Entidad de Certificación Digital

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

Declaración de Prácticas de Certificación para Emisión de Certificados

Información del documento

Nombre	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA EMISIÓN DE CERTIFICADOS
Realizado por	THOMAS SIGNE S.A.S.
País	COLOMBIA
Versión	2.1
Fecha	JUNIO DEL 2020
Tipo de Documento	PÚBLICO
Código	**THS-CO-AC-DPC-01**

Historial de versiones

Versión	Fecha	Descripción
1.0	28/06/2017	Elaboración de documento inicial.
1.1	03/01/2018	Inclusión y adecuación de nuevas estructuras y procedimientos.
1.2	08/05/2018	Correcciones y precisiones en secciones del documento.
1.3	20/05/2018	Se especifican los estándares técnicos aplicables. Se agregan los usos de la clave privada de la CA Raíz. Se detalla el proceso del ciclo de vida de los certificados.
1.4	22/05/2018	Modificación menor en el apartado de Identificación de la ECD y de Obligaciones de Proveedores. Se agregan usos permitidos del certificado digital. Especificaciones en el apartado de Controles de seguridad.
1.5	08/06/2018	Se agregan apartados para formatos y registros aplicables.
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	22/01/2019	Se añade la posibilidad de que, opcionalmente, el OR realice la verificación de la identidad del Solicitante de forma presencial, en vez de por videoconferencia. Correcciones menores.

1.8	09/05/2019	Integración con el sistema de gestión del Grupo Cambio de nombre del documento de THS-DP-CER-01 a THS-CO-DPC-AC-01. Se añade Thomas Signe Root como participante PKI de Thomas Signe S.A.S. (ver sección 3.2.1). Se eliminan las secciones de formatos y registros aplicables. Correcciones menores.
1.9	18/09/2019	Ajuste de la codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.1. En los Certificados Corporativos de Componente, se añaden las posibilidades de que el Suscriptor pueda ser una Persona Natural y de que el Solicitante pueda ser una Persona Jurídica distinta al Suscriptor. En la solicitud del certificado, dependiendo del tipo de certificado, se añade como documento requerido, la Cédula de ciudadanía o la Cédula de extranjería del Representante Legal, además de la autorización firmada por éste con con los datos de la Persona Natural o de la Persona Jurídica autorizada a solicitar un certificado digital. En la revisión de la solicititud del certificado, en la validación del documento de identidad del Solicitante (Persona Natural), se elimina la consulta ante una Base de datos para Personas Naturales. Se añaden las secciones de Formatos y Registros. Correcciones menores.
1.10	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. Añadidos un formato y un registro para las videconferencias de verificación de identidad. 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 seguir recomendaciones del estándar RFC 3647.

		En los Certificados Corporativos de Componente, se añaden las posibilidades de que el Suscriptor pueda ser una Persona Natural que desempeñe una actividad económica del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario y de que el Solicitante pueda ser una Persona Natural distinta al Suscriptor. En los Certificados Corporativos de Pertenencia a Empresa, se añade la posibilidad de que la Corporación o Entidad a la que está vinculada el Suscriptor (Persona Natural) pueda ser una Persona Natural (ya sea ésta una empresa o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario). 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 obligaciones de la Entidad a la cual se encuentra vinculado el Suscriptor. Correcciones menores.

ÍNDICE

1 INTRODUCCIÓN

1.1 PRESENTACIÓN DEL DOCUMENTO

Este documento constituye la Declaración de Prácticas de Certificación (DPC) para la emisión de certificados de Thomas Signe S.A.S., en el marco del cumplimiento de los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-4.1-10 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, gestionar, revocar y renovar certificados digitales, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", y conforme a los siguientes estándares:

- 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.

- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates. Actualizado por ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

Adicionalmente a la prácticas establecidas en esta DPC, cada tipo de certificado emitido por Thomas Signe S.A.S. se rige por los requisitos particulares establecidos en la correspondiente Política de Certificados (PC). Estas PC se encuentran publicadas en la misma página web de Thomas Signe S.A.S. que el presente documento (ver sección 1.2).

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 el siguiente OID.

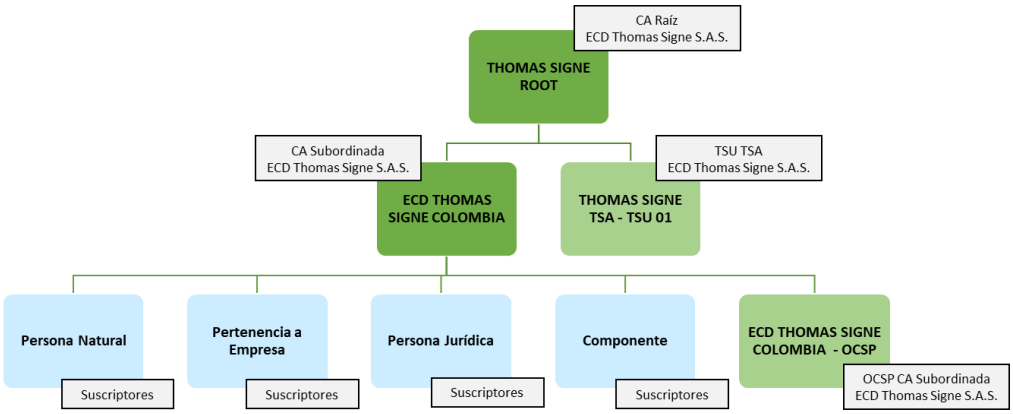
OID DE LA DPC PARA LA EMISIÓN DE CERTIFICADOS DE THOMAS SIGNE S.A.S.	
1.3.6.1.4.1.51362.0.0.1	DPC

Este documento se encuentra publicado en la siguiente página web:

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

1.3 PARTICIPANTES DE LA PKI DE THOMAS SIGNE S.A.S

1.3.1 JERARQUÍA DE CERTIFICADOS DE LA PKI DE THOMAS SIGNE S.A.S.



1.3.2 THOMAS SIGNE ROOT

Thomas Signe Root es la Autoridad de Certificación Raíz (CA Raíz) de Thomas Signe S.A.S. que emite el certificado de la Autoridad de Certificación Subordinada (CA Subordinada) de la ECD Thomas Signe S.A.S. (ECD Thomas Signe Colombia). Por tanto, Thomas Signe Root es la CA Raíz de la jerarquía de certificados de la PKI de Thomas Signe S.A.S.

La CA Raíz de Thomas Signe S.A.S. también emite el certificado de la Unidad de Sellado de Tiempo (TSU) de la Autoridad de Sellado de Tiempo (TSA) de la ECD Thomas Signe S.A.S. (Thomas Signe TSA – TSU 01).

Asimismo, la CA Raíz de Thomas Signe S.A.S podrá emitir certificados de otras CA Subordinadas del grupo Thomas Signe, lo cual deberá quedar reflejado en las correspondientes DPC de estas CA Subordinadas. Por tanto, Thomas Signe Root también podrá ser la CA Raíz de otras PKI del grupo Thomas Signe.

1.3.3 ECD THOMAS SIGNE S.A.S. (ECD THOMAS SIGNE COLOMBIA)

Thomas Signe S.A.S., 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 S.A.S., 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 S.A.S., 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 S.A.S. 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 de la ECD Thomas Signe S.A.S. y de sus proveedores:

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 NIT *900962071*

Domicilio social y de correspondencia - comercial: Avenida 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: +57 (1) 3810240

Fax: +57 (1) 3407434

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

Oficina para PQRSA: PQRSA - pqrsa@thsigne.com

Página Web: www.thomas-signe.co

Proveedor de 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://www.registradores.org/registroonline solicitar una certificación mercantil, buscando la sociedad por el NIF *A11029279*, como usuario abonado o como usuario no abonado que dispone de tarjeta o PayPal (para realizar la búsqueda, no se sumistrará ningún dato de tarjeta o Paypal ni se realizará ningún cargo al usuario)

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

Teléfono: +34 91 806 00 99

Fax: +34 918 06 01 02

Dirección de correo electrónico: comercial@signe.es

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

Página Web: www.signe.es

Proveedor de 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 NIT *830012157*

Domicilio social y de correspondencia - comercial: Avenida 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: +57 (1) 3810240

Fax: +57 (1) 3407434

Dirección de correo electrónico: servicioalclientetgsc@thomasgreg.com

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

Página Web: www.tgscolombia.com

1.3.4 SOLICITANTE

Solicitante es la persona natural o jurídica que solicita a la ECD Thomas Signe S.A.S. la emisión de un certificado.

1.3.5 SUSCRIPTOR

Suscriptor es la persona natural o jurídica a cuyo nombre la ECD Thomas Signe S.A.S. expide un certificado digital y, por tanto, actúa como responsable del mismo, y que, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y en la PC correspondiente y habiendo firmado el respectivo Contrato de Suscripción con Thomas Signe S.A.S., acepta las condiciones del servicio de emisión de certificados prestado por éste.

El Suscriptor es el responsable del uso de la clave privada asociada al certificado expedido a su nombre por la ECD Thomas Signe S.A.S., a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando dicha clave privada.

1.3.6 TERCERO QUE CONFÍA

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

1.3.7 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR

Entidad a la cual se encuentra vinculado el Suscriptor es, en su caso, la persona jurídica o persona natural (ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario) a la que el Suscriptor se encuentra relacionado mediante la vinculación acreditada en el certificado.

1.4 TIPOS Y USOS DE CERTIFICADOS

1.4.1 CERTIFICADOS PERSONALES

Certificado de Persona Natural: son certificados que permiten identificar y firmar al Suscriptor como una Persona Natural sin vinculación a ninguna corporación o entidad.

OID DE POLÍTICAS DE CERTIFICADOS PERSONALES	
1.3.6.1.4.1.51362.0.2.1.1.D	PC de Persona Natural de Thomas Signe S.A.S.

D = Dispositivo (consultar los tipos de soporte admitidos en la PC correspondiente):

1 = Tarjeta/Token, 2 = Otros Dispositivos, 3 = HSM Centralizado

1.4.2 CERTIFICADOS CORPORATIVOS

Los Certificados Corporativos son certificados de firma digital cuyo Suscriptor es una Persona Natural vinculada a una Corporación o Entidad (ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario) o la propia Corporación o Entidad:

Certificado de Pertenencia a Empresa: Son certificados que permiten identificar y firmar al Suscriptor como Persona Natural vinculada a una Corporación o Entidad (Persona Jurídica o Persona Natural), ya sea como empleado, asociado, colaborador, cliente o proveedor.

Certificados de Persona Jurídica: Son certificados que permiten identificar y firmar al Suscriptor como Persona Natural vinculada a una Corporación o Entidad (Persona Jurídica), como su representante legal.

Certificado de Componente: Son certificados que permiten identificar y firmar al Suscriptor como Corporación o Entidad (Persona Jurídica o Persona Natural) que se emiten para dispositivos informáticos, programas o aplicaciones dedicados a firmar en nombre de la Corporación o Entidad en sistemas de firma digital para la actuación administrativa automatizada.

OID DE POLÍTICAS DE CERTIFICADOS CORPORATIVOS	
1.3.6.1.4.1.51362.0.2.1.2.D	PC de Pertenencia a Empresa de Thomas Signe S.A.S.
1.3.6.1.4.1.51362.0.2.1.3.D	PC de Persona Jurídica de Thomas Signe S.A.S.
1.3.6.1.4.1.51362.0.2.1.4.D	PC de Componente de Thomas Signe S.A.S.

D = Dispositivo (consultar los tipos de soporte admitidos en la PC correspondiente):

1 = Tarjeta/Token, 2 = Otros Dispositivos, 3 = HSM Centralizado

1.4.3 USOS APROPIADOS DE LOS CERTIFICADOS

En la descripción de cada tipo de certificado en la presente DPC y en la PC correspondiente se indican los respectivos usos apropiados de los certificados.

En el caso del uso de los certificados para la firma centralizada, los formatos de firmas digitales construidos por servicios ofrecidos por Thomas Signe S.A.S. siguen los siguientes estándares técnicos:

- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES). Actualizado por ETSI EN 319 132 XAdES digital signatures.

- ETSI TS 102 778 PDF Advanced Electronic Signature Profiles (PAdES). Actualizado por ETSI EN 319 142 PAdES digital signatures.

1.4.4 USOS NO AUTORIZADOS DE LOS CERTIFICADOS

No se permite el uso que sea contrario a la normativa colombiana, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta DPC y en la PC correspondiente.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar a la muerte, lesiones personales o daños medioambientales severos.

Los certificados emitidos a los Suscriptores no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

La ECD Thomas Signe S.A.S. no ofrece el servicio de recuperación de la clave privada, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor. El Suscriptor que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, Thomas Signe S.A.S. tenga responsabilidad alguna por pérdida de información derivada de la pérdida de las claves de cifrado. Por ello, Thomas Signe S.A.S. no recomienda el uso de los certificados digitales para el cifrado de la información.

1.5 ADMINISTRACIÓN DE LA DPC Y LAS PC

1.5.1 ORGANIZACIÓN RESPONSABLE

Thomas Signe S.A.S. administra esta DPC y las PC asociadas.

1.5.2 DATOS DE CONTACTO

Para consultas o comentarios relacionados con la presente DPC o las PC asociadas, 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, fax, direcciones de correo electrónico comercial o PQRSA de la Entidad de Certificación Digital indicados en la sección 1.3.3.

1.5.3 PROCEDIMIENTO DE APROBACIÓN

Esta DPC y las PC asociadas son aprobadas por el Comité de Sistemas de Gestión de Thomas Signe S.A.S. antes de ser publicadas, controlando las versiones de las mismas, a fin de evitar modificaciones y suplantaciones no autorizadas y el uso de documentación obsoleta.

Las nuevas versiones aprobadas de esta DPC y de las PC asociadas 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 ABREVIACIONES

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.

Apelación (PQRSA): solicitud presentada por un cliente para reconsiderar cualquier decisión adversa tomada por la ECD con relación a los servicios prestados.

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 Registro: persona jurídica, con excepción de los notarios públicos, o parte interna de las ECD necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para:

- Registrar las peticiones que hagan los solicitantes para obtener un certificado.

- Comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones.
- Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

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.

CA Subordinada: Autoridad de Certificación de segundo nivel o más niveles.

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

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

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.

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.

Corporación (Entidad): persona jurídica o persona natural, ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario.

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, gestionar, revocar y renovar certificados sin y con cambio de claves.

Entidad: ver **Corporación.**

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 emisión de certificados, incluyendo otras gestiones propias de certificados digitales, 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 Centralizada: se llama "firma centralizada" a la gestión centralizada de los certificados digitales, de manera que estos certificados operen desde un repositorio único, controlado y seguro. De manera práctica esto implica que los certificados digitales son generados y almacenados en el servidor, lo que permite que puedan ser usados desde cualquier ordenador o dispositivo móvil.

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.

HSM Centralizado: dispositivo criptográfico en el cual se genera, almacenan y protegen las claves criptográficas de los suscriptores de una forma segura, permitiendo la firma centralizada o firma en la nube.

Lista de Certificados Digitales Revocados (CRL): aquella relación que debe incluir todos los certificados revocados por la ECD.

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.

Persona natural individual: persona natural que no sea una Corporación o Entidad.

Petición (PQRSA): 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.

Política de Certificados (PC): conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

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 (PQRSA): 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 (PQRSA): 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.

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.**

Servicio del estado del certificado en línea OCSP: actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.

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 y la PC correspondiente para acceder al servicio de certificación digital. Persona natural o jurídica que solicita a la ECD la emisión de un certificado.

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

Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital. Persona natural o jurídica que, habiendo firmado el respectivo Contrato de Suscripción, acepta las condiciones del servicio de emisión de certificados 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, y que confía en la validez del correspondiente certificado digital emitido por la ECD.

Token: dispositivo hardware criptográfico suministrado por una ECD, el cual contiene el certificado digital y la llave privada del suscriptor.

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)

DN Distinguished Name (Nombre distinguido)

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.

ETSI European Telecommunications Standards Institute

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

OR Operador de Registro

PC Política de Certificados

PKCS Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA.

PKI Public Key Infrastructure (Infraestructura de clave pública)

PQRSA Peticiones, Quejas, Reclamos, Sugerencias y Apelaciones

RA Registration Authority (Autoridad de Registro)

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.

RSA Rivset, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

RUES Registro Único Empresarial y Social

SAR Signe Autoridad de Registro

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

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

Certificado CA Raíz de Thomas Signe S.A.S.

http://thsigne.com/certs/thomas_signe_root.crt

Certificado CA Subordinada de Thomas Signe S.A.S.

http://thsigne.com/certs/ecd_thomas_signe_colombia.crt

Lista de Certificados Revocados (CRL) CA Raíz de Thomas Signe S.A.S.

http://crl.thsigne.com/thomas_signe_root.crl

Lista de Certificados Revocados (CRL) CA Subordinada de Thomas Signe S.A.S.

http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl

Servicio OCSP

http://ocsp-co.thsigne.com

Declaración de Prácticas de Certificación (DPC), Políticas de Certificados (PC) 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, las PC 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

Certificados de CA Raíz y CA Subordinada

Los certificados de la CA Raíz y la CA Subordinada se publicarán y permanecerán en la página web de Thomas Signe S.A.S. durante todo el tiempo en que la ECD esté prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

Thomas Signe S.A.S. publicará en su página web las CRL de la CA Raíz y la CA Subordinada en los eventos y con la periodicidad definidas en la sección 4.9.6.

Declaración de Prácticas de Certificación (DPC), Políticas de Certificados (PC) y Contrato de Suscripción

Thomas Signe S.A.S publicará en su página web cada nueva versión aprobada de la DPC, las PC 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 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

Todos los certificados requieren un nombre distinguido (DN o distinguished name) del titular conforme al estándar X.500.

Adicionalmente, los DN de los titulares de los certificados son coherentes con lo dispuesto en los siguientes estándares:

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

- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

3.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los campos del DN del titular del certificado referentes a Nombres y apellidos y/o a Nombre o Razón social se corresponderán con los datos registrados legalmente del Suscriptor, expresados exactamente en el

formato que consten en la Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte y/o en el Certificado de Cámara de Comercio y/o Registro Único Tributario (o documentos equivalentes).

En el caso de que los datos consignados en el DN del titular del certificado fueran ficticios o se indique expresamente su invalidez en dicho DN (ej. mediante la palabra "PRUEBA" o "INVALIDO"), se considerará al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

3.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS SUSCRIPTORES

No se admiten anónimos ni seudónimos para identificar a los suscriptores.

3.1.4 UNICIDAD DE LOS NOMBRES

El nombre distinguido (DN) de los titulares de los certificados emitidos será único para cada Suscriptor.

Los atributos del DN del titular del certificado que contienen el tipo y el número del documento de identidad y/o el número de identificación fiscal se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

3.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

La ECD no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial.

Thomas Signe S.A.S. no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Suscriptor. Sin embargo la ECD no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1 MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

En la PC de cada tipo de certificado se especifica el método de prueba de posesión de la clave privada para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA CORPORACIÓN O ENTIDAD

La RA verificará los siguientes datos para poder autenticar la identidad de la Corporación o Entidad (Persona Jurídica o Persona Natural) identificada en el certificado:

- Los datos relativos al nombre o razón social de la Entidad (Persona Jurídica o Persona Natural).

- Los datos relativos a la constitución y personalidad jurídica de la Entidad (Persona Jurídica).

- Los datos relativos a la extensión y vigencia de las facultades de representación del representante legal de la Entidad (Persona Jurídica).

- Los datos relativos al número de identificación tributaria de la Corporación o Entidad (Persona Jurídica o Persona Natural).

- Los datos relativos a la dirección completa de la Entidad (Persona Jurídica o Persona Natural).

La RA verificará los datos anteriores mediante los siguientes procedimientos:

- Solicitud de Certificado de la Cámara del 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.

- Solicitud de Registro Único Tributario o documento equivalente, en todos los casos; expedido en Colombia (por defecto) o en otro país.

- Solicitud de un documento oficial adicional en el que conste una dirección completa actual de la Entidad (por ejemplo, un Certificado de Residencia para Personas Naturales), en el caso de que el Solicitante desee que figure en el certificado una dirección distinta a las incluidas en el Certificado de la Cámara del Comercio y/o en el Registro Único Tributario o documentos equivalentes; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.

- Para aquellos casos en los que sea posible, consulta del número de identificación tributaria de la Entidad en una Base de datos online (en Colombia, para las empresas del tipo Persona Jurídica o Persona Natural, Base de datos RUES), para verificar la existencia de la Entidad y que se encuentra activa.

La ECD se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

La RA guardará la documentación relativa al sustento de la validación de la identidad de la Corporación o Entidad identificada en el certificado.

Adicionalmente, si el tipo de certificado admite la posibilidad de que el Solicitante sea una Corporación o Entidad distinta al Suscriptor, la RA verificará la identidad de esta Entidad según lo especificado en la correspondiente PC.

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL INDIVIDUAL

La RA verificará de forma fehaciente la identidad de la Persona Natural individual identificada en el certificado (Suscriptor) o de la Persona Natural individual Solicitante del certificado, por videoconferencia o de forma presencial. Para ello, en el caso de verificación por videoconferencia, la Persona Natural individual deberá escanear y enviar un documento reconocido en derecho que le identifique y mostrar el documento original durante la videoconferencia, y, en el caso de verificación de forma presencial, deberá entregar personalmente a un OR una fotocopia de dicho documento.

La RA validará que el documento de identidad presentado sea aparentemente legítimo y que los datos contenidos en el mismo (país de expedición, tipo y número del documento de identidad, nombres y apellidos) son conformes a los correspondientes datos ingresados en el formulario de solicitud del certificado y a los documentos adjuntados en la plataforma SAR . Asimismo, en los casos que sea aplicable, la RA verificará que el documento estaba vigente cuando se presentó.

La RA guardará la documentación relativa al sustento de la validación de la identidad de la persona natural individual Suscriptor y/o Solicitante del certificado.

3.2.4 INFORMACIÓN DE SUSCRIPTOR Y SOLICITANTE NO VERIFICADA

Bajo ninguna circunstancia la RA omitirá las labores de verificación de información que conduzcan a la identificación del Suscriptor y del Solicitante según lo especificado en las secciones 3.2.2 y 3.2.3.

En la PC de cada tipo de certificado se especifica la información del Suscriptor y del Solicitante no verificada para los correspondientes certificados.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN CON CAMBIO DE CLAVES

La ECD Thomas Signe S.A.S. no atiende requerimientos de renovación de certificados digitales con cambio de claves.

Los casos en los que se requiera un nuevo certificado digital con cambio de claves, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado,

realizándose la misma validación de identidad que se hizo inicialmente para el primer certificado digital, según lo especificado en la sección 3.2.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La identificación y autenticación del Suscriptor o Solicitante para una petición de revocación de un certificado podrá ser realizada por:

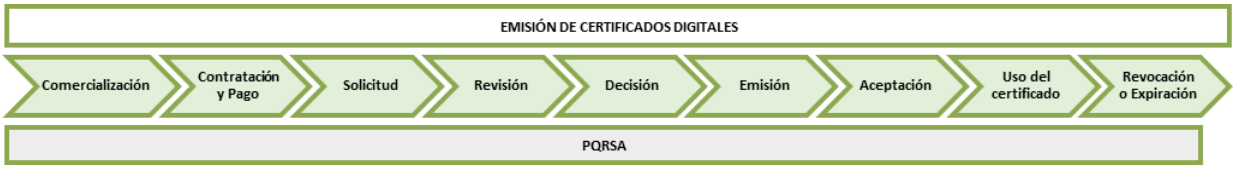
- El propio Suscriptor o Solicitante, en el caso de que éste utilice el procedimiento de revocación online. En la PC de cada tipo de certificado se especifica el método por el que se identifica y autentica al Suscriptor o Solicitante para una petición de revocación online, dependiendo del tipo de soporte en el que haya sido emitido el certificado.

- Un Operador de Registro (OR), en el caso de que el Suscriptor o Solicitante utilice el procedimiento de revocación mediante Operador de Registro, consistente en una comunicación enviada por correo electrónico. El OR identificará y autenticará al Suscriptor o Solicitante ante una petición de revocación recibida por correo electrónico, comprobando que ésta se ha enviado desde la respectiva dirección de correo electrónico declarada en el formulario de solicitud para la emisión del certificado.

La identificación y autenticación de cualquier persona autorizada distinta al Suscriptor y al Solicitante para una petición de revocación recibida será realizada por un OR, según los medios que considere necesarios.

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

El ciclo de vida de los certificados digitales emitidos por la ECD Thomas Signe S.A.S. se extiende desde la comercialización inicial hasta la revocación o expiración del certificado.



4.1 SOLICITUD DE CERTIFICADOS

4.1.1 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Están autorizados para solicitar la emisión de un certificado:

1) El futuro Suscriptor que sea Persona Natural y que sustente correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.

2) Una Persona Natural individual (no Corporación o Entidad) vinculada a la Corporación o Entidad futuro Suscriptor (Persona Jurídica o persona Natural), incluyendo un representante legal, apoderado, empleado o persona autorizada por un representante legal de la Persona Jurídica Suscriptor o por la propia Persona Natural Suscriptor a solicitar y obtener un certificado para sistemas de firma digital para la actuación administrativa automatizada, que pueda sustentar correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.

3) Una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta a la Corporación o Entidad futuro Suscriptor, que haya sido autorizada por el representante legal de la Persona Jurídica Suscriptor o por la propia Persona Natural Suscriptor a solicitar y obtener un certificado para sistemas de firma digital para la actuación administrativa automatizada, que pueda sustentar correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.

4.1.2 COMERCIALIZACIÓN

El Solicitante y/o, en los casos que sea aplicable, el Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor podrán recibir información acerca del proceso de certificación digital de las siguientes maneras:

- Consultando la página web www.thomas-signe.co

- Mediante correo electrónico informativo desde la dirección comercial@thomas-signe.co

- El trato directo con Agentes comerciales.

Por cualquiera de estos medios, se les brindará información acerca de dicho proceso, requisitos necesarios, tarifas u otros relativos.

Luego de ser informado, si el Solicitante es una Persona Natural individual, el Solicitante y/o, en los casos que sea aplicable, el Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor indicarán al Área Comercial y/o a un OR:

1) El tipo de certificado requerido y, si éste admite varios tipos de soporte, el tipo de soporte requerido.

2) La vigencia del certificado requerida.

3) El nombre completo del Solicitante.

4) El tipo y el número del su documento de identidad del Solicitante.

5) La cuenta de correo electrónico del Solicitante que estará asociada al certificado digital y por medio de la cual la ECD le realizará notificaciones y comunicaciones oficiales. Cabe destacar que para los certificados personales, se debe indicar la cuenta de correo electrónico personal y para los certificados corporativos, la cuenta de correo electrónico corporativa.

En los casos que sea aplicable:

6) El nombre o la razón social del Suscriptor o de la Entidad a la cual se encuentra vinculado el Suscriptor.

7) El NIT del Suscriptor o de la Entidad a la cual se encuentra vinculado el Suscriptor.

Si el Solicitante es una Persona Natural individual, el Área Comercial y/o un OR enviarán por correo electrónico al Solicitante y/o, en los casos que sea aplicable, al Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor: la Propuesta Comercial, en los casos que sea aplicable; el Contrato de Suscripción; en los tipos de certificado que lo permiten, un modelo de autorización para la solicitud y obtención del certificado en el caso de que se requiera; opcionalmente, un enlace a la plataforma SAR; y las indicaciones respectivas.

4.1.3 CONTRATACIÓN Y PAGO

Para proceder con la contratación y el pago, el Solicitante y/o, en los casos que sea aplicable, el Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor deberán:

- 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 entre Thomas Signe S.A.S. y el Suscriptor, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Suscripción firmado.

- Si el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, aprobar todos los términos y condiciones dispuestos en un Contrato de Prestación de Servicios entre Thomas Signe S.A.S. y el Solicitante, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Prestación de Servicios firmado.

Cabe resaltar que, además del Contrato de Suscripción con cada Suscriptor de un certificado digital, dependiendo del tipo de contratación, se podría necesitar un Contrato de Prestación de Servicios entre

Thomas Signe S.A.S. y, para los certificados personales, el Suscriptor del certificado digital, o, para los certificados corporativos, la Corporación o Entidad que consta en el certificado digital.

4.1.4 SOLICITUD

El proceso de solicitud de emisión dependerá del tipo de certificado requerido. En la PC de cada tipo de certificado se especifica el proceso particular de solicitud de emisión para los correspondientes certificados. A continuación, se describe el proceso general de solicitud de emisión.

Para solicitar la emisión de un certificado digital, el Solicitante y/o, en los casos que sea aplicable, al Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor deberán ingresar a la plataforma SAR. Dentro de la plataforma, procederán a ingresar los datos requeridos y adjuntar los documentos solicitados, para finalmente guardar su solicitud. Alternativamente, el Solicitante y/o, en los casos que sea aplicable, al Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor podrán entregar personalmente o enviar los datos y los documentos requeridos al Área Comercial y/o a un OR, y éstos ingresarán en la plataforma SAR los datos y adjuntarán los documentos solicitados.

La RA de la ECD Thomas Signe S.A.S. solicita toda la información necesaria para la verificación de identidad del Solicitante y/o del Suscriptor. Los documentos requeridos dependerán del tipo de certificado (especificado en la PC respectiva), los cuales pueden ser y no se limitan a los siguientes:

- Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte del Solicitante (Persona Natural individual); expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Certificado de Cámara del Comercio o documento equivalente del Suscriptor o de la Entidad a la que se encuentra viculado el Suscriptor; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Registro Único Tributario o documento equivalente del Suscriptor o de la Entidad a la que se encuentra viculado el Suscriptor; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Autorización firmada por el Representante Legal de la Persona Jurídica, o por la propia Persona Natural, del Suscriptor o de la Entidad a la que se encuentra viculado el Suscriptor, con los datos de la Persona Natural o de la Persona Jurídica autorizada a solicitar y obtener un certificado digital; expedida un máximo de 30 días antes.
- Cédula de Ciudadanía o Cédula de Extranjería del Representante Legal de la Persona Jurídica, o por la propia Persona Natural, que firma la autorización; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Documento adicional oficial en el que conste una dirección completa actual del Suscriptor, por ejemplo, un Certificado de Residencia para Personas Naturales, expedido un máximo de 30 días antes.

Asimimismo, la RA de la ECD Thomas Signe S.A.S. solicita los siguientes documentos adicionales para la emisión de un certificado:

- Constancia del pago de la tarifa del certificado indicada en la Propuesta Comercial, en los casos que sea aplicable.
- Contrato de Suscripción firmado.

Thomas Signe S.A.S. cuenta con el derecho de solicitar documentos adicionales para garantizar la correcta autenticación del Solicitante y/o del Suscriptor y llevar a cabo un adecuado servicio de certificación digital.

4.2 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

4.2.1 REVISIÓN

Es responsabilidad de la RA realizar de forma fehaciente la identificación y autenticación del Solicitante y/o Suscriptor de acuerdo al tipo de certificado solicitado. Para lo cual, la RA verificará la validez de la documentación presentada y, en los casos que sea posible, consultará una Base de datos online para

verificar la Corporación o Entidad Suscriptor o a la que el Suscriptor se encuentra vinculado, según lo especificado en las secciones 3.2.2 y 3.2.3 y en la PC correspondiente.

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

Una vez recolectada y revisada satisfactoriamente toda la documentación y evidencias requeridas, si el Solicitante es una Persona Natural individual, el OR coordinará con él una cita para realizar una videoconferencia. En dicha sesión, el OR hará una serie de preguntas para verificar la identidad del Solicitante y le solicitará que le muestre el documento de identidad original que ha enviado escaneado, para comprobar que coincide con el documento recibido. A fin de evidenciar dicha videoconferencia, la plataforma de la RA grabará toda la sesión y se guardará la grabación junto a la información recabada del Solicitante. Este proceso será realizado previamente a la emisión del certificado.

Alternativamente a la videoconferencia, el OR podrá haber verificado la identidad del Solicitante, si éste es una Persona Natural individual, de forma presencial, en cuyo caso deberá haber recibido del Solicitante los documentos requeridos, que deberá haber ingresado en la plataforma SAR en formato digital y, además, deberá archivar y conservar en formato papel los documentos originales recibidos en dicho formato (no escaneados), entre los cuales se incluirán obligatoriamente el Contrato de Suscripción firmado por el Suscriptor y, en los casos que sea aplicable, la autorización firmada por el Representante Legal con los datos de la Persona Natural autorizada a solicitar un certificado digital.

Una vez que el OR ha validado los documentos presentados y los datos ingresados en el formulario de solicitud de certificado y que, en el caso de que el Solicitante sea una Persona Natural individual, ha verificado su identidad, el OR aprobará la solicitud de emisión en la plataforma de la RA.

Si la información o verificación de identidad no fuese correcta, la RA deberá denegar la petición, contactando al Solicitante para comunicarle el motivo.

Asimismo, si el servicio solicitado no corresponde con los servicios de Thomas Signe S.A.S acreditados por ONAC, se rechazará la petición, comunicando al Solicitante el motivo del mismo.

4.2.2 DECISIÓN

La ECD Thomas Signe S.A.S. es responsable de la decisión tomada con respecto a la certificación digital. Es decir, la ECD es responsable de aprobar o denegar la certificación digital. En el caso de denegación, la ECD se encarga de comunicar el motivo del rechazo al Solicitante.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA ECD DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud, se procederá a la emisión del certificado, que deberá ser emitido de forma segura al Suscriptor. En la emisión del certificado digital, la ECD Thomas Signe S.A.S.:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

- Protege la confidencialidad e integridad de los datos de registro.

- Todos los certificados iniciarán su vigencia en el momento que se indica en el propio certificado.

En la PC de cada tipo de certificado se especifican las acciones particulares de la ECD durante la emisión del certificado para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

4.3.2 NOTIFICACIÓN AL SOLICITANTE POR LA ECD DE LA EMISIÓN DEL CERTIFICADO

La ECD Thomas Signe S.A.S. notificará al Solicitante la emisión del certificado y le enviará por correo electrónico la documentación de la certificación digital.

En la PC de cada tipo de certificado se especifica cómo notifica la ECD al Solicitante la emisión del certificado y qué documentación de la certificación digital le envía, para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

El certificado se considerará aceptado por el Suscriptor y por el Solicitante, una vez que la RA ha realizado su entrega y la ECD ha notificado la misma al Solicitante, según lo especificado en la PC respectiva.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA ECD

La ECD Thomas Signe S.A.S.no publica los certificados emitidos en ningún repositorio.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA ECD A OTRAS ENTIDADES

La ECD Thomas Signe S.A.S. no notifica la emisión de certificados a terceros.

4.5 USOS DE LAS CLAVES Y EL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

Los certificados podrán ser utilizados según lo estipulado en esta DPC y la PC respectiva.

Las extensiónes Key Usage y Extended Key Usage podrán ser utilizadas para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas de terceros, quedando su regulación fuera del alcance de este documento.

4.5.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

Los Terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la PC respectiva.

Es responsabilidad de los Terceros que confían verificar el estado del certificado mediante los servicios ofrecidos por Thomas Signe S.A.S., concretamente para ello y especificados en el presente documento.

4.6 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

La ECD Thomas Signe S.A.S. no atiende requerimientos de renovación de certificados digitales sin cambio de claves.

Los casos en los que se requiera un nuevo certificado digital, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado, con cambio de claves.

4.7 RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

La ECD Thomas Signe S.A.S. no atiende requerimientos de renovación de certificados digitales con cambio de claves.

Los casos en los que se requiera un nuevo certificado digital, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado, con cambio de claves.

4.8 MODIFICACIÓN DE CERTIFICADOS

La ECD Thomas Signe S.A.S. no atiende requerimientos de modificación de certificados digitales.

Los casos en los que se requiera modificar algún dato en un certificado digital (actualización de la información contenida en un certificado) se tratan como una revocación de certificado y una nueva emisión de certificado, con cambio de claves.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación de un certificado supone la pérdida de validez del mismo y es irreversible. Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL.

Asimismo, no se permite la suspensión de certificados que no conduzca a un estado de revocación inmediato. La ED Thomas Signe S.A.S. no realiza suspensiones de certificados.

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Un certificado podrá ser revocado debido a las siguientes causas:

a) Circunstancias que afectan a la información contenida en el certificado:

- Modificación de alguno de los datos contenidos en el certificado.

- Confirmación de que alguna información o hecho contenido en el certificado es falso.

- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

- Pérdida o cambio de la vinculación del Suscriptor con la Corporación o Entidad que consta en el certificado.

- Liquidación de la persona jurídica que consta en el certificado.

- Pérdida de la condición de Corporación o Entidad en una persona natural distinta al Suscriptor que consta en el certificado, por ejemplo, porque deja de desempeñar cualquier tipo de actividad económica.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:

- Compromiso de la clave privada o de la infraestructura o sistemas de la ECD, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

- Infracción, por parte de la ECD o de la RA, de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la presente DPC o en la PC correspondiente.

- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Suscriptor.

- Acceso o utilización no autorizados, por un tercero, de la clave privada del Suscriptor.

- El incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la presente DPC, en la PC correspondiente o en el Contrato de Suscripción.

c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.

- Pérdida o inutilización por daños del dispositivo criptográfico.

- Acceso no autorizado, por un tercero, a los datos de activación del Suscriptor.

- El incumplimiento por parte del Suscriptor de las normas de uso del dispositivo criptográfico expuestas en la presente DPC, en la PC correspondiente o en el Contrato de Suscripción.

d) Circunstancias que afectan al Suscriptor y/o Solicitante:

- Finalización de la relación jurídica entre la ECD y el Suscriptor.

- Terminación del Contrato de Suscripción, de conformidad con las causales establecidas en dicho contrato.

- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al Suscriptor.

- Oposición o modificación, por parte del Suscriptor y/o Solicitante, de los datos contenidos en el fichero de datos de carácter personal de Thomas Signe S.A.S.

- Infracción por el Solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

- Infracción por el Suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en las condiciones generales de contratación.

- La incapacidad sobrevenida, total o parcial por el fallecimiento del Suscriptor.

e) Otras circunstancias:

- Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.

- Por resolución judicial o administrativa que lo ordene.

- Por la concurrencia de cualquier otra causa especificada en la presente DPC o en la PC correspondiente.

- Por cualquier causa que induzca a creer razonablemente que el servicio de certificación haya sido comprometido, poniendo en duda la confiabilidad del certificado digital.

4.9.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

Pueden solicitar la revocación de un certificado:

a) El propio Suscriptor y/o Solicitante, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

b) Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la revocación del certificado:

- Los operadores autorizados de la ECD (Operadores de Registro).

4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

Existen dos alternativas a la hora de solicitar la revocación del certificado.

En todo caso, en el momento de revocarse el certificado, se enviará un comunicado al Suscriptor, comunicando la hora y la causa de la misma.

Procedimiento online

Thomas Signe S.A.S. brinda el servicio de revocación online a través de los enlaces contenidos en su página web. Los Suscriptores y/o Solicitantes que deseen revocar sus certificados deberán ingresar en estos enlaces.

Mediante Operador de Registro

De forma alternativa, se podrá solicitar la revocación de un certificado mediante comunicación con el Responsable de PQRSA de la ECD Thomas Signe S.A.S. enviada a la dirección de correo electrónico pqrsa@thsigne.com, la cual será derivada a un Operador de Registro.

Cabe destacar que la solicitud de revocación tendrá que ser enviada desde la cuenta de correo electrónico declarada en el Formulario de solicitud respectivo (revocación solicitada por el Suscriptor o Solicitante) o, en otro caso, el Operador de Registro deberá verificar la causa de revocación comunicada y que ésta se corresponde con alguna de las circunstancias anteriormente indicadas.

4.9.4 PLAZO EN EL QUE LA ECD DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Una vez que la identidad del Suscriptor y/o Solicitante haya sido autenticada o que el Operador de Registro haya verificado la causa de revocación comunicada, según lo expuesto anteriormente, y que la revocación haya sido debidamente tramitada por la RA, la revocación se hará efectiva inmediatamente.

4.9.5 OBLIGACIÓN DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.9.6 FRECUENCIA DE EMISIÓN DE LAS CRLS

La CRL de Thomas Signe Root (CA Raíz) se emite antes de que hayan transcurrido 180 días desde la emisión de la anterior CRL (antes de su fin de validez) o cuando se produzca una revocación.

La CRL de la ECD Thomas Signe Colombia (CA Subordinada) se emite al menos cada 4 días (antes del fin de validez de la anterior CRL); en condiciones normales, la CRL se emite cada 24 horas o cuando se produzca una revocación.

4.9.7 TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DE LAS CRLS

Una vez emitida la CRL de Thomas Signe Root (CA Raíz), ésta se publica al menos antes del fin de validez de la anterior CRL (180 días después de su emisión); en condiciones normales, la CRL se publica el mismo día de su emisión.

Una vez emitida la CRL de la ECD Thomas Signe Colombia (CA Subordinada), ésta se publica al menos antes del fin de validez de la anterior CRL (4 días después de su emisión); en condiciones normales, la CRL se publica en el momento de la generación de la misma, por lo que se considera cero o nulo el tiempo transcurrido.

4.9.8 DISPONIBILIDAD DEL SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS

La información relativa al estado de los certificados 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, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 8 horas.

4.9.9 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA

Para el uso del servicio de CRLs, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión CRL Distribution Points.

- Se deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.

- Se deberá comprobar que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.

- Los certificados revocados que expiren podrán ser retirados de la CRL.

También se puede comprobar la revocación en línea por medio del servicio OCSP, de libre acceso, en la dirección URL contenida en el propio certificado en la extensión Authority Information Access.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 CARACTERÍSTICAS OPERACIONALES

Con el fin de proporcionar información sobre la validez de un certificado electrónico, y por consiguiente de la fiabilidad de la firma electrónica de un documento, Thomas Signe S.A.S., ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

Thomas Signe S.A.S. ofrece un servicio gratuito de acceso a validación de certificados en línea por medio del protocolo OCSP.

Adicionalmente, Thomas Signe S.A.S. puede ofrecer servicios comerciales de validación de certificados.

4.10.2 DISPONIBILIDAD DEL SERVICIO

La información relativa al estado de los certificados 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, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 8 horas

4.10.3 CARACTERÍSTICAS ADICIONALES

Thomas Signe S.A.S. puede disponer de servicios avanzados de validación de certificados que requieran de una licencia específica.

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES (KEY ESCROW AND RECOVERY)

La ECD Thomas Signe S.A.S. no ofrece un servicio de custodia de copias de respaldo y recuperación de claves privadas de los suscriptores (key escow).

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 el Centro de Datos subcontratado.

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 a los servicios de generación de certificados 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 ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas posee falso suelo, detección y extinción de incendios, sistemas anti-humedad, sistema de refrigeración y sistema 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.

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 del servidor 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 del Centro 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 distintos para la administración y operación de las plataformas de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S., destinadas a la generación y administración de las claves y a la administración de los perfiles de certificados y CRL de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S., y para la administración y operación de las plataformas de la RA de Thomas Signe S.A.S. (plataformas SAR, de la RA y del HSM Centralizado), destinadas a la administración y operación de la Autoridad de Registro de Thomas Signe S.A.S.

De esta forma, se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación y registro.

Los roles de confianza establecidos en el documento THS-CO-AC-MO-01 Diagrama Organizacional para la administración 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 CA Raíz y la CA Subordinada de Thomas Signe S.A.S., cumple el rol de Auditor de la CA.

- 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 CA Raíz y la CA Subordinada de Thomas Signe S.A.S., cumple el rol de Administrador de la CA.

- Administrador de Sistemas de la CA: responsable de supervisar la infraestructura técnica de los servicios de certificación digital de la ECD. Dentro de las plataformas de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S., cumple el rol de Administrador de la CA.

- Responsable de Registro Digital: responsable de la configuración de las plataformas de Thomas Signe RA y de la supervisión de las operaciones de validación de identidad de las personas que solicitan la emisión o revocación de certificados digitales. Dentro de las plataformas de la RA de Thomas Signe S.A.S., cumple el rol de Administrador de la RA.

- Operador de Registro: responsable de las funciones de validación de identidad de los solicitantes de certificados digitales y de la aprobación de las solicitudes. Dentro de las plataformas de la RA de Thomas Signe S.A.S., cumple el rol de Agente de la RA.

- Auditor de la Autoridad de Registro: audita los LOGs de la Autoridad de Registro. Dentro de las plataformas de la RA de Thomas Signe S.A.S., cumple el rol de Auditor de la RA.

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 la clave de las CA.

- La recuperación y back-up de la clave privada de las CA.

- La emisión de certificados de las CA.

- La revocación de certificados de las CA.

- Activación de la clave privada de las CA.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada rol de confianza de la CA Raíz, CA Subordinada y RA se autentica mediante la utilización de mecanismos de autenticación seguros. La autenticación dentro de las plataformas previamente mencionadas 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 procedimiento THS-CO-AC-MO-01 Diagrama Organizacional.

Los roles de la CA (Auditor de la CA, Administrador de la CA) son incompatibles con los de roles de la RA (Administrador de la RA, Agente de la RA, Auditor de la RA).

Los roles de la RA (Administrador de la RA, Agente de la RA, Auditor de la RA) son incompatibles entre ellos.

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 en el centro de operación técnica y tiene contrato laboral fijo.

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

La ECD se asegura que el personal de la RA es personal confiable para realizar las tareas de registro. A tal efecto se exige una Autorización para su rol dentro de Thomas Signe S.A.S.

El Operador de Registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones.

La ECD retirará de sus funciones de confianza a un empleado cuando se 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 proveedores 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 los requerimientos operacionales 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.

- Cambios en la creación de perfiles de certificados.

- Generación de claves propias.

- Eventos del ciclo de vida de de los certificados.

- 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 ceremonias de creación de claves de las CA.

- 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 claves privadas de la ECD.

5.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

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 en función de la importancia de cada log en concreto.

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 analizarán y se corregirán las vulnerabilidades que la ECD crea que son un riesgo para ella.

5.4.8 SUPERVISIÓN

Thomas Signe S.A.S. 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 EVENTOS ARCHIVADOS

La ECD Thomas Signe S.A.S. conservará los eventos que tengan lugar durante el ciclo de vida del certificado. Se almacenarán por la CA o, por delegación de ésta, en la RA:

- todos los datos de la auditoría,

- todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores y/o Solicitantes y los datos relativos a su identificación,

- solicitudes de emisión y revocación de certificados,

- todos los certificados emitidos o publicados,

- CRL's emitidas o registros del estado de los certificados generados,

- la documentación requerida por los auditores y

- las comunicaciones entre los elementos de la PKI

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

5.5.2 PERIODO DE CONSERVACIÓN DE REGISTROS

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán durante al menos un año desde su expiración. Los contratos con los Suscriptores y/o Solicitantes y cualquier información relativa a la identificación y autenticación del Suscriptor y/o Solicitante serán conservados durante al menos tres (03) años desde su finalización o el periodo que establezca la legislación vigente.

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 certificados, mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones externas al Centro de Datos de la ECD en los casos en que así se requiera.

Además, se disponen 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".

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 CA Raíz o de la CA Subordinada, la nueva clave pública de la CA a los Suscriptores, Solicitantes y Terceros aceptantes de los certificados emitidos con las nuevas claves es el mismo que para proporcionar la actual clave pública de la CA Raíz y de la CA Subordinada.

En consecuencia, el nuevo certificado de la CA conteniendo su nueva clave pública se publicará en la página web de Thomas Signe S.A.S.

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 CA Raíz o de la CA Subordinada, la seguridad del servicio de emisión de certificados 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 certificados e información relativa al estado de la revocación 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 EMISIÓN DE CERTIFICADOS

Ante el cese del servicio de emisión de certificados 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 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 certificados 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 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

La generación de las claves de la CA se realiza, de acuerdo con el proceso documentado de ceremonia de claves, en dispositivos criptográficos hardware certificados (HSM) FIPS 140-2 nivel 3, por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de Thomas Signe S.A.S., de la organización titular de la ECD y de un auditor externo.

Para los certificados de entidad final, la generación de claves se realizará en dispositivos que aseguren razonablemente que la clave privada únicamente puede ser utilizada por el Suscriptor, bien por medios físicos, bien estableciendo el Suscriptor los controles y medidas de seguridad adecuadas.

En los casos en que Thomas Signe S.A.S. pueda garantizar que las claves criptográficas del Suscriptor han sido creadas en un dispositivo criptográfico que cumpla con los requisitos mínimos (si el tipo de soporte es Tarjeta/Token o HSM Centralizado), se indicará en el propio certificado mediante la inclusión del identificador OID correspondiente en la extensión Certificate Policies.

En cualquier otro caso (si el tipo de soporte es Otros Dispositivos), los certificados se emitirán con un identificador OID diferente en la extensión Certificate Policies.

6.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS SUSCRIPTORES

La RA será responsable de garantizar la entrega del certificado al Suscriptor y/o Solicitante, ya sea entregándole el dispositivo de firma o habilitándole los mecanismos para su descarga y/o instalación y posterior uso, tal y como se especifica en la PC respectiva. De esta forma, se asegura que el Suscriptor y/o Solicitante utiliza, con un alto nivel de confianza, bajo su control exclusivo los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El envío de la clave pública a la ECD para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS #10 o equivalente autofirmado, utilizando un canal seguro para la transmisión.

6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA ECD A TERCEROS QUE CONFÍAN

Los Terceros que confían podrán consultar los certificados de la CA Raíz y la CA Subordinada, verificar la cadena de certificación y su fingerprint (huella digital). Dichos certificados se encuentran a disposición de los usuarios en la página web de Thomas Signe S.A.S.

6.1.5 TAMAÑO DE LAS CLAVES Y PERIODO DE VALIDEZ

Certificado	Tamaño claves RSA (bits)	Periodo validez
CA Raíz	4096	20 años Desde: 14/03/2018 13:50:35, tiempo UTC Hasta 14/03/2038 13:50:35, tiempo UTC
CA Subordinada	4096	Desde: 14/03/2018 13:59:37, tiempo UTC Hasta: 14/03/2038 00:00:00, tiempo UTC
OCSP CA Subordinada	2048	Desde: 05/04/2018 10:53:48, tiempo UTC Hasta: 14/03/2038 00:00:00, tiempo UTC
Suscriptores	2048	Como máximo, lo establecido en la legislación y normativa vigentes

6.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas ETSI TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

Signature suite	Hash function	Signature algorithm
sha256-with-rsa	SHA-256	RSA-PKCSv1_5

6.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

Todos los certificados incluyen las extensiones Key Usage y Extended Key Usage, indicando los usos habilitados de la claves.

Los usos admitidos para los certificados de la CA Raíz y la CA Subordinada son firma de certificados y firma de CRLs.

En cuanto a los usos admitidos de la clave para cada certificado de usuario final, se encuentran definidos en la Política de Certificación correspondiente.

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 ECD están certificados con la norma FIPS 140-2 nivel 3.

Las claves de los Suscriptores de certificados HSM Centralizado y de los certitficados de operadores y administradores de la RA en Tarjeta/Token son generadas de forma segura utilizando un dispositivo criptográfico con FIPS 140-2 nivel 3, dando lugar a un nivel de aseguramiento alto para proteger las claves privadas frente a riesgos como:

- Ataques de código malicioso
- Exportación no autorizada de claves
- Suplantación de identidad por descuido del Suscriptor en la custodia de dispositivos criptográficos
- Daño físico del módulo criptográfico

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

El acceso a las claves privadas de la CA Raíz y la CA Subordinada se encuentra bajo control multipersona. Es decir, se requiere más de una persona 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 las claves privadas de la CA Raíz y la CA Subordinada.

6.2.3 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la CA Raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y posterior uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de la CA Subordinada está custodiada en un dispositivo criptográfico seguro certificado 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 anteriormente.

Thomas Signe S.A.S. no custodia copias de respaldo de las claves privadas de los Suscriptores de certificados (key escrow).

6.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Existen unos dispositivos que permiten la restauración de las clave privadas de la CA Raíz y la CA Subordinada, que son almacenados de forma segura y sólo accesibles por personal autorizado según los roles de confianza, usando distintos controles, siendo uno de ellos el control dual en un medio físico seguro.

Las claves de la CA Raíz y la CA Subordinada se pueden restaurar por un proceso que requiere la utilización de 2 de 3 dispositivos criptográficos (llaves).

6.2.5 ARCHIVO DE LA CLAVE PRIVADA

Thomas Signe S.A.S. no archivará las claves privadas de firma de certificados de la CA Raíz y la CA Subordinada después de la expiración del periodo de validez de la misma.

6.2.6 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Existe un documento de ceremonia de claves de Thomas Signe S.A.S., donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.2.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de la CA Raíz y la CA Subordinada se activan por un proceso que requiere la utilización 2 de 3 dispositivos criptográficos (llaves).

6.2.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Cada vez que se reinicie la aplicación las claves privadas de la CA Raíz y de la CA Subordinada se desactivarán por un proceso que requiere la utilización 2 de 3 dispositivos criptográficos (llaves).

6.2.9 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de la CA Raíz y de la CA Subordinada, o de los datos de activación de las mismas, incluyendo también los dispositivos que contengan copias de dichas claves o de sus datos de activación

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Thomas Signe S.A.S. conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este activo y 6 meses más como mínimo, en otro caso.

6.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no se garantiza un servicio de verificación en línea válido para ese certificado.

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de las claves de la CA Raíz y la CA Subordinada fueron generados de forma segura durante la ceremonia de creación de claves de las CA.

En el caso de certificados de operadores y administradores de la RA en Tarjeta/Token, los datos de activación (PIN y PUK) son generados en el momento de inicialización del dispositivo criptográfico.

En el caso de certificados de Suscriptores generados en HSM Centralizado, los datos de activación serán generados al mismo tiempo que las claves en el HSM Centralizado, en el instante previo a la emisión del certificado (contraseña), o cada vez que se accede a una clave en el HSM Centralizado (código recibido en el teléfono celular).

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y/o de los datos de activación, es responsabilidad del Suscriptor de mantener la confidencialidad de estos datos.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

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 el Centro de Datos subcontratado.

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.

Cada una de las Políticas y procedimiento indica su nivel de confidencialidad. 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 de 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 el Diagrama Organizacional.

- 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 del certificado:

- 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 certificados se realiza mediante un sistema m de n operadores para la activación de la clave privada de la CA Raíz y de la CA Subordinada de Thomas Signe S.A.S.

c) Gestión de la revocación:

- 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 al sistema de revocaciones.

- La revocación se refiere a la perdida de efectividad de un certificado digital de forma permanente. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de Thomas Signe S.A.S.

d) Estado de la revocación

- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

Gestión del ciclo de vida del hardware criptográfico

- 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 test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

- El dispositivo criptográfico solo es manipulado por personal confiable.

- Las claves privadas de firma de la CA Raíz y de la CA Subordinada almacenadas en el hardware criptográfico se eliminarán una vez se haya retirado el dispositivo.

- 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, CRL Y OCSP

7.1 PERFIL DE CERTIFICADO

7.1.1 FORMATO DEL CERTIFICADO

Los certificados emitidos por la ECD Thomas Signe S.A.S. son certificados X.509 v3, conforme a los siguientes estándares:

- 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.

Adicionalmente, los certificados emitidos por Thomas Signe S.A.S. son coherentes con lo dispuesto en los siguientes estándares:

- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

En la tabla siguiente se especifica el perfil común de los certificados emitidos por la CA Raíz y la CA Subordinada de la ECD Thomas Signe S.A.S.

PERFIL COMÚN DE LOS CERTIFICADOS			
Campo del certificado		**Descripción**	**Valor**
version		N° de versión	v3
serialNumber		N° de serie	Número entero positivo único con respecto a la CA que emite el certificado [1]
signature		Algoritmo de firma	OID [2] y parámetros del algoritmo de firma
issuer		Emisor (DN)	DN de la CA que emite el certificado [3]
validity	**notBefore**	Válido desde	Fecha y hora de inicio de validez del certificado, tiempo UTC [4]
	notAfter	Válido hasta	Fecha y hora de fin de validez del certificado, tiempo UTC [5]
subject		Asunto (DN)	DN del titular del certificado [6]
subjectPublicKeyInfo		Clave pública	OID [7] y parámetros del algoritmo y valor [8] de la clave pública
extensions		Extensiones del certificado	Extensiones del certificado [9]

[1] Valor aleatorio de 20 bytes

[2] sha256WithRSAEncryption (ver OID en la sección 7.1.3)

[3] Certificados de CA Raíz, CA Subordinada y TSU TSA de la ECD Thomas Signe S.A.S: ver DN de la CA Raíz en la sección 7.1.4; Certificados de OCSP CA Subordinada y de Suscriptores de la ECD Thomas Signe S.A.S: ver DN de la CA Subordinada en la sección 7.1.4

[4] Fecha y hora de emisión del certificado

[5] Certificados de CA Raíz, CA Subordinada y OCSP CA Subordinada de la ECD Thomas Signe S.A.S: ver periodo de validez en la sección 6.1.5; Certificado de TSU TSA de la ECD Thomas Signe S.A.S: ver periodo de validez en la DPC para el estampado cronológico de Thomas Signe S.A.S.; Certificados de Suscriptores de la ECD Thomas Signe S.A.S: ver periodo de validez en la PC correspondiente al tipo de certificado

[6] Certificados de CA Raíz y CA Subordinada de la ECD Thomas Signe S.A.S: ver DN en la sección 7.1.4; Certificado de OCSP CA Subordinada de la ECD Thomas Signe S.A.S: ver DN en la sección 7.4.4; Certificado de TSU TSA de la ECD Thomas Signe S.A.S: ver DN en la DPC para el estampado cronológico de Thomas Signe S.A.S.; Certificados de Suscriptores de la ECD Thomas Signe S.A.S: ver DN del titular en la PC correspondiente al tipo de certificado

[7] rsaEncryption (ver OID en la sección 7.1.3)

[8] Certificados de CA Raíz, CA Subordinada, OCSP CA Subordinada y Suscriptores de la ECD Thomas Signe S.A.S: ver tamaño claves RSA en la sección 6.1.5; Certificado de TSU TSA de la ECD Thomas Signe S.A.S: ver tamaño claves RSA en la DPC para el estampado cronológico de Thomas Signe S.A.S.

[9] Certificados de CA Raíz y CA Subordinada de la ECD Thomas Signe S.A.S: ver extensiones en la sección 7.1.2; Certificado de OCSP CA Subordinada de la ECD Thomas Signe S.A.S: ver extensiones en la sección 7.4.2; Certificado de TSU TSA de la ECD Thomas Signe S.A.S: ver extensiones en la DPC para el estampado cronológico de Thomas Signe S.A.S.; Certificados de Suscriptores de la ECD Thomas Signe S.A.S: ver extensiones en la PC correspondiente al tipo de certificado

7.1.2 EXTENSIONES DEL CERTIFICADO

En las tablas siguientes se especifican las extensiones de los certificados de la CA Raíz y de la CA Subordinada de la ECD Thomas Signe S.A.S.

EXTENSIONES DEL CERTIFICADO DE CA RAÍZ – THOMAS SIGNE ROOT		
Extensión	**Crítica**	**Valor**
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	keyCertSign cRLSign
Certificate Policies	-	OID anyPolicy (2.5.29.32.0) URI de la DPC: http://thsigne.com/cps
Basic Constraints	Sí	cA: TRUE

EXTENSIONES DEL CERTIFICADO DE CA SUBORDINADA – ECD THOMAS SIGNE COLOMBIA		
Extensión	**Crítica**	**Valor**
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Raíz, 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	keyCertSign cRLSign
Certificate Policies	-	OID anyPolicy (2.5.29.32.0) URI de la DPC: http://thsigne.com/cps
Basic Constraints	Sí	cA: TRUE pathLenConstraint: 0
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: http://thsigne.com/certs/thomas_signe_root.crt

En la sección 7.4.2 se especifican las extensiones del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S.

En la PC de cada tipo de certificado se especifican las extensiones de los correspondientes certificados de Suscriptores de la ECD Thomas Signe S.A.S.

En la DPC para el estampado cronológico de Thomas Signe S.A.S se especifican las extensiones del certificado de TSU de la TSA de la ECD Thomas Signe S.A.S.

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Nombre	OID	Descripción
sha256WithRSAEncryption	1.2.840.113549.1.1.11	Algoritmo de firma de certificados, CRL y respuestas OCSP
rsaEncryption	1.2.840.113549.1.1.1	Algoritmo de clave pública en certificados

7.1.4 FORMATOS DE NOMBRES

En las tablas siguientes se especifican los correspondientes atributos del DN de la CA Raíz y de la CA Subordinada la ECD Thomas Signe S.A.S.

DN DE LA CA RAÍZ – THOMAS SIGNE ROOT		
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 Root [2]

[1] Codificado en PrintableString

[2] Codificado en UTF8String

DN DE LA CA SUBORDINADA – ECD THOMAS SIGNE COLOMBIA		
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	ECD Thomas Signe Colombia [2]

En la sección 7.4.4 se especifica el DN del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S.

En la PC de cada tipo de certificado se especifican el DN del titular de los correspondientes certificados de Suscriptores de la ECD Thomas Signe S.A.S.

En la DPC para el estampado cronológico de Thomas Signe S.A.S. se especifica el DN del certificado de TSU de la TSA de la ECD Thomas Signe S.A.S.

7.1.5 RESTRICCIONES DE LOS NOMBRES

Según lo especificado en las secciones 3.1 y 7.1.4 y en la PC de cada tipo de certificado.

7.1.6 IDENTIFICADORES DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICADOS

El OID de la política del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S se encuentra especificado en la sección 7.4.2 y también a continuación: 1.3.6.1.4.1.51362.0.2.0.1

Los OID de la Política de Certificados de cada tipo de certificados de Suscriptores de la ECD Thomas Signe S.A.S. se encuentran especificados en la sección 1.4 y en la PC correspondiente.

El OID de la política del certificado de TSU de la TSA de la ECD Thomas Signe S.A.S. se encuentra especificado en la DPC para el estampado cronológico de Thomas Signe S.A.S.

[1] Codificado en PrintableString

[2] Codificado en UTF8String

7.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINTS

Los certificados emitidos por la CA Raíz y la CA Subordinada de la ECD Thomas Signe S.A.S. no contienen la extensión Policy Contraints.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

La extensión Certificate Policies de los certificados emitidos por la CA Raíz y la CA Subordinada de la ECD Thomas Signe S.A.S. contiene los siguientes Policy Qualifiers:

- id-qt-cps (URI de la DPC): contiene la URI donde se puede encontrar la última versión de la presente DPC, así como, en el caso de los certificados de Suscriptores de la ECD Thomas Signe S.A.S., la PC correspondiente al tipo de certificado.

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY

La extensión Certificate Policies de los certificados emitidos por la CA Raíz y la CA Subordinada de la ECD Thomas Signe S.A.S. permite identificar la política que la ECD Thomas Signe S.A.S. asocia al tipo de certificado y dónde se puede encontrar la presente DPC, así como, en el caso de los certificados de Suscriptores de la ECD Thomas Signe S.A.S., la PC correspondiente al tipo de certificado.

7.2 PERFIL DE CRL

7.2.1 FORMATO Y PERIODO DE VALIDEZ DE LA CRL

Las CRL emitidas por la ECD Thomas Signe S.A.S. son CRL X.509 v2, conforme a los siguientes estándares:

- 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.

En la tabla siguiente se especifica el perfil común de las CRL emitidas por la CA Raíz y la CA Subordinada de Thomas Signe S.A.S.

PERFIL DE CRL			
Campo de la CRL		**Descripción**	**Valor**
version		N° de versión	v2
signature		Algoritmo de firma	OID [1] y parámetros del algoritmo de firma
issuer		Emisor (DN)	DN de la CA que emite la CRL[2]
thisUpdate		Fecha y hora de emisión de esta CRL	Fecha y hora de emisión de la CRL, tiempo UTC
nextUpdate		Fecha y hora de emisión de la próxima CRL	Fecha de fin de validez de la CRL, tiempo UTC [3]
revokedCertificates	**userCertificate**	N° de serie del certificado revocado	N° de serie del certificado revocado
	revocationDate	Fecha y hora de revocación del certificado	Fecha y hora de revocación del certificado, tiempo UTC
	crlEntryExtensions	Extensiones de entrada de CRL	Extensiones de entrada de CRL
crlExtensions		Extensiones de la CRL	Extensiones de la CRL

7.2.2 EXTENSIONES DE LA CRL Y DE ENTRADA DE CRL

EXTENSIONES DE LA CRL		
Extensión	**Crítica**	**Valor**
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA que emite la CRL, obtenido a partir del hash SHA-1 de la misma
CRL Number	-	Número incremental, con respecto a la CA que emite la CRL

EXTENSIONES DE ENTRADA DE CRL		
Extensión	**Crítica**	**Valor**
Reason Code	-	Código del motivo de revocación del certificado

[1] sha256WithRSAEncryption (ver OID en la sección 7.1.3)

[2] CRL de CA Raíz: ver DN de la CA Raíz en la sección 7.1.4; CRL de CA Subordinada: ver DN de la CA Subordinada en la sección 7.1.4

[3] CRL de CA Raíz: 180 días; CRL de CA Subordinada: 4 días

7.3 PERFIL DE OCSP

El perfil OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S. es conforme al estándar RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", con las siguientes particularidades:

- Algoritmo de firma de respuestas OCSP: sha256WithRSAEncryption (ver OID en la sección 7.1.3)

7.4 PERFIL DE CERTIFICADO OCSP

7.4.1 FORMATO DEL CERTIFICADO

El formato del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S. cumple lo especificado en la sección 7.1.1.

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

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

El certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S. ha sido emitido por la propia CA Subordinada (Thomas Signe Colombia).

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

7.4.2 EXTENSIONES DEL CERTIFICADO

En la tabla siguiente se especifican las extensiones del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S.

Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Subordinada, 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 1.3.6.1.4.1.51362.0.2.0.1 URI de la DPC: http://thsigne.com/cps
Basic Constraints	Sí	cA: FALSE
Extended Key Usage	Sí	OCSPSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points	-	URI de la CRL: http://crl-co.thsigne.com/ecd_thomas_signe_colombia.crl
Authority Information Access	-	URI del certificado de la CA Subordinada: http://thsigne.com/certs/ecd_thomas_signe_colombia.crt

7.4.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Según lo especificado en la sección 7.1.3

7.4.4 FORMATOS DE NOMBRES

En la tabla siguiente se especifican los correspondientes atributos del DN del certificado OCSP de la CA Subordinada de la ECD 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	ECD Thomas Signe Colombia – OCSP [2]

7.4.5 RESTRICCIONES DE LOS NOMBRES

Según lo especificado en las secciones 3.1, 7.1.4 y 7.4.4.

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

El OID de la política del certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S se encuentra especificado en la sección 7.4.2 y también a continuación: 1.3.6.1.4.1.51362.0.2.0.1

7.4.7 USO DE LA EXTENSIÓN POLICY CONSTRAINTS

El certificado OCSP de la CA Subordinada de la ECD Thomas Signe S.A.S no contiene la extensión Policy Contraints.

---

[1] Codificado en PrintableString

[2] Codificado en UTF8String

7.4.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Según lo especificado en la sección 7.1.8.

7.4.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY

Según lo especificado en la sección 7.1.9.

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 ningún conflicto de intereses que pueda 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 tratarán 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 TARIFAS DE EMISIÓN DE CERTIFICADOS

En la PC de cada tipo de certificado se especifican las tarifas de emisión para los correspondientes certificados.

Las tarifas especificadas en las PC son referenciales, por lo que pueden variar de acuerdo al tipo de certificado y al contrato con cada cliente.

Las mismas tarifas se encuentran publicadas en la página web de Thomas Signe S.A.S.

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

9.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos, es libre y gratuito.

9.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

No se establece ninguna tarifa para la revocación de certificados, ni para el acceso a la información de estado de los certificados.

9.1.4 TARIFAS DE OTROS SERVICIOS

Las tarifas aplicables a otros posibles servicios se negociarán entre Thomas Signe S.A.S y los clientes de los servicios ofrecidos.

9.1.5 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.

- La entidad aseguradora se encarga de informar previamente a ONAC la terminación del contrato de seguro o si se realizan modificaciones que reducen el alcance o monto de la cobertura pactada.

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 no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.3.1 INFORMACIÓN CONFIDENCIAL

En particular, la siguiente información será considerada confidencial:

- Las claves privadas de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S.

- Acta de Ceremonia de generación de las claves de la CA Raíz y la CA Subordinada.

- Procedimiento de Ceremonia de generación de las claves de la CA Raíz y la CA Subordinada.

- 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 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 contenida en las distintas Políticas de Certificados (PC).

- La información contenida en los certificados, puesto que para su emisión el Suscriptor y/o Solicitante otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.

- Las listas de revocación de certificados (CRL’s), así como las restantes informaciones de estado de revocación.

- Cualquier información cuya publicidad sea impuesta normativamente.

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-4.1-10 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.

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, listas de revocación y cualesquiera otros, relacionados con su actividad como ECD, incluida la presente DPC y las PC asociadas, 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 y en las PC asociadas, así como en el Contrato de Suscripción.

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

c) Informar sobre las modificaciones de esta DPC y de las PC asociadas a los Suscriptores, 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.

e) Utilizar sistemas fiables para almacenar certificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el Suscriptor y/o Solicitante hayan indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Por lo que a los certificados respecta:

a) Emitir certificados conforme a esta DPC, a las PC correspondientes y a los estándares de aplicación.

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

c) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.

d) Revocar los certificados según lo dispuesto en esta DPC y en las PC correspondientes y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados).

Sobre custodia de información:

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

b) No almacenar ni copiar los datos de creación de firma del Suscriptor, cuando así lo disponga la normativa vigente.

c) Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase.

d) Proteger sus claves privadas de forma segura.

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

f) Remitir a ONAC, con frecuencia anual, para la realización de la Etapa 1 de cada evaluación de la acreditación:

- Archivo con los certificados emitidos y su respectivo contenido.

- Archivo con totales de control (emitidos, vigentes, revocados y expirados).

Como Autoridad de Registro (RA) también se obliga en los términos definidos en la presente DPC para la emisión de certificados, principalmente a:

a) Respetar lo dispuesto en esta DPC y en la PC correspondiente al tipo de certificado que emita.

b) Respetar lo dispuesto en los contratos firmados con el Suscriptor. En el ciclo de vida de los certificados:

- Comprobar la identidad de los Solicitantes de certificados según lo descrito en esta DPC o mediante otro procedimiento que haya sido aprobado por la ECD.

- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.

- Informar al Suscriptor, antes de la emisión de un certificado, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de la ECD, de la DPC y de la PC correspondiente al certificado.

- Tramitar y entregar los certificados conforme a lo estipulado en esta DPC y en la PC correspondiente.

- Tramitar el Contrato de Suscripción según lo establecido por la Política de Certificación aplicable.

- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor y/o Solicitante.

- Informar a la CA Subordinada de las causas de revocación.

- Realizar las comunicaciones con los Suscriptores, por los medios que consideren adecuados, para la correcta gestión del ciclo de vida de los certificados. Concretamente, realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las revocaciones de los mismos.

9.6.2 OBLIGACIONES DE LOS PROVEEDORES

El Proveedor de infraestructura tecnológica de Thomas Signe S.A.S. y el Proveedor de Servicios Locales se encuentran obligados a cumplir con los requisitos mínimos exigidos por ONAC, dispuestos en el documento CEA 4.1-10 vigente, tales como:

a) Responsabilidad y financiación

b) Confidencialidad

c) Requisitos para los recursos

d) Requisitos del proceso – Ciclo de vida del certificado digital

e) Requisitos del sistema de gestión

f) Requisitos de la CA

g) Requisitos de la RA

h) Requisitos técnicos

9.6.3 OBLIGACIONES DE LOS SOLICITANTES

El Solicitante de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Suministrar a la RA la información necesaria para realizar una correcta identificación.

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

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

d) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

e) Informar a la mayor brevedad posible del conocimiento de alguna causa de revocación.

9.6.4 OBLIGACIONES DE LOS SUSCRIPTORES

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

a) Custodiar de manera diligente sus claves privadas y/o los datos de activación de las mismas (tales como contraseñas o códigos secretos definidos o recibidos por algún medio).

b) Usar el certificado según lo establecido en la presente DPC y en la PC correspondiente.

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

d) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

e) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.

f) No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la ECD o la RA de la revocación del mismo, o una vez expirado el plazo de validez del certificado.

9.6.5 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

b) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas.

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

9.6.6 OBLIGACIONES DE LA ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR

En los tipos de certificado que sea aplicable, la Entidad a la cual se encuentra vinculado el Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Suministrar al Solicitante y/o a la RA la información necesaria para realizar una correcta identificación.

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

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

d) Notificar cualquier cambio en su conocimiento en los datos aportados para la creación del certificado durante su periodo de validez.

e) Informar a la mayor brevedad posible del conocimiento de alguna causa de revocación.

9.7 RESPONSABILIDADES

9.7.1 RESPONSABILIDADES DE LA ECD

- Cumplir con los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-4.1-10 vigente, establecidos por el ONAC.

- Informar a sus proveedores de que hace extensivo el cumplimiento de los requisitos dispuestos en el documento CEA 4.1-10 vigente, cuando les corresponda.

- Garantizar que los certificados cumplen con todos los requisitos materiales establecidos en la DPC y que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la ECD Thomas Signe S.A.S.

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

- Brindar al Suscriptor información acerca de cómo validar el certificado, incluyendo el requisito de comprobar el estado del mismo y las condiciones en las cuales se puede confiar razonablemente en el certificado, lo cual resulta aplicable cuando el Suscriptor actúa como Tercero que confía.

- 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 R-AC-01 y R-AC-1.4-03.

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

- En cuanto a sus actividades como RA, notificará al ONAC cuando se establezca una nueva Oficina de Registro, donde se seguirá los mismos procedimientos y cumplirá los mismos requisitos que la Oficina Principal de Thomas Signe S.A.S.

- 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.

- Emplear adecuadamente el certificado respecto a su aplicación, limitaciones y prohibiciones de uso; conforme a lo establecido en la DPC de 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.

- Al hacer referencia al servicio de certificación digital en medios de comunicación, tales como documentos, folletos o publicidad, informar de que cumple con los requisitos especificados en la respectiva PC de Thomas Signe S.A.S.

- 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.

- Solicitar la revocación del certificado digital en caso de: pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada; compromiso potencial de la clave privada; pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa; inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer.

- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado

- No utilizar válidamente el certificado expirado a partir de la fecha en la que expira.

- Solicitar la revocación de certificados cuando incumple las obligaciones a las que se encuentra comprometido dentro de los requerimientos de ONAC.

- Informar 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, o cualquier otro caso de fuerza mayor.

b) Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la CA.

c) Por el uso indebido de la información contenida en el Certificado o en la CRL.

d) Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.

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

- Falta de veracidad de la información suministrada para emitir el certificado.

- Retraso en la comunicación de las causas de revocación del certificado.

- Ausencia de solicitud de revocación del certificado cuando proceda.

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

- Uso del certificado fuera de su periodo de vigencia, o cuando la ECD Thomas Signe S.A.S. o la RA le notifique la revocación del mismo.

- Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la DPC de la ECD, en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al Suscriptor por la ECD.

f) En relación a acciones u omisiones del Tercero que confía en el certificado:

- Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la DPC de la ECD en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

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

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 de los servicios de emisión, revocación y distribución de los certificados digitales, así como a la presente DPC y las PC asociadas.

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 una firma o certificado digital durante o después de la fecha de creación del certificado y estarán sujetos al pago de indemnizaciones por los corespondientes daños causados según lo establecido en la normativa reguladora de la prestación de los servicios de emisión, revocación y distribución de los certificados digitales.

9.10 PERIODO DE VALIDEZ

9.10.1 PLAZO

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

9.10.2 SUSTITUCIÓN Y DEROGACIÓN DE LA DPC Y LAS PC

Esta DPC y las PC asociadas serán sustituidas 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 y las PC asociadas, 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 PQRSA

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

Los Solicitantes, Suscriptores, Terceros que confían o el público en general indicarán su PQRSA 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 PQRSA serán gestionados por el Responsable de PQRSA 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 PQRSA y cuando esta sea resuelta. Thomas Signe S.A.S. cuenta con el procedimiento de THS-CO-AC-PR-02 Procedimiento de PQRSA para el tratamiento de PQRSA 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 Y PC

Todos los cambios en esta DPC y en las PC asociadas 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 y de las PC asociadas son enviadas a ONAC y publicadas en la página web de Thomas Signe S.A.S.

9.13 RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC o a las PC asociadas, 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 certificados emitidos.

9.14 LEY APLICABLE

La legislación aplicable al presente documento, así como a las PC asociadas y 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 el apartado anterior.

9.16 ESTIPULACIONES DIVERSAS

9.16.1 CONTRATO DE SUSCRIPCIÓN

El Contrato de Suscripción para el servicio de emisión de certificados vigente se encuentra publicado en la siguiente página web:

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

Se usa el mismo modelo de contrato para todos los tipos de certificados. En el contrato se deberán rellenar el tipo de certificado contratado y su vigencia.

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 y de las PC asociadas.

9.16.3 INDEPENDENCIA

En el caso de que cualquiera de los apartados recogidos en la presente DPC o en las PC asociadas 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-01-F01 Formulario de Solicitud de Certificado de Componente

THS-CO-AC-DPC-01-F02 Formulario de Solicitud de Certificado de Persona Jurídica

THS-CO-AC-DPC-01-F03 Formulario de Solicitud de Certificado de Persona Natural

THS-CO-AC-DPC-01-F04 Formulario de Solicitud de Certificado de Pertenencia a Empresa

THS-CO-AC-DPC-01-F05 Propuesta Comercial de Certificados Digitales - Persona Jurídica

THS-CO-AC-DPC-01-F06 Propuesta Comercial de Certificados Digitales - Persona Natural

THS-CO-AC-DPC-01-F07 Propuesta Comercial de Certificados Digitales - Pertenencia a Empresa

THS-CO-AC-DPC-01-F08 Propuesta Comercial de Certificados Digitales - Componente

THS-CO-AC-DPC-01-F09 Contrato de Suscripción para Emisión de Certificados

THS-CO-AC-DPC-01-F10 Autorización Solicitud Certificado de Componente - Persona Natural

THS-CO-AC-DPC-01-F11 Autorización Solicitud Certificado de Pertenencia a Empresa

THS-CO-AC-DPC-01-F12 Autorización Solicitud Certificado de Componente - Otra Entidad

THS-CO-AC-DPC-01-F13 Autorización Solicitud Previa Certificado de Componente - Otra Entidad

THS-CO-AC-DPC-01-F14 Contrato de Prestación de Servicios para el Suministro de Certificados Digitales de Componente

THS-CO-AC-DPC-01-F15 Protocolo de lectura para videoconferencia de verificación identidad

11 REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
Formularios completos de Solicitud de Certificado	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Propuestas comerciales firmadas de Certificados Digitales	Informático	Gerente Comercial	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Contratos firmados de Suscripción para Emisión de Certificados	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Autorizaciones firmadas Solicitud Certificado	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Contratos firmados de Prestación de Servicios para el Suministro de Certificados Digitales de Componente	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Videoconferencias grabadas verificación identidad	Informático	Operador de Registro	Plataforma de la RA	3 años o de acuerdo a normativa aplicable