Entidad de Certificación Digital

THOMAS SIGNE
Soluciones Tecnológicas Globales

Política de Seguridad

Información del documento

Nombre	POLÍTICA DE SEGURIDAD
Realizado por	THOMAS SIGNE S.A.S.
País	COLOMBIA
Versión	2.8
Fecha	JULIO DE 2022
Tipo de Documento	CONFIDENCIAL
Código	THS-CO-AC-POL-00

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.
2.0	30/03/2018	Adecuación del documento.
2.1	11/06/2018	Se agregan apartados para formatos y registros aplicables.
2.2	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”.
2.3	11/03/2019	Integración en el sistema de gestión del grupo. Cambio de nombre de documento de THS-POL-SI-01 a THS-CO-POL-AC-00
2.4	06/09/2019	Ajuste de la codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.1. Inclusión del rol Auditor de la Autoridad de Registro en

		el apartado 5.3.2.1.
2.5	04/10/2019	Revisión detallada de los documentos refrenciados a lo largo del documento.
2.6	31/01/2020	Ajuste del documento tras revisión de las DPCs por el quipo multidisciplinar para unificar información e incluir criterios revisados.
2.7	24/06/2021	Cambio de imagen THS. Se cambian los nombres de los tipos de certificados.
2.8	07/07/2022	Revisión del documento para cumplimiento del CEA 3.0-07

ÍNDICE

1. OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de seguridad de la información que cumple ThomasSigne para la administración de sus servicios como Entidad de Certificación Digital – ECD, en el marco del cumplimiento de los Criterios específicos de acreditación Entidades de Certificación Digital - CEA-3.0-07 vigente establecidos por el Organismo Nacional de Acreditación de Colombia – ONAC.

2. ÁMBITO DE APLICACIÓN

La presente política es de cumplimiento obligatorio para Thomas Signe S.A.S. y subcontratados que realizan los servicios de certificación digital de la ECD.

3. DOCUMENTACIÓN RELACIONADA

THS-CO-AC-MSG Manual del Sistema de Gestión

THS-CO-RRHH-PR-01 Funciones y Responsabilidades

THS-CO-AC-PR-11 Gestión de acceso al Sistema de la CA

THS-CO-SI-PR-01 Gestión del riesgo - 03 BIA - DRP

THS-CO-AC-PR-05 Gestión de claves

THS-CO-AC-PR-11 Backup y restauración del HSM

THS-CO-AC-DPC-01 Declaración de Prácticas de Certificación para la Emisión de Certificados

THS-CO-AC-DPC-02 Declaración de Prácticas de Certificación para Estampado cronológico

THS-CO-AC-DPC-04 Declaración de Prácticas de Certificación para Archivo y conservación de mensaje de datos

THS-CO-AC-PC-COR-01 Política de Certificados para Firma Automatizada

THS-CO-AC-PC-COR-02 Política de Certificados para Vinculación a Empresa_Entidad

THS-CO-AC-PC-COR-03 Política de Certificados para Representante Legal

THS-CO-AC-PC-PER-04 Política de Certificados para Persona Natural

THS-CO-AC-PC-COR-05 Política de Certificados para Función Pública

GSIGNE-SI-PR-01 Gestión del riesgo

GSIGNE-SI-PR-11 Seguridad Física y del entorno.

GSIGNE-RRHH-PR-02 Selección de personal

GSIGNE-RRHH-PR-03 Formación

GSIGNE-RRHH-PR-05 Procedimiento Sancionador

GSIGNE-SI-PR-17 Aspectos de Seguridad de la Información para la GCN

GSIGNE-SI-PR-12 Seguridad en las operaciones

4. DEFINICIONES

4.1 ACRÓNIMOS Y ABREVIACIONES

PC Políticas de los certificados

CRL Lista de Certificados Revocados

DPC Declaración de prácticas de certificación

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

HSM Hardware Security Module

ONAC Organismo Nacional de Acreditación de Colombia

OCSP Servicio del estado del certificado en línea

PKI Infraestructura de llave pública

RA Autoridad de Registro

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

TSA Time Stamp Authority, (Autoridad de sellado de tiempo).

4.2 DEFINICIONES Y CONCEPTOS

Autoridad de sellado de tiempo: Entidad de confianza que emite sellos de tiempo..

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.

Certificado digital: mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste 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.

Declaración de Prácticas de Certificación: Es el documento en el que consta de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que una ECD emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

Entidad de Certificación: De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, es 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.

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; y 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.

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 o Hash: es una 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.

Lista de Certificados Digitales Revocados: es aquella relación que debe incluir todos los certificados revocados por la entidad de certificación digital.

PKI: Infraestructura de llave 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 y evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío (no repudio).

Políticas de Certificación: Es el 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.

Revocación: Para este documento, es el 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. .

Estampado cronológico (Sellado de tiempo o Time stamping en Ingles): 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

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

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).

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 PC de éstas, para acceder al servicio de certificación digital.

Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital.

Tercero que confía: persona natural o jurídica que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

5. ACTIVIDADES

5.1 POLÍTICA DE SEGURIDAD

La Gerencia General reconoce la importancia de identificar y proteger los activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros que forman parte de los servicios brindados por la Entidad de Certificación Digital de Thomas Signe S.A.S. Asimismo se compromete a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

5.2 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Gerencia de Sistemas de Información realiza periódicamente un proceso de análisis del riesgo y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en la Metodología de Apreciación del Riesgo e Impacto en el Negocio, en los documentos del procedimiento GSIGNE-SI-PR-01 Gestión del riesgo

5.3 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 de Telefónica.

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.

5.3.1 CONTROLES FÍSICOS

La CA 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 electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Robo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

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.

5.3.1.1 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.

5.3.1.2 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.

5.3.1.3 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.

5.3.1.4 EXPOSICIÓN AL AGUA

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

5.3.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

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

5.3.1.6 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.

5.3.1.7 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.

5.3.1.8 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.

5.3.2 CONTROLES DE PROCEDIMIENTO

5.3.2.1 ROLES DE CONFIANZA

Se cuenta con roles de confianza distintos para la administración de las plataformas de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S., destinada a la generación y administración de las claves de la CA Raíz y la CA Subordinada de Thomas Signe S.A.S., y para la administración de las plataformas de Thomas Signe RA, destinada a la administración 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.

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 Thomas Signe RA, 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 Thomas Signe RA, cumplen 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 Thomas Signe RA, cumple el rol de Auditor de la RA.

5.3.2.2 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.

5.3.2.3 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.

5.3.2.4 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).

El rol de Auditor de la CA es incompatible con el rol de Administrador de la CA.

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

.

5.3.3 CONTROLES DE PERSONAL

5.3.3.1 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 del 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.

5.3.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

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

5.3.3.3 REQUISITOS DE FORMACIÓN

Se llevan a cabo los cursos necesarios al personal para asegurar la correcta realización de las tareas asignadas a srus 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.

5.3.3.4 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.

5.3.3.5 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.

5.3.3.6 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.

5.3.3.7 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.

5.3.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.3.4.1 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 ECDa 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.
- Eventos del ciclo de vida de los certificado.
- Eventos asociados al módulo criptográfico
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

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

- Las 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 laECD.

5.3.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

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

5.3.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría por un periodo mínimo de tres (03) años para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

5.3.4.4 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.

5.3.4.5 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.

5.3.4.6 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.

5.3.4.7 ANÁLISIS DE VULNERABILIDADES

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

5.3.4.8 SUPERVISIÓN

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

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

5.3.5 ARCHIVO DE REGISTROS

5.3.5.1 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.

5.3.5.2 PERIODO DE CONSERVACIÓN DE RESGISTROS

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.

5.3.5.3 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.

5.3.5.4 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.

5.3.5.5 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 CA un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

5.3.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

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

5.3.5.7 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.

5.3.6 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.

5.3.7 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.

5.3.7.1 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 ECDs 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.

5.3.7.2 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Thomas Signe S.A.S. ha desarrollado un Plan de contingencia para recuperar todos los sistemas, según el procedimiento 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.

5.3.8 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.

5.4 CONTROLES TÉCNICOS DE SEGURIDAD

5.4.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

5.4.1.1 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".

5.4.1.2 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 instakación 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.

5.4.1.3 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.

5.4.1.4 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.

5.4.1.5 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

5.4.1.6 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

5.4.1.7 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 firmade certificados y firma deCRLs.

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

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

5.4.2.1 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

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

El acceso a las claves privadas de la CA Raíz y 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 Subordinada.

5.4.2.3 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).

5.4.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Existen unos dispositivos que permiten la restauración de las claves 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 AC Raíz y AC Subordinada se pueden restaurar por un proceso que requiere la utilización de 2 de 3 dispositivos criptográficos (llaves).

5.4.2.5 ARCHIVO DE LA CLAVE PRIVADA

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

5.4.2.6 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.

5.4.2.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

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

5.4.2.8 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).

5.4.2.9 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.

5.4.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

5.4.3.1 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.

5.4.3.2 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.

5.4.4 DATOS DE ACTIVACIÓN

5.4.4.1 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 será 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).

5.4.4.2 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 CA Subordinadas.

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.

5.4.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

5.4.5 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.

5.4.5.1 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.

5.4.5.2 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.

5.4.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

5.4.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Thomas Signe S.A.S. y el grupo Signe posee el procedimiento GSIGNE-SI-PR-12 Seguridad en las operaciones, 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.

5.4.6.2 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 y un procedimiento para la gestión de este material para garantizar su uso.

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 un adecuado Pprocedimientos 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 técnico 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 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.

5.4.7 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.

5.4.8 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”.

6. FORMATOS

N/A

7. REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
N/A	N/A	N/A	N/A	N/A