Entidad de Certificación Digital

THOMAS SIGNE
Soluciones Tecnológicas Globales

Declaración de Prácticas de Certificación para Estampado Cronológico

Información del documento

Nombre	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA ESTAMPADO CRONOLÓGICO
Realizado por	THOMAS SIGNE S.A.S.
País	COLOMBIA
Versión	2.7
Fecha	JULIO DEL 2023
Tipo de Documento	PÚBLICO
Código	THS-CO-AC-DPC-02

Historial de versiones

Versión	Fecha	Descripción
1.0	28/12/2017	Elaboración de documento inicial.
1.1	12/05/2018	Modificación en la estructura del documento. Cambio de nombre de documento.
1.2	20/05/2018	Se cambia el nombre del documento. Se modifican las obligaciones de Proveedores. Se agrega como Anexo el Contrato de Suscripción.
1.3	22/05/2018	Modificación menor en el apartado de Identificación de la ECD. Especificaciones en el apartado de Controles de seguridad. Se especifican los tipos de Paquete.
1.4	08/06/2018	Se agregan apartados para formatos y registros aplicables.
1.5	25/06/2018	Se detalla el proceso de comercialización y solicitud del servicio.
1.6	02/11/2018	Se elimina del pie de página la referencia al THS-PR-GRAL-02-F01 Estructura de documento v1.0. Se elimina el apartado “INTRODUCCIÓN”.
1.7	11/03/2019	Integración con el sistema de gestión del Grupo.

		Cambio de nombre del documento de THS-DP-ST-01 a THS-CO-DPC-AC-02
1.8	06/09/2019	Ajuste de la codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.1 Inclusión de los formatos y registros por anulación de la THS-CO-DPC-AC-03 Declaración de Prácticas para Estampado Cronológico Interna v1.3 Correcciones menores
1.9	29/11/2019	Cambios en los datos de identificación de la ECD y de sus proveedores, incluyendo el certificado de existencia y representación legal y el estado activo en Cámara de Comercio o equivalente. Se indica que se tiene establecido y probado el plan de continuidad y contingencia. Los Solicitantes, Suscriptores, Terceros aceptantes o el público en general sólo podrán indicar su PQRSA enviando un email a la dirección de correo pqrsa@thsigne.com. Se añade la responsabilidad de la ECD de informar a sus proveedores de que hace extensivo el cumplimiento de los requisitos del CEA 4.1-10. Cambio del No. de cuenta corriente para realizar el depósito de la cuantía respectiva a cada servicio. Correcciones menores.
2.0	31/01/2020	Revisión general del contenido de la DPC con base en la legislación y normativa aplicable y el contenido de la documentación del Sistema de Gestión por parte de un equipo de trabajo multidisciplinar. Cambios en la organización del contenido del documento para homogeneizarlo con las otras DPC. Se elimina el No. de cuenta corriente para realizar el depósito de la cuantía respectiva a cada servicio (se indicará en la Propuesta Comercial).
2.1	19/06/2020	Ajustes en título del documento. Se añaden las secciones Perfil de CRL y Perfil de OCSP. Correcciones menores.
2.2	06/11/2020	Se indica que la política bajo la cual la TSA de Thomas Signe S.A.S. emite todos los sellos de tiempo, identificada por un OID específico contenido en los sellos de tiempo, es conforme a la política de sellado de tiempo BTSP (OID 0.4.0.2023.1.1) descrita en el estándar ETSI EN 319 421. Se añade el rol de Operador del Servicio de la TSA dentro de las plataformas de la TSA, desempeñado por el rol de confianza Responsable de Registro Digital. Se añaden las responsabilidades de la ECD de informar a los Solicitantes, Suscriptores, Terceros que confían y al público en general en la página web de Thomas Signe S.A.S de las actividades y servicios acreditados atendiendo a lo establecido en el documento RAC-3.0-03 vigente de ONAC, y de la información general de la empresa, como es su naturaleza, el tipo de empresa, etc. Se añaden un formato y un registro para la tabla de retención documental.

		Correcciones menores.
2.3	24/06/2021	Cambio de imagen de Thomas Signe. Se añade la posibilidad de que el tipo de documento de identidad del Representante Legal del Suscriptor (Persona Jurídica) sea el Pasaporte. Se describe con más detalle el control multipersona para el acceso a la clave privada de la TSU. Cambios en el método de destrucción de la clave privada de la TSU, para que no resulten afectadas el resto de claves gestionadas por los dispositivos criptográficos hardware empleados (HSM). Se añade un apartado de responsabilidad en la protección de información confidencial. Correcciones menores.
2.4	19/11/2021	Se elimina el fax en los datos de identificación de la ECD Thomas Signe S.A.S. y de sus proveedores. Se especifican con más detalle las características de los sellos de tiempo. Cambios en los requisitos operacionales para el ciclo de vida del servicio de estampado cronológico, para que las funciones de decisión y notificación sean realizadas por el Área Comercial, quien también realiza la función de revisión. Se especifican con más detalle las obligaciones de los terceros que confían en los certificados. Los cambios en el contenido de esta DPC que pudiesen afectar a la aceptación del servicio serán notificados con antelación a los interesados. Correcciones menores.
2.5	08/07/2022	Adecuación a la nueva versión de CEA-3.0-07. Añadida fuente alternativa de tiempo. Cambiado el procedimiento PQRS en línea con la nueva versión de CEA.
2.6	30/09/2022	Actualizados teléfonos de contacto en adecuación al nuevo prefijo. Actualización de normas y estándares técnicos utilizados. Ajuste de las características del seguro.
2.7	03/07/2023	Añadida información sobre la disponibilidad del servicio.

ÍNDICE

1 INTRODUCCIÓN

1.1 PRESENTACIÓN DEL DOCUMENTO

Este documento constituye la Declaración de Prácticas de Certificación (DPC) para el estampado cronológico de Thomas Signe S.A.S., en el marco del cumplimiento de los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-3.0-07 vigente establecidos por el Organismo Nacional de Acreditación de Colombia – ONAC, conforme a la legislación colombiana y las disposiciones de los entes reguladores.

Esta DPC establece las prácticas que lleva a cabo Thomas Signe S.A.S. para emitir sellos de tiempo, así como los requisitos particulares de los sellos de tiempo emitidos (política de emisión de sellos de tiempo), siguiendo el estándar RFC 3628 "Policy Requirements for Time-Stamping Authorities (TSAs)", y conforme a los siguientes estándares:

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

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

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, Solicitantes, Suscriptores, Terceros que confían y público en general.

En el caso de que se detecten vulnerabilidades o se pierda la vigencia de los estándares técnicos o infraestructura indicados en la presente DPC, Thomas Signe S.A.S se encargará de informar de tal hecho a ONAC, para proceder con la respectiva actualización.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Los datos de identificación del presente documento están especificados en la tabla inicial *Identificación del documento*.

Adicionalmente, el presente documento se identifica con los siguientes OID, correspondientes a la propia DPC, y a la política bajo la cual Thomas Signe S.A.S. emite todos los sellos de tiempo y que se encuentra contenida en éstos .

OID DE LA DPC PARA ESTAMPADO CRONOLÓGICO DE THOMAS SIGNE S.A.S.	
1.3.6.1.4.1.51362.0.1.0.1	DPC
1.3.6.1.4.1.51362.0.1.2.1	Política de emisión de sellos de tiempo

Este documento se encuentra publicado en la siguiente página web:

https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/

1.3 PARTICIPANTES DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

1.3.1 ECD THOMAS SIGNE S.A.S. (THOMAS SIGNE TSA)

Signe S.A. (en adelante 'Signe') es una empresa con domicilio en España que brinda principalmente servicios consistentes en la edición e impresión de documentos de seguridad para empresas públicas y privadas.

Desde el año 2010, Signe realiza su actividad como Prestador de Servicios de Confianza (PSC) para la emisión de certificados cualificados y no cualificados de firma electrónica y certificados cualificados de sello electrónico según 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 la que se deroga la Directiva 1999/93/CE (también conocido como Reglamento eIDAS), y conforme a la Ley española 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

En el año 2016, en una alianza comercial entre Signe y Thomas Greg & Sons de Colombia, se crea la empresa Thomas Signe S.A.S. (en adelante 'Thomas Signe'), para actuar como Entidad de Certificación, Entidad de Registro o Verificación, Software de Firma Digital y Prestador de Servicios de Valor Añadido de Sellado de Tiempo e Intermediación Digital; y así brindar dichos servicios en Colombia y dar cumplimiento a la regulación establecida por la Autoridad Administrativa Competente (AAC), ONAC.

Como Entidad de Certificación - EC, Thomas Signe provee servicios de certificación de emisión, revocación e información del estado de revocación de certificados digitales.

La infraestructura tecnológica y operativa de la EC de Thomas Signe es provista por Signe. Dicha infraestructura ha obtenido la cualificación eIDAS y es verificada anualmente por auditores autorizados.

Junto a los servicios de certificación, Thomas Signe brinda los servicios de registro o verificación, además de los servicios de valor añadido de sellado de tiempo e intermediación digital.

Thomas Signe, en su papel de Entidad de Certificación Digital (ECD), es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

A Thomas Signe, como ECD, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante ONAC a fin de lograr y mantener la acreditación.

La ECD Thomas Signe, en su papel de CA Subordinada, emite y revoca certificados, y presta los servicios de comprobación de revocación mediante CRL y OCSP.

Asimismo, la ECD Thomas Signe presta los servicios de Autoridad 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 el respectivo registro de evidencias, y de gestionar las solicitudes de emisión y de revocación de certificados digitales.

A continuación se indican los datos de identificación los sitios de la ECD Thomas Signe relevantes en la provisión de los servicios de certificación:

Entidad de Certificación Digital

Nombre - Razón Social: THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES S.A.S.

Sigla: THOMAS SIGNE S.A.S.

N.I.T.: 900962071-5

N° matrícula de Cámara de Comercio: 02680791

Certificado de existencia y representación legal en Cámara de Comercio: https://www.thomas-signe.co/CERL_Thomas_Signe.pdf

Estado activo en Cámara de Comercio: en https://www.rues.org.co/ consultar digitando como Número de Identificación *900962071*

Domicilio social y de correspondencia - comercial: Avenida de las Américas No. 44 – 57 - Bogotá D.C., Colombia

Domicilio de correspondencia – notificaciones judiciales: Cr. 42 Bis No. 17 A 75 - Bogotá D.C., Colombia

Teléfono: +60 (1) 3810240

Dirección de correo electrónico: comercial@thomas-signe.co

Oficina para PQRS: PQRS - pqrsa@thsigne.com

Página Web: www.thomas-signe.co

Infraestructura tecnológica y servicios corporativos - Subdirección ejecutiva – Centro de operación técnica

Nombre - Razón Social: SIGNE, S.A.

N.I.F. (equivalente en España a N.I.T. en Colombia): A11029279

Datos de inscripción en Registro Mercantil (equivalente en España a Nº matrícula de Cámara de Comercio en Colombia): Registro Mercantil de Madrid, tomo 8101, libro 7029, folio 95, sección 3.ª, hoja 78156-2, hoja actual M-66591, de la sección 8.ª

Certificación de vigencia y cargos en Registro Mercantil (equivalente en España a certificado de existencia y representación legal en Cámara de Comercio en Colombia): https://www.thomas-signe.co/CVC_Signe.pdf

Estado vigente en Registro Mercantil (equivalente en España a estado activo en Cámara de Comercio en Colombia): en https://sede.registradores.org/site/mercantil buscar por sociedad introduciendo el NIF *A11029279*

Domicilio social y de correspondencia: Avenida de la Industria 18 - 28760 Tres Cantos (Madrid), España

Teléfono: +34 918 06 00 99

Dirección de correo electrónico: comercial@signe.es

Oficina para PQRS: Soporte Técnico - soporte@signe.es

Página Web: www.signe.es

Servicios locales – Dirección ejecutiva

Nombre - Razón Social: THOMAS GREG & SONS LIMITED (GUERNSEY) S.A.

N.I.T.: 830012157-0

N° matrícula de Cámara de Comercio: 00656972

Certificado de existencia y representación legal en Cámara de Comercio: https://www.thomas-signe.co/CERL_TGSL.pdf

Estado activo en Cámara de Comercio: en https://www.rues.org.co/ consultar digitando como Número de Identificación *830012157*

Domicilio social y de correspondencia - comercial: Avenida de las Américas No. 44 – 57 - Bogotá D.C., Colombia

Domicilio de correspondencia – notificaciones judiciales: Cr. 42 Bis No. 17 A 75 - Bogotá D.C., Colombia

Teléfono: +60 (1) 3810240

Dirección de correo electrónico: servicioalclientetgsc@thomasgreg.com

Oficina para PQRS: Servicio al cliente - servicioalclientetgsc@thomasgreg.com

Página Web: www.tgscolombia.com

1.3.2 SOLICITANTE

Solicitante es la persona natural que solicita a la ECD Thomas Signe S.A.S. el servicio de estampado cronológico (la emisión de sellos de tiempo).

1.3.3 SUSCRIPTOR

Suscriptor es la persona natural o jurídica que, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y habiendo firmado el respectivo Contrato de Prestación de

Servicios o de Suscripción con Thomas Signe S.A.S., acepta las condiciones del servicio de estampado cronológico prestado por éste.

1.3.4 TERCERO QUE CONFÍA

Tercero que confía (o Tercero aceptante) son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en un sello de tiempo emitido por la ECD Thomas Signe S.A.S..

1.4 POLÍTICA Y OID DE TSA

La TSA de Thomas Signe S.A.S. dispone de una única Unidad de Sellado de Tiempo (TSU) para firmar los sellos de tiempo que emite.

La TSA de Thomas Signe S.A.S. dispone de un único certificado de firma de sellos de tiempo que ha sido emitido a nombre de su única TSU (Thomas Signe TSA - TSU 01) por la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S. (Thomas Signe Root), con un OID específico en su extensión X.509 v3 Certificate Policies. En la sección 7.1 se especifica el perfil de este certificado de TSU.

La TSA de Thomas Signe S.A.S. emite todos los sellos de tiempo bajo una misma política identificada por un OID específico contenido en los sellos de tiempo, que es conforme a la política de sellado de tiempo BTSP (OID 0.4.0.2023.1.1). Las características de estos sellos de tiempo se especifican en la sección 3.

OID DE CERTIFICADO Y POLÍTICA DE LA TSA DE THOMAS SIGNE S.A.S.	
1.3.6.1.4.1.51362.0.1.1.1	Certificado de firma de sellos de tiempo
1.3.6.1.4.1.51362.0.1.2.1	Política de emisión de sellos de tiempo

1.5 ADMINISTRACIÓN DE LA DPC

1.5.1 ORGANIZACIÓN RESPONSABLE

Thomas Signe S.A.S. administra esta DPC.

1.5.2 DATOS DE CONTACTO

Para consultas o comentarios relacionados con la presente DPC, el interesado podrá dirigirse a Thomas Signe S.A.S. a través de alguno de los medios siguientes: domicilio social y de correspondencia – comercial, teléfono, direcciones de correo electrónico comercial o PQRS de la Entidad de Certificación Digital indicados en la sección 1.3.1.

1.5.3 PROCEDIMIENTO DE APROBACIÓN

Esta DPC es aprobada por el Comité de Sistemas de Gestión de Thomas Signe S.A.S. antes de ser publicada, controlando las versiones de la misma, a fin de evitar modificaciones y suplantaciones no autorizadas y el uso de documentación obsoleta.

Las nuevas versiones aprobadas de esta DPC son enviadas a ONAC y publicadas en la página web de Thomas Signe S.A.S. Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

1.6 DEFINICIONES Y SIGLAS

1.6.1 DEFINICIONES

Algoritmo: conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Autoridad de Certificación: Certification Authority (CA). Es una entidad de confianza, responsable de emitir y revocar los certificados digitales, publicación de certificados, publicación de listas de certificados revocados, etc. Nombrada dentro de la normativa colombiana como Entidad de Certificación Digital – ECD.

Autoridad de sellado de tiempo (TSA): entidad de confianza que emite sellos de tiempo mediante una o más TSU. Nombrada dentro de la normativa colombiana como Entidad de Certificación Digital – ECD. Los sellos de tiempo emitidos por la ECD, conforme a la regulación establecida por la ONAC, incluyen la fecha y hora referenciada por la fuente de tiempo reportada por el Instituto Nacional de Metrología de Colombia.

CA Raíz: Autoridad de Certificación de primer nivel, base de confianza.

Certificado digital: mensaje de datos electrónico firmado por la ECD, el cual identifica tanto a la ECD que lo expide, como al suscriptor y contiene la clave pública de este último.

Clave privada: ver **Datos de Creación de Firma**.

Clave pública: ver **Datos de Verificación de Firma**.

Cliente: en los servicios de certificación digital, el término "cliente" identifica a la persona natural o jurídica con la cual la ECD establece una relación comercial.

Datos de Creación de Firma (Clave privada): valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

Datos de Verificación de Firma (Clave pública): datos que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor.

Declaración de Prácticas de Certificación (DPC): documento en el que constan de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que la ECD emplea para emitir sellos de tiempo.

Entidad de Certificación: de acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, aquella persona natural o jurídica que, autorizada conforme a dicha Ley, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Entidades de Certificación Digital – ECD: denominación que se establece con el fin de particularizar y diferenciar este tipo de organizaciones como Entidades de Certificación de los demás Organismos de Certificación que ONAC acredita. Entidad de Certificación que presta el servicio de estampado cronológico (emite sellos de tiempo), incluyendo otras gestiones propias de sellos de tiempo, de acuerdo a la regulación establecida por ONAC.

Estampado cronológico (Estampa cronológica, Sello de tiempo o Sellado de tiempo, Time stamp o Time stamping en inglés): mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

Firma Digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Función Hash: operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Log: servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

Niveles de seguridad: diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

OID: identificador único de objeto (object identifier). OID. Acrónimo del término en idioma inglés "Object Identifier", que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

Petición (PQRS): solicitud presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD.

PKI: Infraestructura de clave pública (Public Key Infraestructure). Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.
- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

Proveedor: el término "proveedor" incluye a organizaciones, personas, fabricantes, distribuidores, ensambladores de tecnología y otros que suministran productos, bienes y servicios. Entre los proveedores de las ECD están: Entidades recíprocas, empresas de tecnología que prestan servicios en sus diferentes modalidades como son: hosting, colocation, repositorio documental (electrónico o físico), proveedor de dispositivos, proveedor de telecomunicaciones, etc.

Queja (PQRS): expresión de una insatisfacción presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD o al propio proceso de tratamiento de las quejas.

Reclamo (PQRS): expresión de una insatisfacción presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD, por la que se pretende algún tipo de compensación

Revocación: proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación, al presentarse alguna de las causas establecidas en la Declaración de Prácticas de Certificación para la emisión de certificados.

Servicio de certificación digital: conjunto de actividades certificación que ofrece la ECD para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

Sello de tiempo: ver **Estampado cronológico***.*

Solicitante: persona natural o jurídica que con el propósito de obtener servicios de certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC para acceder al servicio de certificación digital. Persona natural que solicita a la ECD el servicio de estampado cronológico (la emisión de sellos de tiempo).

Sugerencia (PQRS): recomendación que propone un cliente o parte interesada para la mejora de los servicios prestados por la ECD.

Suscriptor: persona natural o jurídica que, habiendo firmado el respectivo Contrato de Prestación de Servicios o de Suscripción, acepta las condiciones del servicio de estampado cronológico prestado por la ECD.

Tercero que confía (Tercero aceptante): persona natural o jurídica que recibe un documento, log, notificación o cualquier otro dato, firmado digitalmente o no, con un sello de tiempo emitido por la ECD, y que confía en la validez de dicho sello de tiempo.

Unidad de sellado de tiempo (TSU): conjunto de hardware y software que es gestionado como una unidad y tiene un única clave de firma de sellos de tiempo activa en un instante de tiempo.

1.6.2 SIGLAS

CA Certification Authority (Autoridad de Certificación)

CRL Certificate Revocation List (Lista de Certificados Revocados)

DPC Declaración de Prácticas de Certificación

ECD Entidad de Certificación Digital que prestan servicios de certificación digital y equivale a una Entidad Certificadora definida en la ley 527 de 1999. También se debe entender como un Organismo de Evaluación de la Conformidad – OEC de acuerdo con lo definido en la ISO/IEC 17000.

ERP Entreprise Resource Planning (Planificación de recursos empresariales)

FIPS Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información). Son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándades usados en las comunidades más amplias (ANSA, IEEE, ISO, etc).

HSM Hardware Security Module

IEC International Electrotechnical Commission

ISO International Organization for Standardization

ITU International Telecommunication Union

NIF Número de Identificación Tributaria

NIT Número de Identificación Tributaria

NOC Network Operation Center

OCSP Online Certificate Status Protocol (Servicio del estado del certificado en línea)

ONAC Organismo Nacional de Acreditación de Colombia

PKI Public Key Infrastructure (Infraestructura de clave pública)

PQRS Peticiones, Quejas, Reclamos y Solicitudes

RFC Request For Comments. Son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento del Internet y otras redes de computadoras, como protocolos, procedimientos, etc.

SAR Signe Autoridad de Registro

SOC Security Operation Center

TSA Time Stamping Authority (Autoridad de sellado de tiempo)

TSU Time Stamping Unit (Unidad de sellado de tiempo)

2 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

Declaración de Prácticas de Certificación (DPC) y Contrato de Suscripción

http://thsigne.com/cps

https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/

2.2 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Comité de Sistemas de Gestión de Thomas Signe S.A.S. se encarga de la aprobación de la DPC y el Contrato de Suscripción publicados en http://thsigne.com/cps.

El Responsable de Sistemas de Gestión, el Responsable de Registro Digital y el Administrador del Sistema de la CA son los responsables de la información publicada en la página web de Thomas Signe S.A.S www.thomas-signe.co

2.3 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Declaración de Prácticas de Certificación (DPC) y Contrato de Suscripción

Thomas Signe S.A.S publicará en su página web cada nueva versión aprobada de la DPC y el Contrato de Suscripción, sustituyendo a la anterior versión que no se mantendrá en la página web.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Los repositorios disponibles antes mencionados son de libre acceso para su consulta al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de Thomas Signe S.A.S..

La organización cuenta con los recursos y procedimientos necesarios para restringir el acceso a estos repositorios con otros fines diferentes a la consulta por parte de personas ajenas a Thomas Signe S.A.S.

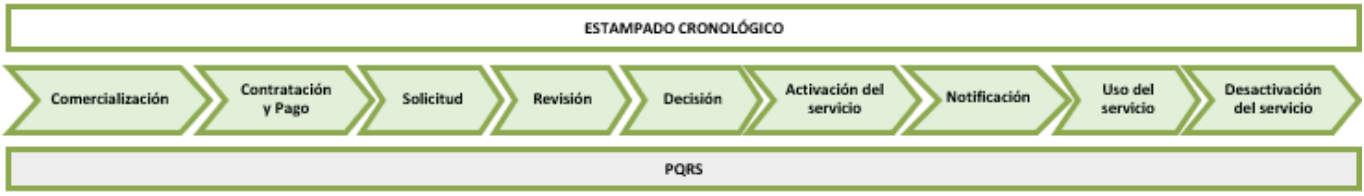
3 CARACTERÍSTICAS DE LOS SELLOS DE TIEMPO

Los sellos de tiempo emitidos por la TSA de Thomas Signe S.A.S. cumplen lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA y la TSU de Thomas Signe S.A.S. (ver sección 1.4).
- Cada sello de tiempo tiene asignado un identificador único, igual a un número entero aleatorio de 20 bytes.
- El sello de tiempo incluye el resumen de los datos firmados (HASH) incluido en la correspondiente petición de sello de tiempo.
- Si la petición de sello tiempo contiene un campo *nonce*, éste se incluye con el mismo valor en el sello de tiempo.
- El sello de tiempo está firmado por una clave generada para este propósito, correspondiente a la TSU de la TSA de Thomas Signe S.A.S.
- El algoritmo de hash de firma de los sellos de tiempo es SHA-256.
- El tiempo incluido en los sellos de tiempo está provisto mediante consulta al Instituto Nacional de Metrología (INM) de Colombia (fuente de tiempo confiable).
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable.
- El tiempo incluido en el sello de tiempo está sincronizado con la hora UTC de la fuente de tiempo confiable dentro de la precisión de +/- 1 segundo, la cual se incluye en el sello de tiempo (el valor del campo *accuracy* en el sello de tiempo es 1 segundo).
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada, los sellos de tiempo no se emiten.
- La sincronización del reloj se mantiene aun cuando se presenta un cambio en el tiempo notificado por una Autoridad Competente. El cambio se realiza cuando el cambio en el tiempo se encuentra debidamente planificado.

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

El ciclo de vida del servicio de estampado cronológico brindado por Thomas Signe S.A.S. se extiende desde la comercialización hasta la transición de salida o terminación del contrato entre el Cliente y Thomas Signe S.A.S.



4.1 QUIÉN PUEDE SOLICITAR EL SERVICIO

Puede solicitar el servicio de estampado cronológico cualquier Persona Natural que se encuentre habilitada para realizar lo siguiente:

En caso de que el Suscriptor sea una Persona Natural:

- Sustentar su identidad (Solicitante), mediante su Cédula de ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- No encontrarse vinculada a actividades que puedan dañar la imagen de la ECD.

En caso de que el Suscriptor sea una Persona Jurídica:

- Sustentar su identidad (Solicitante), mediante su Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Sustentar la existencia de la Persona Jurídica, mediante:
    - Certificado de existencia y representación legal en Cámara de Comercio o documento equivalente, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
    - Registro Único Tributario o documento equivalente, en todos los casos; expedido en Colombia (por defecto) o en otro país.
- En caso de que el Solicitante no sea el Representante Legal de la Persona Jurídica, evidenciar la autorización otorgada al Solicitante.
- No encontrarse vinculada a actividades que puedan dañar la imagen de la ECD.

4.2 COMERCIALIZACIÓN

El Solicitante podrá recibir información acerca del proceso de certificación digital, requisitos, tarifas u otros relativos; por cualquiera de las siguientes vías:

- Consultando la página web www.thomas-signe.co
- Mediante el correo electrónico comercial@thomas-signe.co
- El trato directo con Agentes comerciales.

Cuando el Solicitante se comunique con el Área Comercial manifestando que se encuentra interesado en el servicio de estampado cronológico, dicha Área le enviará: la Propuesta Comercial, en los casos que sea aplicable; el Contrato de Suscripción o de Prestación de Servicios; un Formulario de Solicitud, en los casos que sea aplicable, que solicitará la siguiente información:

- Paquete requerido de acuerdo a la Propuesta comercial
- Tipo y Número de Documento de identidad del Solicitante
- Nombres y apellidos del Solicitante
- Ciudad del Solicitante
- Teléfono del Solicitante

- Correo electrónico del Solicitante
- Nombre o Razón social de la Persona Jurídica (sólo si el Suscriptor es una Persona Jurídica)
- NIT de la Persona Jurídica (sólo si el Suscriptor es una Persona Jurídica)

4.3 CONTRATACIÓN Y PAGO

Para proceder con la contratación y el pago, el Solicitante y/o el Suscriptor deberán, en los casos que sea aplicable:

- Realizar el pago de la tarifa respectiva por un método válido, en los casos que sea aplicable. La evidencia de este proceso será el voucher o comprobante de pago.

  Thomas Signe S.A.S. pone a disposición del público una cuenta bancaria para realizar el depósito de la cuantía respectiva a cada servicio (ver sección 9.1). En la Propuesta Comercial se indicarán los datos de esta cuenta bancaria. No obstante, Thomas Signe S.A.S. puede precisar un método alternativo de pago en el caso de un Contrato de Prestación de Servicios.

- Aprobar todos los términos y condiciones dispuestos en el Contrato de Suscripción o de Prestación de Servicios entre Thomas Signe S.A.S. y el Suscriptor, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Suscripción Contrato de Suscripción o de Prestación de Servicios firmado.

4.4 SOLICITUD

Para solicitar el servicio, el Solicitante deberá, en los casos que sea aplicable, responder el correo electrónico del Área Comercial, adjuntando los documentos indicados a continuación:

En caso de que el Suscriptor sea una Persona Natural:

- Documento de identidad del Solicitante escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Formulario de Solicitud completado y firmado, en los casos que sea aplicable.
- Constancia del pago de la tarifa del paquete elegido indicada en la Propuesta Comercial o en el Contrato de Prestación de Servicios, en los casos que sea aplicable.
- Contrato de Suscripción o de Prestación de Servicios firmado.

En caso de que el Suscriptor sea una Persona Jurídica:

- Documento de identidad del Solicitante escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Formulario de Solicitud completado y firmado, en los casos que sea aplicable.
- Certificado de existencia y representación legal en Cámara de Comercio o documento equivalente de la Persona Jurídica, en copia virtual o escaneado, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país (documento equivalente) un máximo de 30 días antes.
- Registro Único Tributario o documento equivalente de la Persona Jurídica, en copia virtual o escaneado, en todos los casos; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- En caso de que el Solicitante no sea el Representante Legal de la Persona Jurídica:
    - Autorización firmada por el Representante Legal con los datos de la persona autorizada a solicitar el servicio.
    - Documento de identidad del Representante Legal que firma la autorización escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).

- Constancia del pago de la tarifa del paquete elegido indicada en la Propuesta Comercial, en los casos que sea aplicable.
- Contrato de Suscripción o de Prestación de Servicios firmado.

4.5 REVISIÓN

El Área Comercial se encarga de revisar que todos los datos fueron cumplimentados correctamente en el Formulario de Solicitud, en los casos que sea aplicable, y que se adjuntaron los documentos correctos de las evidencias de identidad, contratación y pago.

Si hace falta regularizar pagos o documentación, se notificará lo requerido a la dirección de correo electrónico declarada por el Solicitante.

4.6 DECISIÓN

La ECD Thomas Signe S.A.S. es responsable de la decisión tomada con respecto a la certificación digital. Para lo cual, el Área Comercial, una que vez que ha realizado la revisión de los documentos presentados en la solicitud, tomará la decisión de otorgar o de cancelar el servicio solicitado al Suscriptor.

En el caso de cancelación, el Área Comercial enviará un correo electrónico al Solicitante y al Suscriptor notificándoles las razones de la decisión de no otorgar el servicio solicitado.

En el caso de tomar la decisión de otogar el servicio al Suscriptor, el Área Comercial se comunicará con un Operador del Servicio de la TSA, enviándole toda la información necesaria para realizar los trabajos de activación del servicio para el Suscriptor.

4.7 ACTIVACIÓN DEL SERVICIO

El Operador del Servicio de la TSA contactado realizará la configuración en el servicio de estampado cronológico para su uso por el Suscriptor, conforme a la información que le ha proporcianado el Área Comercial.

Una vez finalizada su configuración, el servicio quedará activado para su uso por el Suscriptor, y el Operador del Servicio de la TSA se lo comunicará al Área Comercial, para que ésta realice la notificación al Solicitante y al Suscriptor.

4.8 NOTIFICACIÓN

La ECD Thomas Signe S.A.S. notificará al Solicitante y al Suscriptor la activación del servicio adquirido y les suministrará la documentación de la certificación digital. Para lo cual, una vez activado el servicio para su uso por el Suscriptor, el Área Comercial enviará un correo electrónico al Solicitante y al Suscriptor que incluye lo siguiente:

- Documento de datos del servicio adquirido, que constituye la documentación formal del servicio de certificación digital, con el siguiente contenido: datos de contacto de la ECD Thomas Signe S.A.S.; información sobre las características del servicio adquirido (servicio de estampado cronológico, fechas de activación y de término de uso del servicio, paquete del servicio), datos de contacto del Suscriptor; datos necesarios para la configuración y el uso del servicio por el Suscriptor; firma de la persona del Área Comercial que ha tomado la decisión de otorgar el servicio al Suscriptor.
- Enlace a la página web donde se encuentra publicada la presente DPC.
- Manual de uso y/o de integración del servicio de estampado cronológico en su versión vigente, en los casos que sea aplicable.

4.9 USO DEL SERVICIO

Durante el periodo contratado o hasta llegar al límite de sellos de tiempo del paquete contratado, Thomas Signe S.A.S. garantiza a los Suscriptores una adecuada prestación del servicio de estampado cronológico adquirido, mediante lo mencionado a continuación:

- Se prestará el servicio de estampado cronológico conforme al Contrato de Prestación de Servicios o de Suscripción y a la Propuesta Comercial acordados. Se efectuará un monitoreo constante y automático del rendimiento del servicio.
- Se prestará el servicio complementario de atención a PQRS
- , para resolver peticiones, quejas, reclamos y solicitudes.

4.10 DESACTIVACIÓN DEL SERVICIO

Al finalizar el periodo contratado por el Suscriptor o al llegar al límite de sellos de tiempo del paquete contratado por el Suscriptor, se efectuará automáticamente la desactivación del servicio de estampado cronológico para el Suscriptor, de forma que no se le permita su uso. Finalmente, se enviará automáticamente un correo electrónico al Suscriptor notificándole el motivo de cancelar el servicio (fin del periodo contratado o límite alcanzado de sellos de tiempo del paquete contratado).

Por otro lado, antes de finalizar el periodo contratado o de llegar al límite de sellos de tiempo del paquete contratado, en los casos de terminación especificados en el Contrato de Suscripción o de Prestación de Servicios, el Área Comercial tomará la decisión de cancelar el servicio de estampado cronológico para el Suscriptor. En estos casos, el Área Comercial se comunicará con un Operador del Servicio de la TSA, enviándole toda la información necesaria para realizar la desactivación del servicio, y el Operador del Servicio de la TSA contactado realizará la configuración en el servicio para no permitir su uso al Suscriptor. Finalmente, el Área Comercial enviará un correo electrónico al Suscriptor notificándole las razones de la decisión de cancelar el servicio.

4.11 DISPONIBILIDAD DEL SERVICIO

El servicio de estampado cronológico estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la ECD, esta realizará los mayores esfuerzos para asegurar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo de 8 horas.

5 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Los sistemas y equipamientos empleados para las operaciones del servicio de certificación digital se encuentran administrados en los Centros de Datos subcontratados.

Los controles de seguridad abarcan el ambiente físico, las redes, los sistemas, entre otros; los cuales se especifican a continuación.

Todos los controles de seguridad física están descritos en el procedimiento GSIGNE-SI-PR-11 Seguridad física y del entorno.

5.1 CONTROLES FÍSICOS

La ECD tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La seguridad física y ambiental aplicable al servicio de estampado cronológico ofrece protección frente:

- Accesos físicos no autorizados.

- Desastres naturales.

- Incendios.

- Fallo de los sistemas de apoyo (energía eléctrica, telecomunicaciones, etc.)

- Inundaciones.

- Robo.

- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios de la ECD.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos.

5.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Las instalaciones de la ECD están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y están ubicadas en una zona de bajo riesgo de desastres y permiten un rápido acceso.

La sala donde se realizan las operaciones criptográficas posee falso suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

5.1.2 ACCESO FÍSICO

El acceso físico a las dependencias donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

El acceso está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión.

El acceso a las salas se realiza con lectores de tarjeta de identificación

5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones de la ECD disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 EXPOSICIÓN AL AGUA

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

5.1.6 SISTEMA DE ALMACENAMIENTO

Los sistemas de los servidores se ejecutan mediante el despliegue de un entorno virtualizado en alta disponibilidad, soportado sobre dispositivos redundantes de computación, almacenamiento de alto rendimiento y redes independientes de producción, gestión y almacenamiento.

5.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado, mediante su destrucción física o haciendo ilegible la información contenida.

5.1.8 COPIAS DE SEGURIDAD FUERA DE LA INSTALACIÓN

La ECD mantiene un almacén externo seguro para la custodia de documentos en papel, y de dispositivos y documentos electrónicos independiente de los Centros de Datos.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 CONTROLES DE PROCEDIMIENTO

5.2.1 ROLES DE CONFIANZA

Se cuenta con roles de confianza para la administración y la operación de las plataformas de la TSA de Thomas Signe S.A.S, destinadas a la generación de las claves y a la administración y la operación del servicio de estampado cronológico de la TSA de Thomas Signe S.A.S.

Los roles de confianza establecidos en el documento THS-CO-RRHH-PR-01 Funciones y Responsabilidades para la administración y la operación de estas plataformas son:

- Gerente de Sistemas de la Información: responsable general de los procesos de certificación digital, registro y servicios de firma digital y protección de mensajes de datos. Dentro de las plataformas de la TSA de Thomas Signe S.A.S., cumple el rol de Auditor de la TSA.
- Responsable de Certificación Digital: responsable de administrar la infraestructura técnica de servicios electrónicos de la ECD, bajo el cumplimiento de las Prácticas de Certificación. Dentro de las plataformas de la TSA de Thomas Signe S.A.S., cumple los roles de Administrador de la TSA y Auditor de la TSA.
- Responsable de Registro Digital: responsable de la configuración de las plataformas de la RA de Thomas Signe, de la supervisión de las operaciones realizadas en dichas plataformas por los operadores con los demás roles, de la activación y la desactivación de los servicios de sellado de tiempo y de archivo y conservación de mensajes de datos, y de los trabajos de transición de entrada y salida de los servicios de archivo y conservación de mensajes de datos. Dentro de las plataformas de la TSA de Thomas Signe S.A.S., cumple el rol de Operador del Servicio de la TSA.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Thomas Signe S.A.S. garantiza al menos dos personas para realizar las tareas que requieren control multipersona, según el procedimiento THS-CO-AC-PR-10 Gestión de acceso al Sistema de la CA, y que se detallan a continuación:

- La generación de las claves de la TSU.
- La recuperación de un back-up de la clave privada de la TSU.
- La emisión del certificado de la TSU.

- La revocación del certificado de la TSU.
- Activación de la clave privada de la TSU.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada rol de confianza de las plataformas de la TSA se autentica mediante la utilización de mecanismos de autenticación seguros. La autenticación dentro de estas plataformas permite el acceso a determinados activos de información de Thomas Signe S.A.S.

Cada persona controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

5.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

La segregación de funciones e incompatibilidades se determinan en el documento THS-CO-RRHH-PR-01 Funciones y Responsabilidades.

Los roles de Auditor de la TSA y Administrador de la TSA son incompatibles con el rol de Operador del Servicio de la TSA.

5.3 CONTROLES DE PERSONAL

5.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables sin supervisión lleva al menos dos meses trabajando para la ECD con una relación laboral indefinida.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

La ECD retirará de sus funciones de confianza a un empleado cuando tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

Existe un procedimiento del Grupo Signe GSIGNE-RRHH-PR-02 Selección de personal que define todos los requisitos para la selección de personal para los roles profesionales.

5.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Se realizan investigaciones pertinentes antes de la contratación de cualquier persona.

5.3.3 REQUISITOS DE FORMACIÓN

Se llevan a cabo los cursos necesarios al personal para asegurar la correcta realización de las tareas asignadas a sus respectivos roles, y en función de los conocimientos personales de cada persona.

Existe un procedimiento, GSIGNE-RRHH-PR-03 Formación, que determina las acciones que realizan las empresas del grupo para una adecuada formación. También existe un plan anual de formación.

5.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se realizarán actualizaciones de formación al personal cuando se realicen modificaciones en las tareas asignadas a un rol que así lo requieran, o cuando lo solicite alguna persona.

5.3.5 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Se dispone de un régimen sancionador interno (GSIGNE-RRHH-PR-05 Procedimiento Sancionador) por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

5.3.6 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados de las empresas de infraestructura tecnológica y de servicios locales de Thomas Signe S.A.S. que tengan un rol asignado dentro de la actividad de Thomas Signe S.A.S para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y la de requerimientos operacionales y aceptación del rol empleados por Thomas Signe S.A.S.. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

5.3.7 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Thomas Signe S.A.S. pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Thomas Signe S.A.S. registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la ECD. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados a los sistemas de la ECD a través de la red.
- Registros de las aplicaciones de la ECD.
- Encendido y apagado de las aplicaciones de la ECD.
- Cambios en la configuración de la ECD y/o sus claves.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al módulo criptográfico.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Thomas Signe S.A.S. conserva, ya sea manual o electrónicamente, la siguiente información:

- Las actas de creación de claves de la TSA.
- Cambios en el personal que realiza tareas de confianza.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con las clave privadas de la ECD.

5.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOGS)

Se revisarán los logs de auditoría trimestralmente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

5.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría por un periodo de tres (03) años para garantizar la seguridad del sistema.

5.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de los sistemas son protegidos de su manipulación mediante mecanismos que aseguran su integridad.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Thomas Signe S.A.S. dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Se realizan copias diarias incrementales y completas semanales.

Adicionalmente se mantiene copia de los logs de auditoría en centro de custodia externo.

5.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

5.4.7 ANÁLISIS DE VULNERABILIDADES

La ECD realiza periódicamente una revisión de vulnerabilidades y test de intrusión para analizar la infraestructura de la ECD. Después se analizaran y se corregirán las vulnerabilidades que la ECD crea que son un riesgo para ella.

5.4.8 SUPERVISIÓN

Thomas Signe dispone de un SOC (Security Operation Center) y un NOC (Network Operation Center) para monitorizar todas las tareas de supervisión de la seguridad y las comunicaciones de los servicios ofrecidos.

Estos centros de operación están descritos en el procedimiento GSIGNE-SI-PR-11 Seguridad física y del entorno, y están en áreas seguras.

5.5 ARCHIVO DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

La ECD Thomas Signe S.A.S. conservará los datos del sistema que tengan lugar durante el ciclo de vida del servicio. Por lo tanto, se almacenarán:

- todos los registros de auditoría (logs),

- todos los datos relativos a los contratos con los suscriptores y los datos relativos a su identificación,

La ECD es responsable del correcto archivo de todo este material y documentación.

5.5.2 PERIODO DE CONSERVACIÓN DE REGISTROS

Los datos del sistema relativos al ciclo de vida del servicio se conservarán de acuerdo con la tabla de retención documental. Los datos se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos siete (07) años desde su finalización.

5.5.3 PROTECCIÓN DEL ARCHIVO

Thomas Signe S.A.S. asegura la correcta protección de los archivos, incluyendo, entre otros, la información que se recopila con el fin de expedir los sellos de tiempo, mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones externas a los Centros de Datos de la ECD en los casos en que así se requiera.

Además, se dispone de documentos técnicos y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.4 PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO

Thomas Signe S.A.S. dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

5.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los registros están fechados con la fuente fiable del Instituto Nacional de Metrología (INM) de Colombia, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”. Como fuente de tiempo secundaria, se utiliza la Sección de Hora del Real Instituto y Observatorio de la Armada en España.

Existe dentro de la documentación técnica y de configuración de la ECD un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

5.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNO O EXTERNO)

El sistema de archivo de la información de auditoría de la ECD es interno, si bien se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Los eventos registrados están protegidos contra manipulaciones no autorizadas.

Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

5.6 CAMBIO DE CLAVES

El procedimiento para proporcionar, en caso de cambio de claves de la TSA, una nueva clave pública de la TSA a los Terceros aceptantes de los sellos de tiempo emitidos con las nuevas claves es el mismo que para proporcionar la actual clave pública de la TSA.

En consecuencia, el nuevo certificado de TSU conteniendo su nueva clave pública estará contenido en los sellos de tiempo emitidos con esa nueva clave.

5.7 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Thomas Signe S.A.S. tiene establecido y probado el plan de continuidad y contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio (procedimiento GSIGNE-SI-PR-17 Aspectos de Seguridad de la Informacion para la GCN).

Cualquier fallo en la consecución de las metas marcadas por este plan de continuidad y contingencia será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la ECD para implementar dichos procesos.

El procedimiento de seguridad para el manejo de incidentes, definido en el procedimiento GSIGNE-SI-PR-16 Gestión de incidentes de Seguridad de la Información, cumple con el anexo A de la norma ISO 27001.

Como parte de los incidentes de seguridad que son registrados por Thomas Signe S.A.S., se encuentran:

- Cuando la seguridad de una llave privada de la ECD se ha visto comprometida.
- Cuando el sistema de seguridad de la ECD ha sido vulnerado.
- Cuando se presenten fallas en el sistema de la ECD que comprometan la prestación del servicio.
- Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el Suscriptor.
- Cuando se presente cualquier otro evento o incidente de seguridad de la información.

5.7.1 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE

El plan de contingencia de la jerarquía de Thomas Signe S.A.S. trata el compromiso de una clave privada de la ECD como un desastre.

En caso de compromiso de la clave privada de la TSA o de la CA que ha emitido el certificado de la TSA (CA Raíz de Thomas Signe S.A.S.), la seguridad del servicio de estampado cronológico se verá afectada gravemente, y se procederá según el procedimiento THS-CO-AC-PR-05 Gestión de claves a:

- Informar a todos los suscriptores, usuarios y otras ECD con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de Thomas Signe S.A.S.
- Indicar que los sellos de tiempo firmados usando esta clave no son válidos.

5.7.2 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Thomas Signe S.A.S. ha desarrollado el plan de continuidad para recuperar todos los sistemas después de un desastre según los procedimientos GSIGNE-SI-PR-17 Aspectos de Seguridad de la Información para la GCN y THS-CO-SI-PR-01 Gestión del riesgo - 03 BIA - DRP.

5.8 CESE DEL SERVICIO DE ESTAMPADO CRONOLÓGICO

Ante el cese de servicios de estampado cronológico de la ECD Thomas Signe S.A.S. se procederá según el procedimiento THS-CO-AC-PR-01 Procedimiento de Cesación de servicios de la siguiente forma:

- Informar en primera instancia a ONAC y a la Superintendencia de Industria y Comercio acerca del cese de actividades con una anticipación de treinta (30) días y solicitar su autorización.

- Luego de haber sido autorizado, informar por medio de dos avisos publicados en diarios de amplia difusión y por el correo electrónico declarado, a todos los suscriptores con un intervalo de quince (15) días sobre la terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de ésta respecto de los sellos de tiempo expedidos.

En cualquier caso, se garantiza la continuidad del servicio a los usuarios quienes ya hayan contratado los servicios de la ECD Thomas Signe S.A.S., directamente o por medio de terceros, sin ningún costo adicional a los servicios que contrató.

6 CONTROLES TÉCNICOS DE SEGURIDAD

6.1 CICLO DE VIDA DE LA GESTIÓN DE LA CLAVE

6.1.1 GENERACIÓN DE LA CLAVE PRIVADA DE LA TSU

La generación de la clave privada de la TSU es realizada en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628), en un dispositivo criptográfico hardware (HSM) certificado FIPS 140-2 nivel 3, por personal autorizado con un control dual.

6.1.2 PROTECCIÓN DE LA CLAVE PRIVADA DE LA TSU

La clave privada de la TSU es resguardada durante su uso en dispositivos criptográficos hardware (HSM) certificados FIPS 140-2 nivel 3 y su administración es protegida por al menos dos personas. Las copias de respaldo se almacenan en un módulo criptográfico del mismo nivel de seguridad.

6.1.3 DISTRIBUCIÓN DE LA CLAVE PÚBLICA DE LA TSU

La clave pública de la TSU está contenida dentro de un certificado X.509 v3, firmado digitalmente por la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S. (Thomas Signe Root), regulada por la DPC para la emisión de certificados de Thomas Signe S.A.S.

Este certificado de la TSU está contenido en los sellos emitidos por Thomas Signe S.A.S. firmados con la clave privada asociada.

6.1.4 RE-EMISIÓN DE LA CLAVE DE LA TSU

La clave privada de la TSU de Thomas Signe S.A.S. será reemplazada antes de la expiración de su periodo de validez y en caso de obsolescencia o vulnerabilidad declarada del algoritmo, del tamaño de la clave o de otra medida de seguridad relevante.

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

Las claves privadas con las cuales se firman los sellos de tiempo emitidos por Thomas Signe S.A.S., no serán usadas luego de terminado su ciclo de vida sino que será emitida una nueva clave privada de la TSU y puesta en operación, realizando el cambio de un certificado digital por otro, incluyendo la generación segura y la distribución del nuevo certificado.

La clave privada de la TSU cuyo certificado ha expirado o ha sido revocado, o cualquier parte de ella, incluyendo cualquier copia, será destruida de modo que no pueda ser recuperada.

6.1.6 TAMAÑO DE LAS CLAVES Y PERIODO DE VALIDEZ

Certificado	Tamaño claves RSA (bits)	Periodo validez
TSU	2048	Desde: 05/04/2018 09:09:36, tiempo UTC Hasta: 14/03/2038 00:00:00, tiempo UTC

6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos empleados para generar y almacenar las claves de la TSU (HSM) están certificados con la norma FIPS 140-2 nivel 3.

6.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

El acceso a la clave privada de la TSU se encuentra bajo control multipersona, requiriendo 2 de 3 personas autorizadas, con uso de sus respectivos dispositivos criptográficos protegidos con un PIN, para el acceso y activación de la mencionada clave privada.

Dicho control garantiza que una persona no posea el control individual, descentralizando la responsabilidad de activar y usar la clave privada de la TSU.

6.2.3 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la TSU está custodiada por dispositivos criptográficos hardware (HSM) certificados con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación de la clave privada requiere el control multipersona detallado en la sección 6.2.2.

6.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Existen unos dispositivos que permiten la restauración de la clave privada de la TSU, que son almacenados de forma segura y sólo accesibles por personal autorizado, usando distintos controles, siendo uno de ellos el control dual en un medio físico seguro.

La clave privada de la TSU se pueden restaurar por un proceso que requiere la utilización de 2 de 3 dispositivos criptográficos.

6.2.5 ARCHIVO DE LA CLAVE PRIVADA

Thomas Signe S.A.S. no archivará la clave privada de firma de sellos de tiempo de la TSU después de la expiración del periodo de validez de la misma.

6.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA A O DESDE UN MÓDULO CRIPTOGRÁFICO

La clave privada de la TSU se puede transferir a o desde un módulo criptográfico (HSM) por un proceso que requiere la utilización de 2 de 3 dispositivos criptográficos.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRIPTOGRÁFICO

Existe un documento de ceremonia de claves de Thomas Signe S.A.S., donde se describen los procesos de generación y almacenamiento de las claves privada por los módulos criptográficos empleados (HSM).

6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la TSU se activa en sus HSM por un proceso que requiere la utilización de 2 de 3 dispositivos criptográficos, los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.

6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la TSU sólo se desactivará en sus HSM en situaciones extraordinarias.

6.2.10 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

La destrucción de la clave privada de la TSU se realiza según el procedimiento THS-CO-AC-PR-05 Gestión de claves, por personal autorizado.

Se realizará un borrado seguro de la clave privada de la TSU, utilizando las funciones que proveen los dispositivos criptográficos hardware empleados (HSM), de forma que no resulten afectadas el resto de claves gestionadas por los dispositivos.

Asimismo, se realizará un borrado seguro de todas las copias de seguridad de la clave privada de la TSU, las cuales habrán sido identificadas.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

No se contemplan.

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada de la TSU fueron generados de forma segura durante la ceremonia de claves de Thomas Signe S.A.S.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Sólo el personal autorizado tiene acceso/conocimiento a/de los datos de activación de la clave privada de la TSU.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Thomas Signe S.A.S. emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Thomas Signe S.A.S., en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.

- Configuración de seguridad de las aplicaciones.

- Dimensionamiento correcto del sistema.

- Configuración de usuarios y permisos.

- Configuración de eventos de log.

- Plan de backup y recuperación.

- Requerimientos de tráfico de red.

La documentación técnica y de configuración de Thomas Signe S.A.S. detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de Thomas Signe S.A.S. incluye las siguientes funcionalidades:

- Control de acceso a los servicios de Thomas Signe S.A.S. y gestión de privilegios.

- Imposición de separación de tareas para la gestión de privilegios.

- Identificación y autenticación de roles asociados a identidades.

- Archivo del historial del Suscriptor y de Thomas Signe S.A.S. y datos de auditoría.

- Auditoría de eventos relativos a la seguridad.

- Auto-diagnóstico de seguridad relacionado con los servicios de Thomas Signe S.A.S.

- Mecanismos de recuperación de claves y del sistema de Thomas Signe S.A.S.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en los Centros de Datos subcontratados.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Thomas Signe S.A.S. posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Gestión de seguridad

Thomas Signe S.A.S. desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad.

Clasificación y gestión de información y bienes

Thomas Signe S.A.S. mantiene un inventario de activos y documentación.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

Operaciones de gestión

Thomas Signe S.A.S. dispone de procedimientos de gestión de incidencias (GSIGNE-SI-PR-16 Gestión de incidentes de Seguridad de la Información) y de la continuidad del negocio (GSIGNE-SI-PR-17 Aspectos de Seguridad de la Informacion para la GCN).

Thomas Signe S.A.S. dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

Thomas Signe S.A.S. tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el proceso de certificación.

Tratamiento de los soportes y seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planning del sistema

El departamento de Sistemas de Thomas Signe S.A.S. mantiene un registro de las capacidades de los equipos.

Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Gestión del sistema de acceso

Thomas Signe S.A.S. realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de Thomas Signe S.A.S.:

- Se dispone de controles basados en firewalls en alta disponibilidad.

- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.

- Se dispone de un procedimiento de cambio de titulares y cambio de custodios de las cajas fuertes.

- Se dispone de un procedimiento para asegurar que las operaciones se realizan respetando los roles establecidos.

- Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.

- El personal de Thomas Signe S.A.S. será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación de los sellos de tiempo:

- Las instalaciones de la ECD están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar ante un intento de acceso a sus recursos no autorizado y / o irregular.

- La autenticación para realizar el proceso de emisión de sellos de tiempo se realiza mediante un sistema n de m operadores para la activación de la clave privada de la TSA de Thomas Signe S.A.S.

Gestión del ciclo de vida del hardware criptográfico de la TSU

- Thomas Signe S.A.S. se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.
- El hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.
- Thomas Signe S.A.S. registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Thomas Signe S.A.S.
- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
- Thomas Signe S.A.S. realiza tests periódicos para asegurar el correcto funcionamiento de los dispositivos.
- Los dispositivos criptográficos solo son manipulados por personal confiable
- La clave privada de firma de la TSU almacenada en el hardware criptográfico se eliminará una vez que se hayan retirado los dispositivos.
- La configuración del sistema de la ECD así como sus modificaciones y actualizaciones son documentadas y controladas.
- Thomas Signe S.A.S. posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7 CONTROLES DE SEGURIDAD DE LA RED

La ECD protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

6.8 SELLADO DE TIEMPO

El tiempo para los servicios de la ECD se obtienen mediante consulta al Instituto Nacional de Metrología (INM) de Colombia, de acuerdo con lo establecido en el artículo 14 del Decreto 4175 de 2011, por el cual se escindieron unas funciones de la Superintendencia de Industria y Comercio y se creó el Instituto Nacional de Metrología –INM, a partir del 3 de noviembre del año 2011 esta última institución es la encargada de mantener, coordinar y difundir la hora legal de la República de Colombia, adoptada mediante Decreto 2707 de 1982.

Los servidores se mantienen actualizados con la hora UTC, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 5905 “Network Time Protocol Version 4: Protocol and Algorithms Specification”.

7 PERFILES DE CERTIFICADO

7.1 PERFIL DE CERTIFICADO DE TSU

7.1.1 FORMATO DEL CERTIFICADO

El formato del certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S cumple lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

Adicionalmente, el certificado de TSU de la TSA de la ECD Thomas Signe S.A.S. es coherente con lo dispuesto en los siguientes estándares:

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

El certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S ha sido emitido por la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S. (Thomas Signe Root).

El tamaño de claves y perio de validez del certificado se indica en la sección 6.1.6

7.1.2 EXTENSIONES DEL CERTIFICADO

En la tabla siguiente se especifican las extensiones del certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S.

Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S., obtenido a partir del hash SHA-1 de la misma
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	digitalSignature nonRepudiation
Certificate Policies	-	OID 1.3.6.1.4.1.51362.0.1.1.1 URI de la DPC: http://thsigne.com/cps
Basic Constraints	Sí	cA: FALSE
Extended Key Usage	Sí	timeStamping (1.3.6.1.5.5.7.3.8)
CRL Distribution Points	-	URI de la CRL: http://crl.thsigne.com/thomas_signe_root.crl
Authority Information Access	-	URI del certificado de la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S.: http://thsigne.com/certs/thomas_signe_root.crt

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Nombre	OID	Descripción
sha256WithRSAEncryption	1.2.840.113549.1.1.11	Algoritmo de firma del certificado de TSU
rsaEncryption	1.2.840.113549.1.1.1	Algoritmo de clave pública en certificado de TSU Algoritmo de firma de sellos de tiempo
id-sha256	2.16.840.1.101.3.4.2.1	Algoritmo de hash de firma de sellos de tiempo

7.1.4 FORMATOS DE NOMBRES

En la tabla siguiente se especifican los correspondientes atributos del DN del certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S.

Atributo del DN	Descripción	Valor
Country Name (C)	País	CO [1]
State or Province Name (ST)	Estado/Provincia	Distrito Capital [2]
Locality Name (L)	Localidad	Bogotá [2]
Street Address (STREET)	Dirección	see current address at www.thomas-signe.com [2]
Organization Identifier (2.5.4.97)	Identificador de Organización	900962071-5 [2]
Organization Name (O)	Nombre de Organización	Thomas Signe Soluciones Tecnológicas Globales S.A.S. [2]
Common Name (CN)	Nombre	Thomas Signe TSA – TSU 01 [2]

7.1.5 RESTRICCIONES DE LOS NOMBRES

Según lo especificado en la sección 7.1.4 y en la DPC para la emisión de certificados de Thomas Signe S.A.S.

7.1.6 IDENTIFICADORES DE OBJETO (OID) DE LAS POLÍTICAS DE CERTIFICADOS

El OID de la política del certificado de TSU de la TSA de la ECD Thomas Signe S.A.S. se encuentra especificado en las secconesn 1.4, 7.1.2 y también a continuación: 1.3.6.1.4.1.51362.0.1.1.1

7.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINTS

El certificado de TSU de la TSA de la ECD Thomas Signe S.A.S. no contiene la extensión Policy Contraints.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

---

[1] Codificado en PrintableString

[2] Codificado en UTF8String

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

7.2 PERFIL DE CRL

El estado del certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S se puede verificar mediante la consulta de la última CRL emitida por la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S. (Thomas Signe Root).

El perfil de esta CRL es conforme a lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

7.3 PERFIL DE OCSP

El estado del certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S no se puede verificar mediante la consulta de un servicio OCSP.

8 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

Thomas Signe S.A.S. se somete a las auditorías de acreditación que realiza ONAC de conformidad con los dispuesto en el artículo 162 del Decreto-ley 19 de 2012. Asimismo, de acuerdo con lo exigido en los Criterios Específicos de Acreditación de ONAC, Thomas Signe S.A.S. se somete a auditoría interna y auditoría de tercera parte en los términos previstos en dicho documento.

En caso de requerirse, Thomas Signe S.A.S. permite y facilita la realización de auditorías por parte de la Superintendencia de Industria y Comercio de Colombia.

8.1 FRECUENCIA DE LAS AUDITORÍAS

Las auditorías se realizarán con carácter anual siguiendo el procedimiento interno GSIGNE-GRAL-PR-03 Auditoria.

8.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

Las auditorías de acreditación que competen a Thomas Signe S.A.S. son realizadas por auditores designados por ONAC.

Las auditorías internas y de tercera parte se realizan por auditores que cumplan con lo establecido en los Criterios Específicos de ONAC vigentes y siguiendo el procedimiento interno GSIGNE-GRAL-PR-03 Auditoria..

8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Las empresas que realizan las auditorías externas nunca representan conflictos de intereses que puedan desvirtuar su actuación en su relación con Thomas Signe S.A.S.

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

Las auditorías verifican de forma general que se cumple con los principios establecidos en los requisitos de acreditación (Criterios Específicos de ONAC vigentes), la legislación vigente aplicable y la documentación establecida en el sistema de gestión de la ECD. Dichos aspectos de deben identificar y controlar siguiendo el procedimiento interno GSIGNE-GRAL-PR-03 Auditoria.

8.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

En caso de que sean detectadas incidencias o no-conformidades se tomarán las medidas oportunas para su resolución en el menor tiempo posible siguiendo el procedimiento interno GSIGNE-GRAL-PR-03 Auditoria.

8.6 COMUNICACIÓN DE RESULTADOS

El organismo auditor se comunicará con la ECD a través del interlocutor establecido en cada caso.

9 OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 PAQUETES

Los paquetes para el servicio de estampado cronológico que ofrece Thomas Signe S.A.S. pueden ser los siguientes:

TIPO DE PAQUETE	**N° ESTAMPAS CRONOLÓGICAS**
Paquete ilimitado	Servicio ilimitado de estampado cronológico
Paquete premium	Servicio de hasta 1.000.000 estampas cronológicas
Paquete 750 mil	Servicio de hasta 750.000 estampas cronológicas
Paquete 500 mil	Servicio de hasta 500.000 estampas cronológicas
Paquete 250 mil	Servicio de hasta 250.000 estampas cronológicas
Paquete 100 mil	Servicio de hasta 100.000 estampas cronológicas
Paquete 50 mil	Servicio de hasta 50.000 estampas cronológicas
Paquete 20 mil	Servicio de hasta 20.000 estampas cronológicas
Paquete 10 mil	Servicio de hasta 10.000 estampas cronológicas
Paquete 5000	Servicio de hasta 5.000 estampas cronológicas
Paquete 2000	Servicio de hasta 2.000 estampas cronológicas
Paquete 500	Servicio de hasta 500 estampas cronológicas

Las tarifas respectivas a cada paquete pueden ser consultadas a comercial@thomas-signe.co

En la propuesta comercial se indicará el precio final con IVA para el paquete solicitado.

9.1.2 POLÍTICA DE REEMBOLSO

La ECD Thomas Signe S.A.S. dispone de una Política de reembolso (THS-CO-AC-POL-07 Política de reembolso), que se referencia en los contratos celebrados con sus clientes y se publica en la página web de Thomas Signe.

9.2 RESPONSABILIDADES FINANCIERAS

9.2.1 COBERTURA DEL SEGURO

Thomas Signe S.A.S. dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad como ECD tal como se define en la legislación colombiana vigente.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a la exigida por la legislación colombiana vigente.

Las características de dicho seguro, son las siguientes:

- Es expedido por una entidad aseguradora vigilada por la Superintendencia Financiera de Colombia.

- Cubre riesgos y perjuicios contractuales y extracontractuales de suscriptores y terceros de buena fe.

- Cubre la restitución automática del valor asegurado.

- La entidad aseguradora, el tomador y el asegurado están obligados a informar previamente a ONAC la terminación del contrato de seguro o si se realizan modificaciones que reducen el alcance o monto de la cobertura.

El seguro se hará cargo de todas las cantidades que Thomas Signe S.A.S. resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros.

No existe cobertura para los terceros aceptantes.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

Thomas Signe S.A.S. considera confidencial toda la información que esté catalogada expresamente como confidencial. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la persona o entidad que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal, en cuyo caso, a menos que lo prohíba la ley, dicha persona o entidad será notificada de la información suministrada.

9.3.1 INFORMACIÓN CONFIDENCIAL

En particular, la siguiente información será considerada confidencial:

- Las claves privadas de la TSA de Thomas Signe S.A.S.

- Acta de generación de las claves de la TSA

- Procedimiento de generación de las claves de la TSA.

- La información de negocio suministrada y/o elaborada conjuntamente con Thomas Signe S.A.S. por parte de sus clientes, proveedores u otras personas con las que Thomas Signe se comprometió a guardar secreto establecido legal o convencionalmente.

- Los resultados de validaciones de identidad de Suscriptores y/o Solicitantes, provistas por fuentes públicas o privadas.

- La información del Suscriptor y/o Solicitante obtenida por fuentes diferentes del Suscriptor y/o Solicitante y que haya sido catalogada expresamente como confidencial.

- Los datos recogidos durante la certificación digital.

9.3.2 INFORMACIÓN NO CONFIDENCIAL

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.

- La información contenida en los sellos de tiempo, puesto que para su emisión el Suscriptor y/o Solicitante otorga previamente su consentimiento.

- Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3 RESPONSABILIDAD EN LA PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL

Es responsabilidad de la ECD Thomas Signe S.A.S. y de sus proveedores establecer medidas adecuadas para la protección de la información confidencial.

9.4 POLÍTICA DE PROTECCIÓN DE DATOS

Thomas Signe S.A.S. garantiza la protección de datos personales de los Suscriptores y/o Solicitantes de los servicios de certificación digital, en cumplimiento de la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 del 2013; de los Decretos 1377 de 2013 y 886 de 2014, ley 1266 de 2008 de demás decretos reglamentarios relacionados, donde se reglamenta lo establecido en la Ley 1581 de 2012, por la cual se expidió el Régimen General de Protección de Datos Personales, cuyo objeto es "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma" y de los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-3.0-07 vigente.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico, y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los Suscriptores y/o Solicitantes. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de certificación digital estipuladas, a excepción que exista un previo consentimiento del usuario final de dichos datos o medie una orden judicial o administrativa que así lo determine, en cuyo caso, a menos que lo prohíba la ley, el Suscriptor o la persona implicada será notificada de la información suministrada.

Es responsabilidad de los Suscriptores y/o Solicitantes garantizar que la información provista a Thomas Signe S.A.S. sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

Thomas Signe S.A.S. cuenta con una Política de Privacidad de datos personales que detalla los principios, recolección y tratamiento de datos personales y que se encuentra publicada en la página web: https://thomas-signe.co/otras-politicas-y-procedimientos/.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

De conformidad con lo dispuesto por las leyes nacionales y los tratados internacionales, todos los derechos en materia de propiedad intelectual e industrial relacionados con los sistemas, documentos, procedimientos, sellos de tiempo y cualesquiera otros, relacionados con su actividad como ECD, incluida la presente DPC, corresponderán en exclusiva a Thomas Signe S.A.S.

9.6 OBLIGACIONES

9.6.1 OBLIGACIONES DE LA ECD

La ECD Thomas Signe S.A.S. se obliga según lo dispuesto en este documento, principalmente a:

a) Respetar lo dispuesto en la presente DPC, así como en el Contrato de Suscripción.

b) Publicar esta DPC y el Contrato de Suscripción en su página Web, en su versión vigente.

c) Informar sobre las modificaciones de esta DPC a los Suscriptores, Solicitantes y público en general, incluyendo dichas modificaciones en la tabla inicial de historial de versiones.

d) Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.

Por lo que a los sellos de tiempo respecta:

a) Emitir sellos de tiempo conforme a esta DPC y a los estándares de aplicación.

b) Emitir sellos de tiempo según la información que obra en su poder y libres de errores de entrada de datos.

c) Entregar los servicios con la confiabilidad y exactitud establecida en los respectivos contratos y en el presente documento.

Sobre custodia de información:

a) Conservar la información sobre el sello de tiempo emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable.

b) Proteger sus claves privadas de forma segura.

c) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.

9.6.2 OBLIGACIONES DE LOS PROVEEDORES

Los proveedores de la ECD Thomas Signe S.A.S. se encuentran obligados a cumplir con los requisitos mínimos exigidos por ONAC, dispuestos en el documento CEA 3.0-07 vigente, tales como:

a) Responsabilidad y financiación

b) Confidencialidad

c) Requisitos para los recursos

d) Requisitos del proceso – Ciclo de vida del servicio de estampado cronológico

e) Requisitos del sistema de gestión

f) Requisitos de la TSA

g) Requisitos técnicos

9.6.3 OBLIGACIONES DE LOS SOLICITANTES

El Solicitante del servicio de estampado cronológico estará obligado a cumplir con lo dispuesto por la normativa y además a:

a) Suministrar a Thomas Signe S.A.S. la información veraz y vigente.

b) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.

e) Respetar lo dispuesto en los documentos contractuales firmados con la ECD.

f) Notificar cualquier cambio en los datos aportados para la puesta en marcha del servicio durante su periodo de validez.

9.6.4 OBLIGACIONES DE LOS SUSCRIPTORES

El Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Integrar, configurar y utilizar el servicio de estampado cronológico de la ECD, conforme a las instrucciones enviadas por la ECD al Solicitante.

b) Utilizar sistemas cliente que envíen peticiones al servicio de estampado cronológico de la ECD e interpreten sus respuestas conforme al formato establecido en la RFC 3161, y que realicen las verificaciones del estado del certificado de la TSA.

c) Respetar lo dispuesto en los instrumentos jurídicos vinculantes con la ECD.

9.6.5 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los Terceros que confían estarán obligados a verificar que los documentos hayan sido firmados con un sello de tiempo, y que éste haya sido firmado con la clave privada asociada a un certificado de TSU de la TSA de la ECD de Thomas Signe S.A.S vigente en el momento de la verificación (para comprobar que la clave privada usada para firmar el sello de tiempo no ha sido comprometida).

Además será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y también:

a) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los sellos de tiempo en los que confían, y aceptar sujetarse a los mismos.

b) Notificar a Thomas Signe S.A.S. cualquier situación irregular con respecto al servicio prestado por la ECD.

9.7 RESPONSABILIDADES

9.7.1 RESPONSABILIDADES DE LA ECD

- Cumplir con los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-3.0-07 vigente, establecidos por el ONAC.

- Informar a sus proveedores de que hace extensivo a ellos el cumplimiento de los requisitos dispuestos en el documento CEA 3.0-07 vigente, cuando les corresponda.

- Informar a los Solicitantes, Suscriptores, Terceros que confían y al público en general en la página web de Thomas Signe S.A.S de las actividades y servicios acreditados atendiendo a lo establecido en el documento RAC-3.0-03 vigente de ONAC.

- Informar a los Solicitantes, Suscriptores, Terceros que confían y al público en general en la página web de Thomas Signe S.A.S de la información general de la empresa, como es su naturaleza, el tipo de empresa, etc.

- Garantizar que el servicio cumple con todos los requisitos materiales establecidos en la DPC.

- Facilitar los documentos necesarios y en su última versión al Suscriptor y al Solicitante.

- Notificar al Suscriptor acerca de los cambios en las políticas y prácticas de la ECD Thomas Signe S.A.S.

- Notificar al Suscriptor cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de Suscriptor, forma de validación de un certificado, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según los requerimientos del ONAC).

- El uso de los símbolos que caractericen la acreditación de la ECD de Thomas Signe S.A.S. estarán restringidos al alcance acreditado, y no podrán ser transferidos a terceros ni heredados fuera de los servicios

de certificación digital, personas, procesos y terceros evaluados por el ONAC; tal como lo describe el documento Política de uso de símbolos de Thomas Signe S.A.S.

- Ejercer control, sobre los servicios de certificación digital acreditados, respecto a la propiedad y el uso de símbolos, certificados, cualquier otro mecanismo para indicar que el servicio de certificación digital está acreditado.

- Las referencias al alcance de acreditación otorgado, o el uso engañoso del alcance de acreditación otorgado, los símbolos, los certificados, y cualquier otro mecanismo para indicar que un servicio de certificación digital, o que la ECD está acreditada, en la documentación o en otra publicidad estarán sujetas al cumplimiento de las Reglas de Acreditación de ONAC RAC-3.0-01 y RAC-3.0-03 vigentes .

- Atender y dar respuesta a las peticiones, quejas, reclamos y apelaciones de los Suscriptores y partes relacionadas.

- Actuar de forma imparcial de acuerdo a su Política de Imparcialidad y de No Discriminación.

9.7.2 RESPONSABILIDADES DEL SUSCRIPTOR

- Actuar conforme a lo estipulado en la presente DPC de la ECD Thomas Signe S.A.S.

- Facilitar información completa, actual y veraz a la ECD Thomas Signe S.A.S.

- Cumplir con los requisitos estipulados por Thomas Signe S.A.S. para el respectivo servicio de certicación digital.

- Cumplir con nuevos requisitos, cuando Thomas Signe S.A.S implemente cambios en los servicios de certificación digital, previa comunicación de dichos cambios por parte de la ECD al Suscriptor.

- Que las declaraciones sobre la certificación son coherentes con el alcance del servicio de certificación digital.

- No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD Thomas Signe S.A.S. y no hace ninguna declaración relacionada con su certificación que Thomas Signe S.A.S. pueda considerar engañosa o no autorizada. Lo que a su vez implica no monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica del ONAC y la ECD Thomas Signe S.A.S.; así como comprometer intencionadamente la seguridad de la Jerarquía del ONAC y la ECD Thomas Signe S.A.S.

- Inmediatamente después de la cancelación o la terminación de la certificación digital, dejar de utilizarla en todo el material publicitario que contenga alguna referencia a ella, y emprender las acciones exigidas por el servicio de certificación digital y cualquier otra medida previamente notificada.

- Cumplir con los requisitos que pueda prescribir el servicio de certificación digital con relación al uso de las marcas de conformidad y a la información relacionada con el servicio.

- Informar a la ECD, sin retraso, acerca de los cambios que puedan afectar a la certificación digital que le fue expedida por la ECD.

- Ser diligente en la custodia de su clave privada y las contraseñas de acceso que protegen su clave privada, con el fin de evitar usos no autorizados.

- En todo momento ser responsable de proteger su clave privada, las contraseñas de acceso y el dispositivo criptográfico donde se encuentra almacenada su clave privada sin poder transferir esta responsabilidad a ningún tercero.

- Informar de que cumple con lo estipulado en la DPC de Thomas Signe S.A.S., cuando haga referencia al servicio de certificación digital en medios de comunicación (artículos, documentos, folletos o publicidad).

9.8 LIMITACIÓN DE RESPONSABILIDAD

Thomas Signe S.A.S. no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

a) Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros que confían, o cualquier otro caso de fuerza mayor.

b) Por el uso indebido de la información contenida en los sellos de tiempo, en el certificado de la TSU o en la CRL.

c) Por el contenido de los mensajes o documentos con sello de tiempo.

d) En relación a acciones u omisiones del Solicitante y Suscriptor:

- Falta de veracidad de la información suministrada para solicitar el servicio

- Negligencia en conservación de sus datos de acceso al servicio, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

- Extralimitación en el uso de los sellos de tiempo, según lo dispuesto en la normativa vigente y en la presente Declaración de Prácticas de Certificación.

- Retraso en la comunicación de las causas de cancelación del servicio.

e) En relación a acciones u omisiones del Tercero que confía:

- Falta de comprobación de la pérdida de vigencia del certificado de la TSA publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma digital.

9.9 INDEMNIZACIONES

9.9.1 INDEMNIZACIONES POR DAÑOS OCASIONADOS POR LA ECD

Thomas Signe S.A.S asumirá las indemnizaciones correspondientes por daños efectuados a Solicitantes, Suscriptores, Terceros que confían o a cualquier otra parte interesada en base a los términos establecidos en la normativa reguladora de la prestación del servicio de estampado cronológico, así como a la presente DPC.

9.9.2 INDEMNIZACIONES POR LOS DAÑOS CAUSADOS POR LOS SOLICITANTES, POR LOS SUSCRIPTORES Y POR LOS TERCEROS QUE CONFÍAN

Tanto los Suscriptores, como los Solicitantes, como los Terceros que confían son responsables por apoderarse, destruir, modificar, adulterar indebidamente los datos de un sello de tiempo durante o después de la fecha de creación del sello de tiempo y estarán sujetos al pago de indemnizaciones por los corespondientes daños causados según lo establecido en la normativa reguladora de la prestación del servicio de estampado cronológico.

9.10 PERIODO DE VALIDEZ

9.10.1 PLAZO

Esta DPC entrará en vigor desde el momento de su publicación en la página web de Thomas Signe S.A.S y permanecerá en vigor mientras no se deroguen expresamente por la publicación de una nueva versión.

9.10.2 SUSTITUCIÓN Y DEROGACIÓN DE LA DPC

Esta DPC será sustituida por nuevas versiones con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad. Cuando la DPC quede derogada se retirará de la página web de Thomas Signe S.A.S, si bien se conservará durante al menos tres (03) años desde su finalización o el periodo que establezca la legislación vigente.

9.10.3 EFECTOS DE LA FINALIZACIÓN

Las obligaciones y restricciones que establece esta DPC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de Thomas Signe S.A.S nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11 PQRS

Las peticiones, quejas, reclamos y solicitudes (PQRS) sobre los servicios prestados por Thomas Signe S.A.S., son recibidas directamente por el Responsable de PQRS de la ECD.

Los Solicitantes, Suscriptores, Terceros que confían o el público en general indicarán su PQRS con respecto a los servicios de certificación digital ofrecidos por Thomas Signe S.A.S. enviando un correo electrónico a la dirección pqrsa@thsigne.com en el que se detalla la situación por la que se presenta.

Los PQRS serán gestionados por el Responsable de PQRS de Thomas Signe S.A.S., quien se encargará de derivar la incidencia al Departamento o rol respectivo. Dicha gestión se llevará a cabo, dando lugar a una solución en un lapso no mayor a quince (15) días. El usuario recibirá un mensaje de correo electrónico confirmando la recepción de la PQRS y cuando ésta sea resuelta. Thomas Signe S.A.S. cuenta con el procedimiento de THS-CO-AC-PR-02 Procedimiento de PQRS para el tratamiento de PQRS que detalla cada uno de los procesos y se encuentra publicado en la página web de Thomas Signe S.A.S.

9.12 CAMBIOS EN DPC

El contenido de esta DPC puede ser cambiado unilateralmente por Thomas Signe S.A.S. sin preaviso, excepto cuando los cambios pudiesen afectar a la aceptación del servicio por los Suscriptores y/o los Terceros que confían, en cuyo caso serán notificados con antelación a los interesados (por ejemplo, mediante la publicación de la notificación en la página web de Thomas Signe S.A.S.), sin necesidad de incluir los detalles de los cambios en la notificación. Los cambios pueden tener como causa justificativa motivos legales, técnicos o comerciales.

Todos los cambios en esta DPC requerirán nuevas versiones de los documentos. Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

Las nuevas versiones aprobadas de esta DPC serán enviadas a ONAC y publicadas en la página web de Thomas Signe S.A.S.

Aquellos cambios que puedan afectar sustancialmente a los Suscriptores serán notificados a los interesados.

9.13 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Tribunales colombianos, con independencia del lugar dónde se hubieran utilizado los sellos de tiempo emitidos.

9.14 LEY APLICABLE

La legislación aplicable al presente documento, así como a las operaciones que derivan de ellas se registra en el documento de carácter interno GSIGNE-GRAL-PR-01-F05 Listado de Documentos Externos, entre ella se encuenta la siguiente, así como los reglamentos que la modifiquen o complementen:

a) Ley 527 de 1999
b) Ley Estatuaria 1581 de 2012
c) Decreto Ley 0019 de 2012
d) Decreto 1074 de 2015
e) Decreto 333 de 2014
f) Decreto 1471 de 2014

9.15 CONFORMIDAD CON LA LEY APLICABLE

Es responsabilidad de Thomas Signe S.A.S. velar por el cumplimiento de la legislación aplicable recogida en la sección anterior.

9.16 ESTIPULACIONES DIVERSAS

9.16.1 CONTRATO DE SUSCRIPCIÓN

El modelo del Contrato de Suscripción para el servicio de estampado cronológico vigente se encuentra publicado en la siguiente página web:

https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/

En cada contrato se deberán rellenar los datos de identificación del Suscriptor y la fecha de la firma del contrato por el Suscriptor.

Puesto que cada contrato se rellena con los datos de identificación del Suscriptor, el documento está catalogado con nivel CONFIDENCIAL, a pesar de que el modelo del contrato está publicado en la página web indicada.

Será responsabilidad del Suscriptor difundir, conforme corresponda en términos de confidencialidad, las condiciones establecidas en el contrato, a toda la comunidad de usuarios que defina para el uso del servicio contratado.

9.16.2 CLÁUSULA DE ACEPTACIÓN COMPLETA

Todos los Solicitantes, Suscriptores, Terceros que confían y cualquier otra parte interesada asumen en su totalidad el contenido de la última versión de esta DPC.

9.16.3 INDEPENDENCIA

En el caso de que cualquiera de los apartados recogidos en la presente DPC sea declarado, parcial o totalmente, nulo o ilegal no afectará tal circunstancia al resto del documento.

9.17 OTRAS ESTIPULACIONES

No se contemplan.

10 FORMATOS

THS-CO-AC-DPC-02-F01 Formulario de Solicitud de Estampado Cronológico

THS-CO-AC-DPC-02-F02 Propuesta Comercial de Estampado Cronológico

THS-CO-AC-DPC-02-F03 Contrato de Suscripción para Estampado Cronológico

THS-CO-AC-DPC-F16 Tabla de Retención Documental

11 REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
Formularios completos de Solicitud de Estampado Cronológico	Informático	Gerente Comercial	ERP	7 años o de acuerdo a normativa aplicable
Propuestas Comerciales firmadas de Estampado Cronológico	Informático	Gerente Comercial	ERP	7 años o de acuerdo a normativa aplicable
Contratos firmados de Suscripción para Estampado Cronológico	Informático	Gerente Comercial	ERP	7 años o de acuerdo a normativa aplicable
Tabla de Retención Documental Completada	Informático	Gerente de Sistemas de Información	Sistema de archivos	7 años o de acuerdo a normativa aplicable