


Autoridad de Certificación




THOMAS SIGNE
SOLUCIONES TECNOLÓGICAS GLOBALES

P002

**Declaración de Prácticas de Certificación
para Firma Electrónica Avanzada**

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 2 de 62



	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 3 de 62

Información del documento

Nombre	PO02 DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA FIRMA ELECTRÓNICA AVANZADA
Realizado por	THOMAS SIGNE
País	CHILE
Versión	1.2
Tipo de documento	PÚBLICO
Código	THS-CL-AC-DPC-01
Requisito	PO02



Historial de versiones

Versión	Fecha	Descripción
1.0	02/02/2019	Elaboración de documento inicial.
1.1	15/09/2019	Incluir CPD de Telefónica Tier IV Gold
1.2	21/04/2020	Se agrega emisión y custodia de certificados en HSM Centralizado. Se agrega la utilización de Clave Única


	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 4 de 62

ÍNDICE



1	INTRODUCCIÓN	11
2	OBJETIVO	11
3	DEFINICIONES Y ABREVIACIONES	11
3.1	ACRÓNIMOS Y ABREVIACIONES	11
3.2	DEFINICIONES Y CONCEPTOS	11
4	JERARQUÍA Y PARTICIPANTES DEL SISTEMA DE CERTIFICACIÓN DIGITAL	13
4.1	JERARQUÍA PKI DE THOMAS SIGNE	13
4.2	PARTICIPANTES PKI DE THOMAS SIGNE	14
4.2.1	PRESTADOR DE SERVICIO DE CERTIFICACIÓN THOMAS SIGNE (PSC THOMAS SIGNE)	14
4.2.2	TITULAR	14
4.2.3	SOLICITANTE	14
4.2.4	TERCERO QUE CONFÍA	14
5	DOCUMENTOS NORMATIVOS DEL PSC	14
5.1	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	14
5.2	POLÍTICAS Y PROCEDIMIENTOS	15
6	RESPONSABILIDADES	15
6.1	THOMAS SIGNE	15
6.2	TITULAR	15
7	TIPOS DE CERTIFICADO	16
7.1	CERTIFICADOS PERSONALES	16
	or! Marcador no definido.	iErr
7.2	CERTIFICADOS CORPORATIVOS	17
8	USO DEL CERTIFICADO	18
8.1	USO PERMITIDO DEL CERTIFICADO	18
8.2	USOS NO AUTORIZADOS DE LOS CERTIFICADOS	18
9	IDENTIFICACIÓN DEL PSC	18
10	ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS	19
11	RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	19
11.1	PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN	19
11.2	PLAZO O FRECUENCIA DE LA PUBLICACIÓN	19
11.3	CONTROLES DE ACCESO A LOS REPOSITORIOS	20
12	IDENTIFICACIÓN Y AUTENTICACIÓN	20

	P002 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 5 de 62


12.1	NOMBRES	20
12.1.1	TIPOS DE NOMBRES	20
12.1.2	NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO	20
12.1.3	ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES	20
12.1.4	UNICIDAD DE LOS NOMBRES	21
12.1.5	RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS	21
13	VALIDACIÓN INICIAL DE LA IDENTIDAD	21
13.1	MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA	21
13.2	AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA JURÍDICA	21
13.3	AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL	21
	or! Marcador no definido.	iErr
13.4	INFORMACIÓN DE TITULAR NO VERIFICADA	22
14	IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REEMISIÓN DE CLAVES	22
14.1	IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REEMISIÓN	22
15	IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN	22
15.1	IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN	22
16	REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS	22
16.1	QUIÉN PUEDE SOLICITAR UN CERTIFICADO	23
16.2	COMERCIALIZACIÓN	23
16.3	VERIFICAR IDENTIDAD DEL SOLICITANTE	23
16.3.1	Personación	24
16.3.2	Clave Única	24
16.4	CONTRATACIÓN Y PAGO	24
16.5	SOLICITUD DEL CERTIFICADO	24
17	TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS	24
17.1	REVISIÓN	24
17.1.1	APROBACIÓN DE LA SOLICITUD	25
17.1.2	DENEGACIÓN DE LA SOLICITUD	25
17.1.3	PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO	25
18	EMISIÓN DE CERTIFICADOS	25
18.1	ACTUACIONES DE LA AC DURANTE LA EMISIÓN DE CERTIFICADOS	25
18.2	NOTIFICACIÓN AL TITULAR POR LA AC DE LA EMISIÓN DEL CERTIFICADO	25
19	ACEPTACIÓN DEL CERTIFICADO	25
19.1	FORMA EN LA QUE SE ACEPTA EL CERTIFICADO	25

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 6 de 62


19.1.1	Para el caso de token o tarjeta inteligente:	25
19.1.2	Para el caso de HSM centralizado	26
19.2	PUBLICACIÓN DEL CERTIFICADO POR EL PSC	26
19.3	NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES	26
20	USOS DE LAS CLAVES Y EL CERTIFICADO	26
20.1	USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR	26
20.2	USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN	26
21	RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES	26
22	RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES	26
23	MODIFICACIÓN DE CERTIFICADOS	27
24	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS	27
24.1	CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO	27
24.2	QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN	28
24.3	PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN	28
24.4	PLAZO EN EL QUE EL PSC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN	28
24.5	OBLIGACIÓN DE VERIFICACIÓN DE LAS REVOCAACIONES POR LOS TERCEROS QUE CONFÍAN	28
24.6	FRECUENCIA DE EMISIÓN DE LAS CRLS	29
24.7	TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS	29
24.8	DISPONIBILIDAD DEL SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS	29
24.9	REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA	29
25	SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS	29
25.1	CARACTERÍSTICAS OPERACIONALES	29
25.2	DISPONIBILIDAD DEL SERVICIO	29
25.3	FINALIZACIÓN DE LA SUSCRIPCIÓN	30
26	CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES	30
26.1	CONTROLES FÍSICOS	30
26.1.1	UBICACIÓN FÍSICA Y CONSTRUCCIÓN	30
26.1.2	ACCESO FÍSICO	31
26.1.3	EXPOSICIÓN AL AGUA	31
26.1.4	ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO	31
26.1.5	PREVENCIÓN Y PROTECCIÓN DE INCENDIOS	31
26.1.6	SISTEMA DE ALMACENAMIENTO	31

	P002 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 7 de 62


26.1.7	ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN	31
26.1.8	BACKUP FUERA DE LA INSTALACIÓN	32
26.2	CONTROLES DE PROCEDIMIENTO	32
26.2.1	ROLES DE CONFIANZA	32
26.2.2	NÚMERO DE PERSONAS REQUERIDAS POR TAREA	32
26.2.3	IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL	33
26.2.4	ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES	33
26.3	CONTROLES DE PERSONAL	33
26.3.1	REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES	33
26.3.2	PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES	33
26.3.3	REQUISITOS DE FORMACIÓN	33
26.3.4	REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN	33
26.3.5	SANCIONES POR ACTUACIONES NO AUTORIZADAS	34
26.3.6	REQUISITOS DE CONTRATACIÓN DE TERCEROS	34
26.3.7	DOCUMENTACIÓN PROPORCIONADA AL PERSONAL	34
26.4	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	34
26.4.1	TIPOS DE EVENTOS REGISTRADOS	34
26.4.2	FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)	35
26.4.3	PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA	35
26.4.4	PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA	35
26.4.5	PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA	35
26.4.6	SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)	35
26.4.7	ANÁLISIS DE VULNERABILIDADES	36
26.5	ARCHIVO DE REGISTROS	36
26.5.1	TIPOS DE EVENTOS ARCHIVADOS	36
26.5.2	PERIODO DE CONSERVACIÓN	36
26.5.3	PROTECCIÓN DE ARCHIVOS	36
26.5.4	PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS	37
26.5.5	REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS	37
26.5.6	SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)	37
26.5.7	PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA	37
26.6	PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES	37

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 8 de 62


26.6.1	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE	38
26.6.2	CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	38
26.7	CESE DE UN PSC	38
27	CONTROLES TÉCNICOS DE SEGURIDAD	39
27.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	39
27.1.1	GENERACIÓN DEL PAR DE CLAVES	39
27.1.2	ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES	39
27.1.3	ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	39
27.1.4	ENTREGA DE LA CLAVE PÚBLICA DEL PSC A TERCEROS ACEPTANTES	39
27.1.5	TAMAÑO DE LAS CLAVES	40
27.1.6	PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD	40
27.1.7	USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)	40
27.2	PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	41
27.2.1	CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS	41
27.2.2	CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA	41
27.2.3	CUSTODIA DE LA CLAVE PRIVADA	41
27.2.4	BACKUP DE LA CLAVE PRIVADA	41
27.2.5	ARCHIVO DE LA CLAVE PRIVADA	42
27.2.6	ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO	42
27.2.7	MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA	42
27.2.8	MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA	42
27.2.9	MÉTODO PARA DESTRUIR LA CLAVE PRIVADA	42
27.3	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES	42
27.3.1	ARCHIVO DE LA CLAVE PÚBLICA	42
27.3.2	PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES	42
27.4	DATOS DE ACTIVACIÓN	43
27.4.1	GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	43
27.4.2	PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN	43
27.4.3	OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN	43
27.5	CONTROLES DE SEGURIDAD INFORMÁTICA	43
27.5.1	REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS	43

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 9 de 62

27.5.2	EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA	44
27.6	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	44
27.6.1	CONTROLES DE DESARROLLO DE SISTEMAS	44
27.6.2	CONTROLES DE GESTIÓN DE SEGURIDAD	44
27.7	CONTROLES DE SEGURIDAD DE LA RED	46
28	PERFILES DE CERTIFICADOS, CRL Y OCSP	46
28.1	PERFIL DE CERTIFICADO	46
28.1.1	NÚMERO DE VERSIÓN	47
28.1.2	PERFILES	47
28.1.3	EXTENSIONES DEL CERTIFICADO	50
28.1.4	IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS	52
28.1.5	FORMATOS DE NOMBRES	52
28.1.6	RESTRICCIONES DE LOS NOMBRES	52
28.1.7	IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN	52
28.1.8	SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS	52
28.1.9	TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY	53
28.2	PERFIL DE CRL	53
28.2.1	NÚMERO DE VERSIÓN	53
28.2.2	CRL Y EXTENSIONES	53
28.3	PERFIL OCSP	54
29	AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES	54
29.1	FRECUENCIA DE LAS AUDITORÍAS	55
29.2	IDENTIDAD/CUALIFICACIÓN DEL AUDITOR	55
29.3	RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA	55
29.4	ASPECTOS CUBIERTOS POR LOS CONTROLES	55
29.5	ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS	56
29.6	COMUNICACIÓN DE RESULTADOS	56
30	OTROS ASUNTOS LEGALES Y COMERCIALES	56
30.1	TARIFAS	56
30.1.1	TARIFAS DE EMISIÓN DE CERTIFICADOS	56
30.1.2	TARIFAS DE ACCESO A LOS CERTIFICADOS	56
30.1.3	TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO	56
30.1.4	TARIFAS DE OTROS SERVICIOS	56
30.2	RESPONSABILIDADES ECONÓMICAS	56

	P002 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 10 de 62

30.3	EXONERACIÓN DE RESPONSABILIDAD	57
30.4	RESPONSABILIDADES FINANCIERAS	58
30.4.1	COBERTURA DEL SEGURO	58
30.4.2	SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES	58
30.5	DERECHOS DE PROPIEDAD INTELECTUAL	58
30.6	OBLIGACIONES	58
30.6.1	OBLIGACIONES DEL PSC	58
30.6.2	OBLIGACIONES DE LA AR	59
30.6.3	OBLIGACIONES DE LOS PROVEEDORES	60
30.6.4	OBLIGACIONES DE LOS SOLICITANTES	60
30.6.5	OBLIGACIONES DE LOS FIRMANTES	60
30.6.6	OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN	61
31	POLÍTICA DE PROTECCIÓN DE DATOS	61
32	CONFIDENCIALIDAD DE LA INFORMACIÓN	61
32.1	INFORMACIÓN CONFIDENCIAL	61
32.2	INFORMACIÓN NO CONFIDENCIAL	62
33	CONFORMIDAD CON LA LEY APLICABLE	62
34	BIBLIOGRAFÍA	62

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 11 de 62

1 INTRODUCCIÓN

Thomas Signe es una empresa multinacional dedicada a desarrollar soluciones tecnológicas a la medida para garantizar el éxito de empresas tanto públicas como privadas; a través de una estrategia de creación de valor sustentada sobre una oferta de gestión global de las necesidades del cliente, desde la consultoría, pasando por el desarrollo de proyectos, la integración e implementación de soluciones.

Thomas Signe fue constituida en Chile en el año 2018 con el objetivo de convertirse en proveedor de servicios de firma electrónica, siendo acreditado y sometido anualmente a las auditorías realizadas por el Ministerio de Economía. Para lo cual, Thomas Signe ha demostrado cumplir con todos los estándares operacionales, de seguridad, privacidad y calidad exigidos en los servicios de certificación brindados a sus clientes.

Como Proveedor de Servicios de Certificación - PSC, Thomas Signe provee servicios de emisión, distribución y revocación de certificados digitales. Además, brinda los servicios de registro o verificación de sus clientes.

2 OBJETIVO

Este documento tiene como objetivo declarar las operaciones y prácticas que utiliza Thomas Signe para la administración de sus servicios como emisor de certificados digitales en el marco del cumplimiento de la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” – EA-103, establecida por la Entidad Acreditadora.


3 DEFINICIONES Y ABREVIACIONES

3.1 ACRÓNIMOS Y ABREVIACIONES

- AC** Autoridad de Certificación
- PC** Políticas de los certificados
- CRL** Lista de Certificados Revocados
- DSCF** Dispositivos Seguros de Creación de Firma
- DPC** Declaración de prácticas de certificación
- PSC** Prestador de Servicios de Certificación
- HSM** Hardware Security Module
- OCSP** Servicio del estado del certificado en línea
- PKI** Infraestructura de clave pública
- AR** Autoridad de Registro
- SHA** Secure Hash Algorithm (Algoritmo de seguridad HASH)

3.2 DEFINICIONES Y CONCEPTOS

Autoridad de Certificación – AC: persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 12 de 62

Autoridad de Registro: persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

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

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

Clave Única: es un mecanismo de identificación digital que permite a los usuarios demostrar su identidad en plataformas digitales, ya que el Servicio de Registro Civil e Identificación verifica que la identidad digital corresponde a determinada persona, validándola contra su base de datos.

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.

HSM: un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. La seguridad que proporcionan los dispositivos HSM de Thomas-Signe está garantizada por estrictas políticas, procedimientos de operación y todas las medidas de seguridad que brinda el CPD Tier IV Gold en el cual se encuentra.

Certificado digital: mensaje de datos electrónico firmado por la Autoridad de Certificación, el cual identifica tanto a la Autoridad de Certificación que lo expide, como al titular 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 AC establece una relación comercial.

Declaración de Prácticas de Certificación: es el documento en el que constan los procedimientos que aplica el PSC para la prestación de sus servicios. Una declaración de las prácticas que se emplean para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

Prestador de Servicios de Certificación: entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada (Ley N°19.799 artículo 1°, letra c).


Autoridad de Registro: persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

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 Revocados: es aquella relación que debe incluir todos los certificados revocados por la Autoridad de Certificación.

PKI: infraestructura de clave pública (Public key infrastructure): 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 titular 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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 13 de 62

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

Políticas de Certificado: 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.

Segundo Factor Autenticación: la autenticación con dos factores es un método para confirmar que un titular de un certificado es quien dice ser; consiste en combinar dos elementos diferentes que son de conocimiento o propiedad del titular, uno algo que él sabe (ejemplo, una contraseña) y dos algo que él tiene (ejemplo, un teléfono, dispositivo de generación de códigos entre otros). Un ejemplo de un segundo factor lo vemos al realizar una transferencia bancaria, donde se utiliza una tarjeta de coordenadas, un generador de números o se recibe un SMS, en todos estos casos, se tiene un conjunto de caracteres que se debe introducir para confirmar la transacción.

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

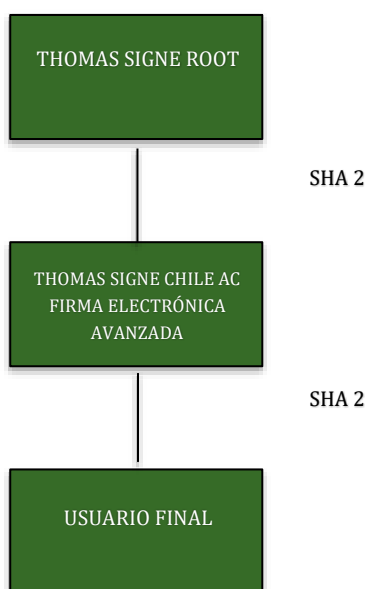
Solicitante: persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una AC, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de estas, para acceder al servicio de certificación digital.



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

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

4 JERARQUÍA Y PARTICIPANTES DEL SISTEMA DE CERTIFICACIÓN DIGITAL

4.1 JERARQUÍA PKI DE THOMAS SIGNE



	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 14 de 62

4.2 PARTICIPANTES PKI DE THOMAS SIGNE

4.2.1 PRESTADOR DE SERVICIO DE CERTIFICACIÓN THOMAS SIGNE (PSC THOMAS SIGNE)

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

A Thomas Signe, como Prestador de Servicios de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la Entidad Acreditadora a fin de lograr y mantener la acreditación.

Asimismo, Thomas Signe brinda 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.

4.2.2 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable de este confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en esta DPC.

Asimismo, el titular es el responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

4.2.3 SOLICITANTE

Se entenderá por Solicitante, la persona que solicita un certificado emitido bajo esta DPC.

4.2.4 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por Thomas Signe a un titular. El Tercero que confía, a su vez puede ser o no titular.



5 DOCUMENTOS NORMATIVOS DEL PSC

Los Documentos Normativos son todas aquellas declaraciones, políticas y procedimientos que regulan los servicios de certificación digital de Thomas Signe.

Todos los Documentos Normativos son aprobados por Thomas Signe antes de ser publicados y se controlan las versiones de estos, a fin de evitar modificaciones y suplantaciones no autorizadas.

5.1 DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

La presente DPC establece todas las operaciones y prácticas que lleva a cabo Thomas Signe para brindar los servicios de emisión, revocación y distribución de los certificados digitales; siguiendo el estándar RFC

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 15 de 62

3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, conforme a la normativa chilena y las disposiciones de los entes reguladores.

Esta DPC es de carácter público y se encuentra dirigida a todas las personas naturales y jurídicas, solicitantes, titulares, terceros que confían y público en general. La misma podrá ser consultada a través de la página web www.thomas-signe.cl

Todas las modificaciones relevantes en la presente DPC serán comunicadas a la Entidad Acreditadora y las nuevas versiones del documento serán publicadas en el mismo sitio web.

5.2 POLÍTICAS Y PROCEDIMIENTOS

Todas las Políticas y Procedimientos aplicables al proceso de certificación digital, tales como las Políticas de Certificados, Política de Privacidad, entre otros; son de carácter público y son de libre acceso mediante la página web de Thomas Signe www.thomas-signe.cl


6 RESPONSABILIDADES

6.1 THOMAS SIGNE

- Cumplir con lo dispuesto en la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” – EA-103 en su versión vigente, establecida por la Entidad Acreditadora.
- Garantizar que los certificados cumplen con todos los requisitos materiales establecidos de la DPC y que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por Thomas Signe.
- Facilitar los documentos necesarios y en su última versión al titular.
- Informar a los titulares las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar.
- Notificar al titular acerca de los cambios en las políticas y prácticas de Thomas Signe.
- Notificar al titular cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de titular, 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 de la Entidad Acreditadora).
- Atender y dar respuesta a las quejas y reclamos de los titulares y partes relacionadas.
- Responsabilizarse por los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. Teniendo como excepción de los daños que tengan origen en el uso indebido o fraudulento de un certificado de firma electrónica.
- Mantener un seguro, que cubra eventual responsabilidad civil, por un monto equivalente o superior al exigido por la Entidad Acreditadora, tanto por los certificados propios como aquellos homologados.

6.2 TITULAR


- Actuar conforme a lo estipulado en la presente DPC de Thomas Signe.
- Facilitar información completa, actual y veraz a Thomas Signe.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 16 de 62

- Emplear adecuadamente el certificado respecto a su aplicación, limitaciones y prohibiciones de uso; conforme a lo establecido en la DPC de Thomas Signe.
- Cumplir con los requisitos estipulados por Thomas Signe para el respectivo servicio de certificación digital.
- Cumplir con nuevos requisitos, cuando Thomas Signe implemente cambios en los servicios de certificación digital, previa comunicación de dichos cambios por parte del PSC al titular.
- No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para Thomas Signe, ni hacer declaraciones relacionadas con su certificación, que Thomas Signe 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 de la Subsecretaría de Economía y Empresas de Menor Tamaño y de Thomas Signe, así como comprometer intencionadamente la seguridad de la Jerarquía de la Subsecretaría de Economía y Empresas de Menor Tamaño y de Thomas Signe.
- Informar a Thomas Signe sin retraso, acerca de los cambios que puedan afectar el servicio de certificación digital que le fue expedido por Thomas Signe.
- 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 el caso de emisión de certificado en token o tarjeta inteligente, en todo momento el titular será 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.
- En el caso de emisión de certificado en HSM centralizado, en todo momento el titular será responsable de proteger las contraseñas que le permiten el acceso a su clave privada custodiada en el HSM centralizado, sin poder transferir esta responsabilidad a ningún tercero.
- Cumplir 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.
- Solicitar la revocación del certificado digital en caso de: pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada de modo centralizado; 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.
- Solicitar la revocación del certificado en caso de compromiso de las contraseñas que le permiten hacer uso de su certificado.
- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado
- Solicitar la revocación del certificado cuando se incumple las obligaciones a las que se encuentra comprometido dentro de los requerimientos de la Subsecretaría de Economía y Empresas de Menor Tamaño.

7 TIPOS DE CERTIFICADO

Thomas Signe emite certificados de Firma electrónica avanzada, tanto para personas naturales como jurídicas. Estos certificados hacen uso de un dispositivo de creación de firma seguro como un token, una tarjeta o un HSM Centralizado, los cuales cuentan con certificación FIPS 140-2 nivel 3, dando lugar a un nivel de aseguramiento alto. En caso de Emisión de Certificados en HSM Centralizado, el titular delega explícitamente la custodia de su certificado y clave privada en un HSM de Thomas-Signe, el cual cuenta con todas las medidas de seguridad físicas y lógicas para garantizar que solo el titular podrá hacer uso del mismo. Para hacer uso de su certificado, el titular accede de forma segura, mediante la clave que el creó durante la emisión del certificado y un segundo factor de autenticación de identidad que cumple con las pautas de identidad digital NIST-SP-800-63

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 17 de 62

7.1 CERTIFICADOS PERSONALES

Certificado de Firma Electrónica Avanzada: son certificados que permiten identificar y firmar al Titular como una Persona Natural sin vinculación a alguna corporación.

OID DE POLÍTICA DE CERTIFICADO PERSONAL	
1.3.6.1.4.1.51362.0.4.1.1.1	Política de Certificado de Firma Electrónica Avanzada de Persona Natural


7.2 CERTIFICADOS CORPORATIVOS

Los Certificados Corporativos son certificados de firma digital cuyo Titular es una Persona Natural vinculada a una Corporación (ya sea una empresa, una organización pública o privada, o colegio profesional) o la propia Corporación (Persona Jurídica):

Certificado de Pertenencia a Empresa: Son certificados que identifican al Suscriptor como Persona Natural vinculada a una Corporación.

Certificados de Persona Jurídica: Son certificados que se emiten a una persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente. Las personas jurídicas son de dos especies: corporaciones y fundaciones de beneficencia pública. Las corporaciones de derecho privado se llaman también asociaciones.

OID DE POLÍTICA DE CERTIFICADO CORPORATIVO	
1.3.6.1.4.1.51362.0.4.1.2.1	Política de Certificado de Firma Electrónica Avanzada de Pertenencia a Empresa
1.3.6.1.4.1.51362.0.4.1.3.1	Política de Certificado de Firma Electrónica Avanzada de Persona Jurídica

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 18 de 62

8 USO DEL CERTIFICADO

8.1 USO PERMITIDO DEL CERTIFICADO

Thomas Signe cuenta con una PC para cada tipo de certificado. Las PCs se encuentran publicadas en la página web de Thomas Signe, tal como se indica en la sección *Documentos normativos del PSC*, del presente documento. Principalmente, el certificado digital deberá permitir a su titular identificar, en forma directa o mediante consulta electrónica, además de comprobar la validez de este.

8.2 USOS NO AUTORIZADOS DE LOS CERTIFICADOS

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

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 la muerte, lesiones personales o daños medioambientales severos.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

Thomas Signe 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 Titular. El Titular que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, Thomas Signe tenga responsabilidad alguna por pérdida de información derivada de la pérdida de las claves de cifrado. Por ello, Thomas Signe no recomienda el uso de los certificados digitales para el cifrado de la información.

9 IDENTIFICACIÓN DEL PSC

Datos de la Autoridad de Certificación:

Razón Social: THOMAS SIGNE CHILE SA

R.U.T.: 76934091-2

Domicilio social: Avenida Presidente Kennedy 5600, Oficina 806, Comuna Vitacura

Ciudad: Santiago, Chile

Teléfono: +56 2 32597822


Correo electrónico: psc-cl@thsigne.com

Página Web: www.thomas-signe.cl

Datos del Proveedor de servicios tecnológicos

Razón Social: SIGNE, S.A.

C.I.F.: A11029279

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 19 de 62

Dirección: Avda. de la Industria, 18 Tres Cantos 28760

Domicilio: Madrid, España

Teléfono: +34 902 30 17 01

Correo electrónico: signe-ac@signe.com

Página Web: www.signe.es

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS

Thomas Signe administra los documentos de Declaración de Prácticas, y todos los documentos normativos de Thomas Signe.

Para cualquier consulta relativa a estos documentos, contactar:

- Oficina: Atención al cliente
- Dirección de correo electrónico: soporte-cl@thsigne.com

11 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

11.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Gestor Documental se encarga de autorizar la publicación de la DPC y demás documentos normativos y es responsable de asegurar la integridad y disponibilidad de la información publicada en:

www.thomas-signe.cl

Asimismo, siguiendo el modelo de confianza, en la página web de Thomas Signe existe un mecanismo de validación donde los titulares podrán cargar su certificado digital y verificar si este es auténtico respecto de la jerarquía de Thomas Signe.

Por otro lado, Thomas Signe entrega a la Entidad Acreditadora el formato ETSI TS 102 231 de la TSL, para la respectiva publicación del certificado de la raíz y subordinada de Thomas Signe Chile.

11.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN



Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de Thomas Signe durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado de la AC Subordinada

El certificado de la AC Subordinada se publicará y permanecerá en la página Web de Thomas Signe durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 20 de 62

Thomas Signe publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en la sección *Frecuencia de emisión de las CRLs*.

Declaración de Prácticas de Certificación (DPC)

Con autorización de Thomas Signe y de la Subsecretaría de Economía y Empresas de Menor Tamaño, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados a la Subsecretaría de Economía y Empresas de Menor Tamaño y publicados en la página Web de Thomas Signe junto con la nueva versión. La siguiente auditoría validará estos cambios y emitirá el informe de cumplimiento.

11.3 CONTROLES DE ACCESO A LOS REPOSITARIOS

La consulta a los repositorios disponibles antes mencionados es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de Thomas Signe que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a Thomas Signe.

12 IDENTIFICACIÓN Y AUTENTICACIÓN

12.1 NOMBRES

12.1.1 TIPOS DE NOMBRES

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500. Adicionalmente, todos los nombres de los certificados son coherentes con lo dispuesto en la norma RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".



12.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los campos del DN referentes al Nombre y Apellidos corresponderán con los datos registrados legalmente del Titular, expresados exactamente en el formato que conste en el Cédula Nacional de Identidad.

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

12.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

No aplica.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 21 de 62

12.1.4 UNICIDAD DE LOS NOMBRES

El nombre distinguido (DN) de los certificados emitidos será único para cada Titular. El atributo de Documento de Identidad se usa para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

12.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

Thomas Signe, no asume compromisos en la emisión de certificados respecto al uso por los Titulares de una marca comercial. Asimismo, no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Titular. Sin embargo, Thomas Signe, no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

13 VALIDACIÓN INICIAL DE LA IDENTIDAD

13.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

El método de prueba de la posesión de la clave privada por el Titular será la entrega de PKCS#10 o una prueba criptográfica equivalente u otro método aprobado por Thomas Signe. Cuando el certificado se emite en HSM Centralizado, la clave privada se genera en el HSM en el instante previo a la emisión del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con el Solicitante.

13.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA JURÍDICA

La AR verificará la identidad de la Persona Jurídica mediante la solicitud de las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar la constitución de la entidad, su vigencia e identificación de los miembros que las integran.

La AR verificará la validez y vigencia respecto a los documentos y al resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar evidencia relativa al sustento de la validación de la identidad del Titular



Thomas Signe S.A. se reserva el derecho de no emitir el certificado si considera que la evidencia aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

13.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL

La AR verificará de forma fehaciente la identidad de la persona natural identificada en el certificado de acuerdo con la Política de Certificación correspondiente.

La AR verificará la validez y vigencia respecto a los documentos y al resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar evidencia relativa al sustento de la validación de la identidad del Titular.

Thomas Signe S.A. se reserva el derecho de no emitir el certificado si considera que la evidencia aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 22 de 62

13.4 INFORMACIÓN DE TITULAR NO VERIFICADA

En ninguna circunstancia Thomas Signe omitirá las labores de verificación que conduzcan a la identificación del Titular y que se traduce en la solicitud de exhibición de los documentos mencionados en las formas que lo permite regulación actual, para personas naturales y jurídicas.

14 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REEMISIÓN DE CLAVES

Thomas Signe no atiende peticiones de reemisión de certificados.

14.1 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REEMISIÓN

Thomas Signe no atiende peticiones de reemisión de certificados.

15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN


Thomas Signe atiende peticiones de revocación de conformidad con las causales de revocación especificadas en la sección *Circunstancias para la revocación de un certificado* en esta DPC y autentica la identidad de quien solicita la revocación del certificado.

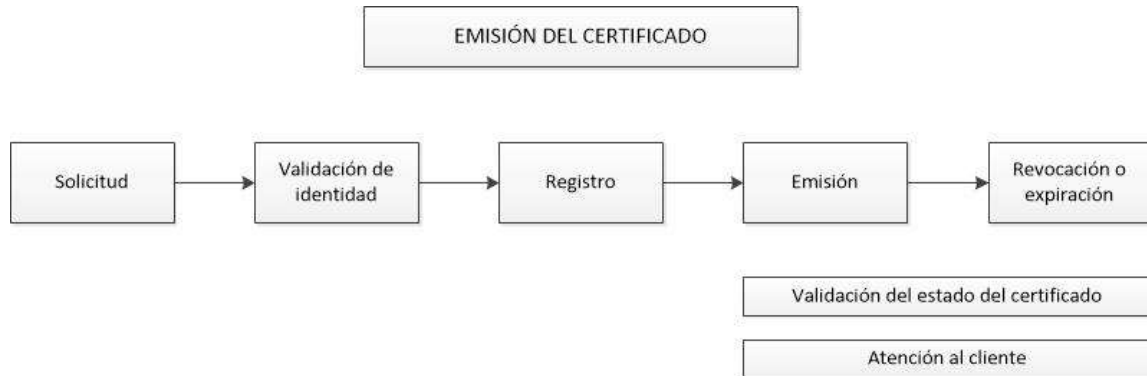
15.1 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN

Thomas Signe autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

16 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 23 de 62



16.1 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Están autorizados para solicitar la emisión de un certificado:

- **De Persona Natural:** una persona natural; que sustente correctamente la información requerida por Thomas Signe, de acuerdo con la sección, Información requerida por la AR de la Política de certificación de Firma Electrónica Avanzada.
- **De Pertenencia a Empresa:** una persona natural vinculada a Empresa o Entidad; que pueda sustentar correctamente toda la información requerida por Thomas Signe S.A., de acuerdo con la sección, Información requerida por la AR de la Política de certificación de Firma Electrónica Avanzada.
- **De Persona Jurídica:** una persona jurídica representada por una persona natural que; pueda sustentar correctamente toda la información requerida por Thomas Signe S.A., de acuerdo con la sección, Información requerida por la AR de la Política de certificación de Firma Electrónica Avanzada

16.2 COMERCIALIZACIÓN



El Solicitante podrá recibir información acerca del proceso de certificación digital de las siguientes maneras:

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

Por cualquiera de estos medios, se le brindará información acerca de dicho proceso, requisitos, tarifas u otros relativos. Asimismo, se le facilitará un Formulario para que el Solicitante complete sus datos.

16.3 VERIFICAR IDENTIDAD DEL SOLICITANTE

La validación de la identidad del solicitante podrá hacerse por cualquiera de los medios siguientes:

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 24 de 62

16.3.1 PERSONACIÓN

Si el Solicitante, se encuentra interesado en contratar los servicios de Thomas Signe, se coordinará una cita presencial. Una vez concretada la cita, Thomas Signe visitará o será visitado por el Solicitante para realizar la validación de la identidad, llevando a cabo las siguientes actividades:

- Validar presencialmente la identidad del Solicitante
- Tomar la firma y huella digital del Solicitante en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.
- Tomar una fotografía del Solicitante
- Ingresar las evidencias digitales al sistema SAR, para efectos de custodia y prueba de los actos de validación realizados.

Dicha validación podrá ser realizada por un Notario según formato de validación. Cabe destacar que, en este caso, todas estas evidencias serán recolectadas y custodiadas por Thomas Signe.

16.3.2 CLAVE ÚNICA

La validación de la identidad del solicitante se realiza totalmente en línea, en completa adhesión a los lineamientos establecidos por el sistema de Clave Única sumando el cumplimiento de la normativa establecida por el decreto 24 Norma Técnica de Seguridad, Santiago, 22 de febrero de 2019. Se utiliza además un segundo factor de autenticación como lo exige la norma técnica referida, este segundo factor está definido y acorde al estándar NIST-SP-800-63. Este segundo factor, se encuentra en evaluación periódica por parte de Thomas-Signe, para garantizar siempre su seguridad y que solo el Titular tiene acceso al certificado.

16.4 CONTRATACIÓN Y PAGO

Para proceder, el Solicitante deberá realizar el pago de la tarifa respectiva por un método válido y aprobar todos los términos y condiciones dispuestos en el Contrato de Prestación de Servicios de Firma Electrónica, tal como se describe en el apartado anterior.


16.5 SOLICITUD DEL CERTIFICADO

Para solicitar la emisión propiamente dicha de un certificado digital, Thomas Signe completará los datos del Solicitante dentro de la plataforma de registro. Además, procederá a adjuntar los documentos solicitados indicados en el apartado 16.2.1 y 16.3

17 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

17.1 REVISIÓN

Thomas Signe verificará que toda la documentación presentada se encuentre completa y validará los documentos presentados se encuentren vigentes.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 25 de 62

17.1.1 APROBACIÓN DE LA SOLICITUD

Una vez verificada satisfactoriamente la identidad del Solicitante, Thomas Signe aprobará la solicitud de emisión en la plataforma de registro.

17.1.2 DENEGACIÓN DE LA SOLICITUD

Por otro lado, si se encuentran inconsistencias o irregularidades en los documentos presentados, Thomas Signe se lo comunicará al Solicitante, a fin de presentar la documentación regularizada o actualizada.

17.1.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

El plazo para la aprobación de una solicitud por parte de la AR de Thomas Signe tiene un plazo máximo de tres (3) días hábiles desde el momento de recibir la constancia del pago de tarifa, la documentación e información completa. El tiempo de entrega del certificado digital una vez recibida la solicitud completa tiene un plazo máximo de cinco (5) días hábiles.

Clave Única: al tratarse de un proceso en línea, este tendrá la duración de la sesión, la cual tiene un tiempo de duración finito como medida de seguridad.

18 EMISIÓN DE CERTIFICADOS

18.1 ACTUACIONES DE LA AC 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 Titular. En la emisión del certificado digital, Thomas Signe:

- 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.
- Se envía la documentación de la certificación digital.

18.2 NOTIFICACIÓN AL TITULAR POR LA AC DE LA EMISIÓN DEL CERTIFICADO


Thomas Signe notificará al Titular la emisión del certificado.

19 ACEPTACIÓN DEL CERTIFICADO

19.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

19.1.1 PARA EL CASO DE TOKEN O TARJETA INTELIGENTE:

El certificado se considerará válido a partir de la fecha en que el Titular descargue su certificado digital.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 26 de 62

19.1.2 PARA EL CASO DE HSM CENTRALIZADO

El propio HSM Centralizado notifica al Solicitante que el certificado ha sido emitido e instalado en el HSM. Además, la RA envía un correo electrónico al Solicitante que incluye información sobre el contenido del certificado.

19.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

Una vez el certificado generado y aceptado por el Titular, el certificado podrá ser publicado en los repositorios de certificados que se consideren necesarios.

19.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES

Thomas Signe no notifica la emisión de certificados a terceros.

20 USOS DE LAS CLAVES Y EL CERTIFICADO

20.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

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

La extensión Key Usage podrá ser utilizada 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.

20.2 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.


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

21 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

Thomas Signe no atiende requerimientos de renovación de certificados digitales sin cambio de claves.

22 RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Thomas Signe no atiende requerimientos de renovación de certificados digitales con cambio de claves.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 27 de 62

23 MODIFICACIÓN DE CERTIFICADOS

Los certificados digitales emitidos por Thomas Signe no pueden ser modificados. La modificación de certificados se trata como una nueva emisión de certificado.

24 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

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

La revocación de un certificado en las circunstancias que se mencionarán en el siguiente punto, cuando ocurriere por causas técnicas, será comunicada previamente por el PSC al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación. La revocación no privará de valor a los certificados antes del momento exacto que sean verificadas por el prestador.

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

24.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Un certificado podrá ser revocado debido a las siguientes circunstancias:

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 digital es falso.
- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
- Pérdida o cambio del Suscriptor de la vinculación con la Corporación, en el caso de Certificados Corporativos.
- Liquidación de la persona jurídica representada que consta en el certificado digital.

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 Thomas Signe, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción, por parte de Thomas Signe, relativa a los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Titular.
- Acceso o utilización no autorizados, por un tercero, de la clave privada del Titular.
- El incumplimiento por parte del Titular de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre Thomas Signe y el Titular.
- El incumplimiento del Contrato de Prestación de Servicios de Firma Electrónica Avanzada proporcionado por Thomas Signe.

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 Titular.
- Manejo indebido por parte del titular del certificado digital.
- El incumplimiento por parte del Titular de las normas de uso del dispositivo criptográfico expuestas en la presente DPC o en el Contrato de Prestación de Servicios de Firma Electrónica Avanzada.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 28 de 62

d) Circunstancias que afectan al Titular:

- Finalización de la relación jurídica entre Thomas Signe y el Titular.
- Terminación del Contrato de Prestación de Servicios de Firma Electrónica Avanzada, 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 Titular.
- Oposición o modificación, por parte del Firmante, de los datos contenidos en el fichero de datos de carácter personal de Thomas Signe.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
- Infracción por el Titular, 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 Titular.

e) Otras circunstancias:

- Por pérdida, inutilización del certificado digital que haya sido informado a Thomas Signe.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la DPC.
- Por cualquier causa que induzca a creer razonablemente que el servicio de certificación haya sido comprometido, poniendo en duda la confiabilidad del certificado digital.

24.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

Pueden solicitar la revocación de un certificado:

- a) El propio Titular, 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 por Thomas Signe de acuerdo con la Política de certificación correspondiente.

24.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN


El procedimiento de revocación se lleva a cabo de acuerdo con lo indicado en la PC respectiva.

24.4 PLAZO EN EL QUE EL PSC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Una vez la identidad del Titular haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por la AR, la revocación se hará efectiva inmediatamente.

24.5 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, mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 29 de 62

24.6 FRECUENCIA DE EMISIÓN DE LAS CRLS

La CRL de Thomas Signe Root se emite antes de que hayan transcurrido 180 días de la emisión de la anterior CRL o cuando se produzca una revocación.

La CRL del PSC Thomas Signe Chile se actualiza al menos cada 24 horas.

24.7 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

Dado que la publicación de las CRL se realiza en el momento de la generación de esta, se considera cero o nulo el tiempo transcurrido.

24.8 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 Thomas Signe, esta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

24.9 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA

Para el uso del servicio de CRLs, que es 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 Point".
- 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 son retirados de la CRL.


25 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

25.1 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, ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

25.2 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.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 30 de 62

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control del PSC, esta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

Cabe resaltar que la utilización del servicio OCSP es público y de uso gratuito.

25.3 FINALIZACIÓN DE LA SUSCRIPCIÓN

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

26 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 Telefónica TIER IV GOLD ubicado en Madrid (España).

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

26.1 CONTROLES FÍSICOS

La AC 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.)
- 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, al encontrarse en el centro urbano de una capital de provincia.

26.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Las instalaciones de la AC 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 es una jaula de Faraday, falso suelo, detección y extinción de incendios, sistemas antihumedad, sistema de refrigeración y sistema de suministro eléctrico.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 31 de 62

26.1.2 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 y su archivo.

Las instalaciones cuentan con cámaras y Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

26.1.3 EXPOSICIÓN AL AGUA

Además, el sistema de climatización se realiza mediante equipos autónomos que aseguran unos niveles de temperatura y humedad óptimos para el funcionamiento de los servidores y la electrónica de red.

26.1.4 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

En el diseño de las instalaciones eléctricas existe redundancia de equipos, añadiéndole una serie de elementos alternativos tales como sistemas de by-pass, transferencias de cargas críticas sin cortes de tensión, aislamiento galvánico, red equipotencial de tierra, etc., que permiten asegurar el máximo nivel de disponibilidad eléctrica para los equipos alojados.

26.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

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


26.1.6 SISTEMA DE ALMACENAMIENTO

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

26.1.7 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 físicamente destruidos o hacer ilegible la información contenida.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 32 de 62

26.1.8 BACKUP FUERA DE LA INSTALACIÓN

La AC mantiene un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos independiente del centro operacional.

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

26.2 CONTROLES DE PROCEDIMIENTO

26.2.1 ROLES DE CONFIANZA

Los roles de confianza de la infraestructura tecnológica de Thomas Signe, son los que se describen en el documento "Gestión de Acceso al Sistema de la CA". 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. Se cuenta con roles para la administración de la plataforma EJBCA, destinada a la generación y administración de las claves de la AC. Por otro lado, se cuenta con roles para la administración de la plataforma de Thomas Signe AR, destinada a la administración de la Autoridad de Registro de Thomas Signe.


El proveedor de infraestructura cuenta con roles que se encargan de la administración de las plataformas, los cuales son:

- Responsable de Certificación digital: Responsable de administrar la infraestructura técnica de servicios electrónicos de la AC, bajo el cumplimiento de las Prácticas de Certificación. Dentro de la plataforma EJBCA, 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 AC. Dentro de la plataforma EJBCA, cumple el rol de Administrador de la CA.
- Responsable de Registro Digital: Responsable de la supervisión de las operaciones de validación de identidad de las personas que solicitan la emisión o revocación de certificados digitales. Dentro de la plataforma 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. Dentro de la plataforma de Thomas Signe RA, cumple el rol de Agente de la RA.

26.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Thomas Signe garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave de las AC's.
- La recuperación y back-up de la clave privada de las AC's.
- La emisión de certificados de las AC's.
- Activación de la clave privada de las AC's.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root AC.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 33 de 62

26.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada rol de confianza de Thomas Signe se autentica mediante usuario y contraseña según las políticas establecidas y/o la utilización de dispositivos criptográficos seguros. La autenticación dentro de las plataformas previamente mencionadas permite el acceso a determinados activos de información de Thomas Signe.

26.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Las tareas de Auditor son incompatibles con las tareas de AC y de AR. Asimismo, los roles de la AC son incompatibles con los de la AR.

26.3 CONTROLES DE PERSONAL

26.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables sin supervisión lleva al menos seis meses trabajando en el centro de operación 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 AC se asegura que el personal de la AR es personal confiable para realizar las tareas de registro. Para el personal de Thomas Signe Chile se exige una autorización para su respectivo rol.

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

La AC 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.

26.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES


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

26.3.3 REQUISITOS DE FORMACIÓN

Se llevan a cabo los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

26.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se realizarán actualizaciones con una frecuencia anual, salvo por modificaciones a la DPC, que serán notificadas a medida que sean aprobadas.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 34 de 62

26.3.5 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Se dispone de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

26.3.6 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados en Thomas Signe Chile para realizar tareas confiables deberán firmar anteriormente los acuerdos de confidencialidad y los requerimientos operacionales respectivos. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

26.3.7 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Thomas Signe 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.

26.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD



26.4.1 TIPOS DE EVENTOS REGISTRADOS

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

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados a la red interna.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la Autoridad de Certificación.
- Encendido y apagado de la aplicación.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

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

- Las ceremonias de creación de claves de las AC y las bases de datos de gestión de claves.
- Registros de acceso físico.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 35 de 62

- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de titular, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las AC que abastezca a Thomas Signe.

26.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

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

26.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

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

26.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Se protege su disponibilidad mediante el almacén en instalaciones externas.

Los dispositivos son manejados en todo momento por personal autorizado.

26.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA



Thomas Signe 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.

La AC tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.

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

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

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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 36 de 62

26.4.7 ANÁLISIS DE VULNERABILIDADES

La AC realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo con el procedimiento interno establecido al efecto en las políticas de seguridad.

Se realizan análisis internos de vulnerabilidades periódicamente y externos al menos una vez al año.

26.5 ARCHIVO DE REGISTROS

26.5.1 TIPOS DE EVENTOS ARCHIVADOS

Thomas Signe conservarán los eventos que tengan lugar durante el ciclo de vida del certificado. Se almacenará por la AC o, por delegación de esta en la AR:

- Todos los datos de la auditoría,
- Todos los datos relativos a los certificados, incluyendo los contratos con los titulares 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 AC es responsable del correcto archivo de todo este material y documentación.

26.5.2 PERIODO DE CONSERVACIÓN


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. Se debe mantener un registro de acceso público de certificados, en los términos señalados en el reglamento. A dicho registro podrá acceder por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador (Thomas Signe) podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la Ley N° 196.28, sobre Protección de la Vida Privada.

Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración. Los contratos con los titulares y cualquier información relativa a la identificación y autenticación del titular serán conservados durante al menos 6 años o el periodo que establezca la legislación vigente.

26.5.3 PROTECCIÓN DE ARCHIVOS

Thomas Signe asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

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

	P002 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 37 de 62

26.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Thomas Signe 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.

26.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los registros están fechados con una fuente fiable.

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

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

No estipulado.

26.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Se verificará la integridad de la información archivada.

El acceso a la información archivada se realiza solo por personal autorizado.



Thomas Signe proporcionará la información y los medios para poder verificar la información archivada.

26.6 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Thomas Signe ha desarrollado un documento de Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio y ha probado Planes de Recuperación de Desastres (DRPs) indicados en dicho documento.

Como parte de los incidentes de seguridad que deben ser registrados por Thomas Signe, se encuentran:

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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 38 de 62

26.6.1 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE

El documento Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio ha sido desarrollado para recuperar todos los sistemas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por el documento Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

26.6.2 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Thomas Signe restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con esta DPC dentro de las 24 horas posteriores a un desastre o emergencia imprevista. Asimismo, se siguen las directrices indicadas en el documento Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.

26.7 CESE DE UN PSC



Ante el cese de servicios de Thomas Signe se procederá de la siguiente forma:

- En primera instancia se solicita la cancelación de su inscripción en el registro de prestadores acreditados a la Entidad Acreditadora; con un tiempo de antelación no inferior a un mes.
- En caso de que Thomas Signe cese en la prestación del servicio, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:
 - a) Si el cese es voluntario, con una antelación de dos meses y señalando al titular que, de no existir objeción a la transferencia de los certificados a otro PSC, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de estos. En este caso, si el prestador es acreditado, deberá traspasar los certificados, necesariamente, a un certificador acreditado.
 - b) Si el cese se produce por cancelación de la acreditación, deberá comunicarse inmediatamente a los titulares. En caso de que el prestador de servicios de certificación decida traspasar los certificados a otro prestador acreditado, deberá informar tal situación en la forma y plazo señalado en la letra a).

En caso de que el cese en la prestación del servicio por voluntad del prestador acreditado de servicios de certificación deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en la página web de ésta, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda.

El cese de la actividad del PSC será registrado como nota de cancelación de la acreditación por la Entidad Acreditadora en la página web de ésta.

Cabe mencionar que los datos proporcionados por el titular del certificado deberán ser conservados por el prestador de servicios de certificación a lo menos durante seis años desde la emisión inicial de los certificados, cualquiera sea estado en que se encuentre el certificado. Por ende, en caso del cese de actividad del PSC, se deberá transferir dichos datos a un prestador de servicios de certificación acreditado o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los seis años desde la emisión de cada certificado.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 39 de 62

27 CONTROLES TÉCNICOS DE SEGURIDAD

27.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

27.1.1 GENERACIÓN DEL PAR DE CLAVES

La generación de las claves de la AC 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, de la organización titular de Thomas Signe, y del 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 firmante, bien por medios físicos, bien estableciendo el titular los controles y medidas de seguridad adecuadas.

Thomas Signe puede garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Seguro de Creación de Firma (DSCF) que cumpla con los requisitos que se indicará en el propio certificado mediante la inclusión del identificador OID correspondiente en la extensión "Certificate Policies".

27.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES


El Titular cargará su certificado en el dispositivo en el que se hayan generado previamente el par de claves. Dicho dispositivo deberá contar con la certificación FIPS 140-2 level 3 pudiendo ser un token/tarjeta o HSM Centralizado. En el caso que el Certificado se genere en un HSM Centralizado, la clave privada y el certificado están custodiados por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3 garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere de las contraseñas definidas por el titular del certificado (contraseña del HSM Centralizado y contraseñad del Certificado) más un segundo factor de autenticación, el cual cumple con el estándar NIST-SP-800-63 y se encuentra en continua evaluación para garantizar siempre su seguridad y que solo el Titular tiene acceso al certificado y a su uso.

27.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El envío de la clave pública al PSC para la generación del certificado se realiza mediante un formato estándar PKCS#10 auto firmado, utilizando un canal seguro para la transmisión.

27.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL PSC A TERCEROS ACEPTANTES

Los Terceros aceptantes podrán consultar certificado de las AC Raíz y 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.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 40 de 62

27.1.5 TAMAÑO DE LAS CLAVES

Certificado	Tamaño claves RSA (bits)	Periodo validez
AC Raíz	4096	20 años
AC Subordinadas	4096	Hasta 14/03/2038 00:00:00, tiempo UTC
Entidad final	2048	Lo establecido en la legislación y normativa vigentes

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

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas de la ETSI: TS 102 176-1.

Concretamente los parámetros utilizados son los siguientes:


Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa

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

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

Los usos admitidos para la AC Raíz y Subordinada son firmar los certificados y firmar las 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.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 41 de 62

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

27.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos empleados para generar y almacenar las claves del PSC están certificados con la norma FIPS 140-2 nivel 3.

Las claves de los titulares de certificados reconocidos con DSCF y de operadores y administradores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico con FIPS 140-2 para la protección de riesgos asociados y los compromisos de seguridad que contiene, dando lugar a un nivel de aseguramiento alto.

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

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

27.2.3 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la AC Raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación y 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 AC Subordinada está custodiada en un dispositivo criptográfico seguro certificado con la norma FIPS 140-2 nivel 3.


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

Si el titular custodia las claves privadas del firmante, deberá realizarlo utilizando dispositivos criptográficos seguros certificados con la norma FIPS 140-2 y garantizando en todo momento el uso exclusivo de las claves por parte del firmante.

27.2.4 BACKUP DE LA CLAVE PRIVADA

Existen unos dispositivos que permiten la restauración de la clave privada de la AC, 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 al menos 2 de 3 dispositivos criptográficos (llaves).

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 42 de 62

27.2.5 ARCHIVO DE LA CLAVE PRIVADA

Thomas Signe no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de esta.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de Thomas Signe para comunicarse entre sí, firmar y cifrar la información serán archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.

27.2.6 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

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

27.2.7 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

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

27.2.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

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

27.2.9 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 AC, o de los datos de activación de estas.

27.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES



27.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Thomas Signe conservará todas las claves públicas durante al menos seis años.

27.3.2 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 existirá un servicio de verificación en línea válido para ese certificado.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 43 de 62

27.4 DATOS DE ACTIVACIÓN

27.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados al titular mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

27.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

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

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

27.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

27.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Thomas Signe 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 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.
- Configuración antivirus.
- Requerimientos de tráfico de red.

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

27.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de Thomas Signe incluye las siguientes funcionalidades:

- Control de acceso a los servicios de Thomas Signe y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 44 de 62

- Archivo del historial del titular y de Thomas Signe y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios de Thomas Signe.
- Mecanismos de recuperación de claves y del sistema de Thomas Signe.

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

27.5.2 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.

27.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

27.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Thomas Signe 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.

27.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Gestión de seguridad

Thomas Signe 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 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 dispone de un adecuado Procedimiento de gestión de incidencias y de la continuidad del negocio.

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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 45 de 62

Thomas Signe 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 mantiene un registro de las capacidades de los equipos.

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

Gestión del sistema de acceso

Thomas Signe 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:


- 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 documentado 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 será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación del certificado:

- Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.
- La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de Thomas Signe.

c) Gestión de la revocación:

- Las instalaciones de Thomas Signe están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.
- La revocación se refiere a la pérdida 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 generaran las pruebas que garantizan el no repudio de la acción realizada por el operador de Thomas Signe.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 46 de 62

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 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 registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Thomas Signe.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Thomas Signe realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo criptográfico solo es manipulado por personal confiable.

La clave privada de firma del almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.

La configuración del sistema del PSC así como sus modificaciones y actualizaciones son documentadas y controladas.

Thomas Signe 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.

27.7 CONTROLES DE SEGURIDAD DE LA RED


El PSC 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.

28 PERFILES DE CERTIFICADOS, CRL Y OCSP

28.1 PERFIL DE CERTIFICADO

El perfil de los certificados se corresponde con el propuesto en las PCs correspondientes, y son coherentes con lo dispuesto en las normas siguientes:

- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- ETSI EN 319 412 Certificate Profiles.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 47 de 62

28.1.1 NÚMERO DE VERSIÓN

Los certificados siguen el estándar X.509 versión 3.

28.1.2 PERFILES

A continuación, se describen los campos del Perfil común, de la AC Raíz y AC Subordinada.


PERFIL COMÚN A TODOS 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
validity	notBefore	Válido desde Fecha y hora de inicio de validez del certificado, tiempo UTC ³
	notAfter	Válido hasta Fecha y hora de fin de validez del certificado, tiempo UTC ⁴
subject	Asunto (DN)	DN del titular del certificado

¹ Valor aleatorio de 20 bytes

² sha256WithRSAEncryption

³ Fecha y hora de emisión del certificado

⁴ Ver en la PC respectiva la validez de cada certificado

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 48 de 62

subjectPublicKeyInfo	Clave pública	OID ⁵ y parámetros del algoritmo y valor ⁶ de la clave pública
extensions	Extensiones del certificado	Extensiones del certificado


CERTIFICADO DE CA RAÍZ		
CAMPO ISSUER DEL CERTIFICADO		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CO ⁷
State or Province Name (ST)	Estado/Provincia	Distrito Capital ⁸
Locality Name (L)	Localidad	Bogotá ⁸
Street Address (STREET)	Dirección	see current address at www.thomas-signe.com ⁸
Organization Identifier (2.5.4.97)	Identificador de Organización	900962071-5 ⁸
Organization Name (O)	Nombre de Organización	Thomas Signe Soluciones Tecnológicas Globales S.A. ¹¹
Common Name (CN)	Nombre	Thomas Signe Root ¹¹

⁵ rsaEncryption

⁶ Ver en la PC respectiva el tamaño de claves RSA de cada certificado

⁷ Codificado en PrintableString

⁸ Codificado en UTF8String

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 49 de 62


CAMPO SUBJECT DEL CERTIFICADO		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CO ⁹
State or Province Name (ST)	Estado/Provincia	Distrito Capital
Locality Name (L)	Localidad	Bogotá
Street Address (STREET)	Dirección	see current address at www.thomas-signe.com
Organization Identifier (2.5.4.97)	Identificador de Organización	900962071-5
Organization Name (O)	Nombre de Organización	Thomas Signe Soluciones Tecnológicas Globales S.A.
Common Name (CN)	Nombre	Thomas Signe Root

CERTIFICADO DE CA SUBORDINADA CHILE		
CAMPO ISSUER DEL CERTIFICADO		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CO ¹⁰
State or Province Name (ST)	Estado/Provincia	Distrito Capital ¹¹

⁹ Codificado en PrintableString

¹⁰ Codificado en PrintableString

¹¹ Codificado en UTF8String

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 50 de 62


Locality Name (L)	Localidad	Bogotá ¹¹
Street Address (STREET)	Dirección	see current address at www.thomas-signe.com ¹¹
Organization Identifier (2.5.4.97)	Identificador de Organización	900962071-5 ¹¹
Organization Name (O)	Nombre de Organización	Thomas Signe Soluciones Tecnológicas Globales S.A. ¹¹
Common Name (CN)	Nombre	Thomas Signe Root ¹¹
CAMPO SUBJECT DEL CERTIFICADO		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CL ¹²
Organization Name (O)	Nombre de Organización	Thomas Signe Chile S.A. ²
Serial Number (serialNumber)	Número de Serie	76934091-2 ¹
Common Name (CN)	Nombre	Thomas Signe Chile AC Firma Electrónica Avanzada ²

28.1.3 EXTENSIONES DEL CERTIFICADO

Las extensiones aquí presentadas corresponden a la AC Raíz y a la AC Subordinada. En la PC de cada tipo de certificado se especificará las extensiones requeridas para cada uno.


EXTENSIONES DE LA CA RAÍZ		
Extensión	Crítica	Valor

¹² Codificado en PrintableString

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 51 de 62

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 DE CA SUBORDINADA CHILE		
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://cl.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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 52 de 62

Authority Information Access	-	URI del certificado de la CA Raíz: http://thsigne.com/certs/thomas_signe_root.crt
-------------------------------------	---	---

28.1.4 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 Algoritmo de firma de sellos de tiempo
id-sha256	2.16.840.1.101.3.4.2.1	Algoritmo de hash de firma de sellos de tiempo

28.1.5 FORMATOS DE NOMBRES

Los valores comunes a todos los certificados se encuentran descritos en la sección “Perfiles”.

28.1.6 RESTRICCIONES DE LOS NOMBRES

Respecto a la codificación de los certificados, y siguiendo el estándar RFC 5280 (“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”), los certificados emitidos a partir del 17 de abril de 2008 emplean la codificación UTF8String para los campos que contengan caracteres especiales, y PrintableString para el resto.


28.1.7 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

Los OID de las Políticas de certificación se encuentran descritas en cada Política de certificación de acuerdo al tipo de certificado y en la sección “Tipos de certificado” de la presente DPC.

28.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Referente a los calificadores de la política de certificación, se utiliza en la extensión Certificate Policies:

- DPC: Contiene la URI donde se puede encontrar la DPC.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 53 de 62

28.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY

La extensión Certificate Policy permite identificar la política que Thomas Signe asocia al certificado y donde se pueden encontrar dichas políticas.

28.2 PERFIL DE CRL


El perfil de las CRL es el siguiente, conforme al estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (TBSCertList):

28.2.1 NÚMERO DE VERSIÓN

Las CRL emitidas por Thomas Signe son de la versión 2.

28.2.2 CRL Y EXTENSIONES

Campo de la CRL	Descripción	Valor
version	Nº de versión	v2
signature	Algoritmo de firma	OID y parámetros del algoritmo de firma
issuer	Emisor (DN)	DN de la CA que emite la CRL
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
revokedCertificates	userCertificate Nº de serie del certificado revocado	Nº de serie del certificado revocado
	revocationDate Fecha y hora de revocación del certificado	Fecha y hora de revocación del certificado, tiempo UTC

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 54 de 62

	crlEntryExtensions	Extensiones de entrada de CRL	Extensiones de entrada de CRL
crlExtensions		Extensiones de la CRL	Extensiones de la 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

28.3 PERFIL OCSP

El perfil OCSP 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.

29 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

Thomas Signe se somete a las auditorías de conformidad que realiza la Entidad Acreditadora, directamente o a través de terceros, de conformidad con lo dispuesto en el artículo 162 del Decreto-ley 19 de 2012. Asimismo, de acuerdo con lo exigido en la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" – EA-103 en su versión vigente, establecida por la Entidad Acreditadora.

En caso aplique, Thomas Signe permite y facilita la realización de auditorías por parte de la Superintendencia de Industria y Comercio.

Por otro lado, Signe en calidad de proveedor de infraestructura tecnológica, cuenta con la certificación eIDAS, ISO 9001, ISO 14001, ISO 14298, ISO 27001 y ENS (Esquema Nacional de Seguridad) nivel medio; sometiéndose a auditorías anuales que cubren los servicios de emisión de certificados digitales.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 55 de 62

29.1 FRECUENCIA DE LAS AUDITORÍAS

Se realizarán auditorías periódicas, generalmente con carácter anual.

Específicamente, la auditoría realizada por la Entidad Acreditadora a los servicios de Thomas Signe, se realiza cada año. De la misma manera, cumple anualmente con la Auditoría de tercera parte.

Por otro lado, Signe se somete anualmente a la auditoría eIDAS, ISO 9001, ISO 14001, ISO 14298, ISO 27001 y ENS (Esquema Nacional de Seguridad) nivel medio.

Cabe destacar que Signe se compromete a realizar las auditorías necesarias para obtener en su propio nombre dicha certificación.

29.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

Las auditorías de conformidad que competen a Thomas Signe son realizadas por auditores designados por la Entidad Acreditadora.

Las auditorías de tercera parte se realizan por auditores que cumplan con lo establecido en los Criterios Específicos de la Entidad Acreditadora vigente.

Las auditorías a las que se somete Signe, pueden ser de carácter tanto interno como externo. En este segundo caso, se realizan por empresas de reconocido prestigio en el ámbito de las auditorías.


29.3 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.

29.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría verifica, en general, los siguientes principios:

- a) **Publicación de la Información:** Que Thomas Signe hace públicas las Prácticas de Negocio y de Gestión de Certificados (la presente DPC), así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.
- b) **Integridad de Servicio.** Que Thomas Signe mantiene controles efectivos para asegurar razonablemente que:
 - La información del titular es autenticada adecuadamente (para las actividades de registro realizadas por Thomas Signe), y
 - La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.
- c) **Controles generales.** Que Thomas Signe mantiene controles efectivos para asegurar razonablemente que:
 - La información de titulares y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio de Thomas Signe publicadas.
 - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 56 de 62

Las tareas de explotación, desarrollo y mantenimiento de los sistemas de Thomas Signe son adecuadamente autorizadas y realizadas para mantener la integridad de estos.

29.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

En caso de que sean detectadas incidencias o no conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible. Para no conformidades graves (afectan a los servicios críticos); Thomas Signe se compromete, según corresponda, a su resolución en un plazo máximo de tres meses.

29.6 COMUNICACIÓN DE RESULTADOS

El auditor se comunicará con el Director de Sistemas de la Información.

30 OTROS ASUNTOS LEGALES Y COMERCIALES

30.1 TARIFAS

30.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS

Las Tarifas pueden ser consultadas al correo electrónico certificados@thomas-signe.cl

30.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos es libre y gratuito y por tanto no aplica una tarifa.

30.1.3 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.

30.1.4 TARIFAS DE OTROS SERVICIOS

Una vez se ofrezcan otros servicios por parte de Thomas Signe, se publicarán en la dirección: www.thomas-signe.cl

30.2 RESPONSABILIDADES ECONÓMICAS

Thomas Signe, 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

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 57 de 62

responsabilidades en su actividad. La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a la exigida por la normativa vigente.



Se deberá contratar y mantener vigente un seguro de responsabilidad civil, que cubra los posibles daños y perjuicios que ocasionen, con motivo de certificación y homologación de firmas electrónicas, el que deberá contener las siguientes estipulaciones mínimas:

- a) Una suma asegurada de al menos el equivalente de cinco unidades de fomento.
- b) La ausencia de deducibles o franquicias, en la parte de no indemnización que no exceda el equivalente de cinco mil unidades de fomento.
- c) La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante, sea reclamada con posterioridad a ella.

30.3 EXONERACIÓN DE RESPONSABILIDAD

Thomas Signe, 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 Titular 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 AC.
- 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 con acciones u omisiones del Solicitante y Titular:
 - Falta de veracidad de la información suministrada para emitir el certificado.
 - Retraso en la comunicación de las causas de suspensión o revocación del certificado.
 - Ausencia de solicitud de suspensión o 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 Thomas Signe o la AR le notifique la revocación o suspensión de este.
 - Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la DPC de Thomas Signe, 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 firmante por Thomas Signe.
- f) En relación con 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 Thomas Signe en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
 - Falta de comprobación de la suspensión o 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.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 58 de 62

30.4 RESPONSABILIDADES FINANCIERAS

30.4.1 COBERTURA DEL SEGURO

El seguro se hará cargo de todas las cantidades que Thomas Signe 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.

30.4.2 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

No existe cobertura para los terceros aceptantes.

30.5 DERECHOS DE PROPIEDAD INTELECTUAL

- a) Propiedad de la DPC.
 - La propiedad intelectual de esta DPC y de las distintas PC pertenece a Thomas Signe.
- b) Propiedad de los certificados.
 - Thomas Signe será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita si no se acuerda explícitamente lo contrario.
 - Thomas Signe concede licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política y de acuerdo con el correspondiente instrumento vinculante entre Thomas Signe y la parte que reproduzca y/o distribuya el certificado, así como con las correspondientes condiciones generales de emisión.
- c) Propiedad de las claves.
 - El par de claves es propiedad del titular.



30.6 OBLIGACIONES

30.6.1 OBLIGACIONES DEL PSC

Thomas Signe se obligan según lo dispuesto en este documento, principalmente a:

- d) Respetar lo dispuesto en las Políticas y Prácticas de Certificación (la presente DPC), así como en el Contrato de Suscripción.
- e) Publicar esta DPC en su página Web.
- f) Informar sobre las modificaciones de esta DPC a los titulares, mediante la publicación de estas y sus modificaciones en su página web.
- g) Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.
- h) Utilizar sistemas fiables para almacenar certificados reconocidos 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 firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Por lo que a certificados respecta:

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 59 de 62

- a) Emitir certificados conforme a esta DPC 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) Publicar los certificados emitidos en un Registro de Certificados, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- e) Suspender y revocar los certificados según lo dispuesto en la DPC 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 periodo mínimo exigido por la normativa vigente, cuando sea aplicable.
- b) No almacenar ni copiar los datos de creación de firma del Titular, 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.

30.6.2 OBLIGACIONES DE LA AR

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

- i) Respetar lo dispuesto en esta DPC y en la PC correspondiente al tipo de certificado que emita.
- j) Respetar lo dispuesto en los contratos firmados con Thomas Signe.
- k) Respetar lo dispuesto en los contratos firmados con el Titular. 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 Thomas Signe.
 - Verificar la exactitud y autenticidad de la información suministrada por el titular o solicitante.
 - Informar al solicitante, 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 y de verificación 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 Thomas Signe, 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.
 - Formalizar 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 titular.
 - Informar a Thomas Signe las causas de revocación.
 - Realizar las comunicaciones con los titulares, por los medios que consideren adecuados, para correcta gestión del ciclo de vida de los certificados. Concretamente

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 60 de 62

realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las suspensiones, rehabilitaciones y revocaciones de estos.

30.6.3 OBLIGACIONES DE LOS PROVEEDORES

El Proveedor de infraestructura y servicios tecnológicos de Thomas Signe se encuentra obligado a cumplir con los requisitos mínimos exigidos por la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" – EA-103 Versión 2.4 establecida por la Entidad Acreditadora, 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 AC
- g) Requisitos de la AR
- h) Requisitos técnicos

30.6.4 OBLIGACIONES DE LOS SOLICITANTES



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

- a) Suministrar a la AR 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) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- d) Respetar lo dispuesto en los documentos contractuales firmados con Thomas Signe y los solicitantes.

30.6.5 OBLIGACIONES DE LOS FIRMANTES

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

- a) Custodiar sus claves privas y códigos secretos de manera diligente.
- b) Usar el certificado según lo establecido en la presente DPC.
- c) Respetar lo dispuesto en los instrumentos jurídicos vinculantes con Thomas Signe y los firmantes.
- d) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.
- e) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- f) No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por Thomas Signe de la revocación de este, o una vez expirado el plazo de validez del certificado.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 61 de 62

30.6.6 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Será obligación de los usuarios cumplir con lo dispuesto por la normativa vigente y además a:

- 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 confía, y aceptar sujetarse a las mismas.
- c) Notificar a Thomas Signe cualquier situación irregular con respecto al servicio prestado por el PSC.

31 POLÍTICA DE PROTECCIÓN DE DATOS

Thomas Signe garantiza la protección de datos personales de los titulares de los servicios de certificación digital. Además, se compromete a no usar ni divulgar la información entregada por el titular, clasificada como confidencial, más que para los fines propios del procedimiento de acreditación. Este compromiso es extensible a todo Organismo y persona que intervenga en el proceso de acreditación.

En cumplimiento de la Ley-19628 de “Protección de datos de carácter personal” y la Ley-19799 “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”, y de la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” – EA-103 Versión 2.4 establecida por la Entidad Acreditadora.

Se entiende por información sensible la contemplada en el artículo 2° de la Ley N°19.628 letra g) que señala “g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.”

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


32 CONFIDENCIALIDAD DE LA INFORMACIÓN

Thomas Signe, 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.

32.1 INFORMACIÓN CONFIDENCIAL

La siguiente información será considerada confidencial:

- Las claves privadas de la AC raíz y AC subordinada de Thomas Signe.
- Acta de Ceremonia de generación de las claves
- Procedimiento de Ceremonia de generación de las claves.
- La información de negocio suministrada y/o elaborada juntamente con Thomas Signe por parte de sus clientes, proveedores u otras personas con las que Thomas Signe se comprometió a guardar secreto establecido legal o convencionalmente. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos.
- Las validaciones de identidad de titulares, provistas por fuentes públicas o privadas.

	PO02 Declaración de Prácticas de Certificación para Firma Electrónica Avanzada	Versión 1.2
	Código: THS-CL-AC-DPC-01	Página 62 de 62

- La información obtenida del titular por fuentes diferentes del titular y que haya sido catalogada como "Confidencial".
- Los datos recogidos durante la certificación digital.

32.2 INFORMACIÓN NO CONFIDENCIAL

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en las distintas Políticas de Certificación (CP).
- La información contenida en los certificados, puesto que para su emisión el titular 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.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

33 CONFORMIDAD CON LA LEY APLICABLE

Thomas Signe es afecta y cumple con las obligaciones establecidas por la Entidad Acreditadora, a los requerimientos de la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" - EA-103 Versión 2.4 establecida por la Entidad Acreditadora. vigente, a lo establecido en la Ley 19.799 de 2002, ley 19.799 de 2007, el Decreto 181 de 2002, modificación del Decreto 181 de 2012, y los reglamentos que los modifiquen o complementen.

34 BIBLIOGRAFÍA

- a) Criterios específicos de la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" - EA-103 Versión 2.4 establecida por la Entidad Acreditadora.
- b) Ley 19799 de 2002
- c) Ley 19628 de 1999