Autoridad de Certificación

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

PS01

Política de Seguridad

Información del documento

Nombre	PS01 POLÍTICA DE SEGURIDAD
Realizado por	THOMAS SIGNE
País	CHILE
Versión	1.0
Tipo de documento	PÚBLICO
Código	THS-CL-AC-POL-02
Requisito	PS01

Historial de versiones

Versión	**Fecha**	**Descripción**
1.0	02/04/2019	Elaboración de documento inicial.

ÍNDICE

1 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de seguridad de la información que cumple Thomas Signe para la administración de sus servicios como Autoridad de Certificación, en el marco del cumplimiento de la Guía de Acreditación del Organismo de Acreditación competente.

2 ALCANCE

La presente política es de cumplimiento obligatorio por Thomas Signe y aplicable a todos los servicios de certificación brindados por Thomas Signe.

3 DEFINICIONES Y ABREVIACIONES

3.1 ACRÓNIMOS Y ABREVIACIONES

PSC Prestador de Servicios de Certificación

PKI Infraestructura de llave pública

AR Autoridad de Registro

CPS Declaración de Prácticas de Certificación

CP Política de Certificados

CRL Lista de Certificados Revocados

OCSP Online Certificate Status Protocol

DSCF Dispositivos Seguros de Creación de Firma

PKI Infraestructura de Llave Pública

3.2 DEFINICIONES

Autoridad de Registro: Persona jurídica, con excepción de los notarios públicos, o parte interna de los PSC 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.

Autoridad de Certificación – AC: 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 Prestador de Servicios de Certificación – PSC.

CA raíz: Autoridad certificadora de primer nivel, base de confianza.

CA subordinada: Autoridad certificadora de segundo nivel o más niveles.

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

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

4 CUMPLIMIENTO DEL REQUERIMIENTO NORMATIVO

La Política de Seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por Thomas Signe. Si Thomas Signe externaliza en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

La Política de Seguridad debe cumplir a lo menos con los siguientes requerimientos:

- Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que Thomas Signe sea un ente de confianza.
- Debe estar basada en las recomendaciones del estándar ISO 27002 sección 5.
- Los objetivos de la política son de alto nivel y no técnicos. Por lo tanto, debe ser lo suficientemente general para permitir alternativas de implementación tecnológica.
- Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas. Los elementos de la política de seguridad que estén incorporados tanto en la Declaración de Prácticas de Certificación (DPC) como la Política de los Certificados de firma electrónica avanzada (PC) deben estar incluidos en este documento.

Se recomienda que este documento identifique los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.

Adicionalmente, se recomienda que la documentación describa las reglas, directivas y procedimientos que indican cómo son provistos los servicios específicos y las medidas de seguridad asociadas.

4.1 REQUERIMIENTOS NORMATIVOS CUBIERTOS

Este documento y los documentos relacionados buscan cubrir los siguientes requerimientos normativos:

- Ley N°19.799, Artículo 14. Y 15.
- Reglamento, ART. 22 Y. 23, Reglamento Disposición Transitoria Primera, Segunda y Tercera.
- ISO/IEC 9594-8
- ITU-T X.690

4.2 DEPENDENCIAS

Este requisito no se encuentra asociado a otros contemplados en la guía de acreditación, pero sí a los siguientes documentos externos de Thomas Signe y el Grupo Signe:

- THS-CL-AC-DPC-01 PO02 Declaración de Prácticas de Certificación de Firma Electrónica Avanzada
- THS-CL-AC-POL-PER-01 PO01 Política de Certificación de Firma Electrónica Avanzada de Persona Natural
- THS-CL-AC-POL-COR-02 PO01 Política de Certificación de Firma Electrónica Avanzada de Pertenencia a Empresa

- THS-CL-AC-POL-COR-03 PO01 Política de Certificación de Firma Electrónica Avanzada de Persona Jurídica
- THS-CL-AC-PR-05 Procedimiento de gestión de claves
- THS-CL-AC-PR-00 Guion de Generación de Claves de subCA Thomas Signe Chile
- THS-CL-AC-PR-02 PO03 Modelo Operacional de la Autoridad Certificadora
- THS-CL-AC-PR-03 PO04 Modelo Operacional de la Autoridad de Registro AR
- THS-CL-AC-PR-04 AD01 Manual de Operaciones de la AC
- THS-CL-AC-PR-06 AD02 Manual de Operaciones de la AR
- THS-CL-PR-AC-10 Gestión de Acceso al Sistema de la CA
- THS-CL-PR-AC-11 Backup y Restauración del HSM
- THS-CL-AC-PR-12 TB03 Registro de Acceso Público
- GSIGNE-GRAL-MSG Manual de sistemas de gestión
- GSIGNE-PR-GRAL-08 Políticas Internas
- GSIGNE-PR-SI-05 Políticas de Seguridad de la Información

4.3 REQUERIMIENTOS SOPORTADOS

En la estructura presentada se soportan los requerimientos del numeral 4.4.2 de la Guía de Acreditación.

5 DECLARACIÓN DE POLÍTICA DE SEGURIDAD

THOMAS SIGNE opera como prestador de servicios de certificación (PSC) y la Autoridad de Certificación Subordinada "THOMAS SIGNE CHILE" emite certificados digitales a personas naturales personas jurídicas y personas vinculadas a empresas, conforme a lo establecido en la Ley N°19.799 sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma. THOMAS SIGNE forma parte de la Jerarquía de Certificación de THOMAS SIGNE ROOT, que está compuesta por una Autoridad de Certificación Raíz y varias Autoridades de Certificación Subordinadas entre las que se encuentra "THOMAS SIGNE CHILE Autoridad de Certificación", proporcionando los siguientes servicios:

- Registro del suscriptor
- Gestión del ciclo de vida de los certificados electrónicos (emisión, revocación, distribución – utilizando el repositorio online).
- Publicación del estado de los certificados mediante lista de certificados revocados (CRL) y Online Certificate Status Protocol (OCSP).
- Gestión del ciclo de vida de dispositivos seguros de creación de firma (DSCF) como tarjetas de circuito integrado criptográficas o tokens USB criptográficos.

Para llevar a cabo la prestación de los servicios de certificación, THOMAS SIGNE subcontrata la infraestructura tecnológica y recursos humanos a la Empresa del Grupo SIGNE, según permite la Ley N°19.799. No obstante, los servicios subcontratados se llevan a cabo según lo establecido en la Declaración de Prácticas y Políticas de Certificación de THOMAS SIGNE y en los acuerdos suscritos entre SIGNE y THOMAS SIGNE.

La Dirección de Thomas Signe es responsable de establecer y mantener los controles efectivos sobre las operaciones y procedimientos, incluyendo las Manifestaciones de sus prácticas de negocio como AC, la integridad del servicio (incluyendo controles para gestionar el ciclo de vida de las claves, los certificados y los dispositivos criptográficos, en este último caso, si procede) y los controles del entorno de las AC. Estos controles contienen mecanismos de monitorización y se toman acciones para corregir las deficiencias encontradas.

Existen limitaciones inherentes en algunos controles, incluyendo la posibilidad de errores humanos y la evasión o anulación de los controles. En las ocasiones en que un análisis de riesgos recomienda la inclusión de controles compensatorios para cubrir las mencionadas limitaciones inherentes, éstos se incluyen. Aun así, incluso los controles efectivos pueden proporcionar solamente una seguridad razonable en relación con las operaciones, procedimientos y entorno de Thomas Signe como PSC. Adicionalmente, debido a cambios en las condiciones, la efectividad de los controles puede variar cada cierto tiempo.

Por todo ello, THOMAS SIGNE en colaboración con SIGNE, y con pleno apoyo de la dirección, se compromete a lo siguiente:

- Hacer públicas sus Prácticas de Negocio sobre la gestión del ciclo de vida de las claves y los certificados, así como su política de privacidad de la información y proporciona sus servicios conforme a dichas afirmaciones.
- Mantiene controles efectivos para proporcionar una seguridad razonable de que:
    - La información del suscriptor es autenticada correctamente (para las actividades de registro realizadas por THOMAS SIGNE)
    - La integridad de claves y certificados gestionados se mantiene a lo largo de todo su ciclo de vida
    - La privacidad de las claves privadas se mantiene a lo largo de todo su ciclo de vida
    - El acceso a la información de suscriptores y usuarios está restringida a personal autorizado y la información está protegida de usos no especificados en las prácticas de negocio publicadas por THOMAS SIGNE
    - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados
    - Las tareas de explotación, desarrollo y mantenimiento de los sistemas de la AC son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos

Todo ello alineado con los estándares internacionalmente aceptados:

- ISO 27001 Information Technology – Security techniques – Information security management systems – Requirements.
- ISO 27002 Tecnología de la información – Técnicas de Seguridad – Código de Prácticas para los controles de seguridad de la información.
- WEBTRUST (SM/TM) FOR CERTIFICATION AUTHORITIES, Trust Service Principles and Criteria for Certification Authorities.

PRINCIPIO 1: DECLARACIÓN DE PRÁCTICAS DE NEGOCIO

Declaración de Prácticas y Políticas de Certificación para "THOMAS SIGNE" (www.thomas-signe.cl), incluyendo:

- Declaración de Prácticas de Certificación para Firma Electrónica Avanzada
- Política de Certificación de Firma Electrónica Avanzada de Persona Natural
- Política de Certificación de Firma Electrónica Avanzada de Pertenencia a Empresa
- Política de Certificación de Firma Electrónica Avanzada de Persona Jurídica

PRINCIPIO 2: INTEGRIDAD DEL SERVICIO

- Controles de la Gestión del Ciclo de Vida de las Claves
- Generación de las claves de la AC
- Almacenamiento, copias de seguridad y recuperación de las claves de la AC
- Distribución de la clave pública de la AC
- Uso de las claves de la AC y de los certificados de entidad final
- Destrucción de las claves de la AC
- Archivo de claves de AC
- Gestión del ciclo de vida de hardware criptográfico
- Servicio de Gestión de la provisión de la clave del suscriptor
- Controles de la Gestión del Ciclo de Vida de los certificados
- Registro de suscriptores
- Emisión de certificados
- Revocación de certificados
- Distribución de certificados
- Información sobre el estado de los certificados
- Gestión del ciclo de vida del DSCF

PRINCIPIO 3: CONTROLES AMBIENTALES DE LA AUTORIDAD DE CERTIFICACIÓN

- Restringir el acceso lógico y físico a los sistemas de CA y los datos dando solo acceso a las personas autorizadas
- Mantener la continuidad de las operaciones de gestión de claves y certificados
- Autorizar y ejecutar adecuadamente la operación, el mantenimiento y el desarrollo de los sistemas de la Autoridad de Certificación, con el fin de mantener su integridad.

6 FORMATOS APLICABLES

N/A

7 REGISTROS APLICABLES

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