1 INFORMACIÓN CONSIDERADA CONFIDENCIAL

Los prestadores de servicios de certificación digital deben mantener de manera confidencial la siguiente información:

- Material comercialmente reservado de la EC: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

7.10.2 INFORMACIÓN QUE PUEDE SER PUBLICADA

La información que puede ser publicada es:

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.
- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

7.11 RESPONSABILIDADES

El Responsable de Seguridad de INDENOVA S.L. gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

7.12 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la EC de INDENOVA S.L., y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.