



POLÍTICA DE SELLO DE TIEMPO

Versión 1.1a

Santiago, 22 de Febrero de 2023



Tabla de Contenido

1. Introducción	5
1.1 Presentación	5
1.1.1 Sobre las Políticas de Sello de Tiempo	5
1.1.2 Alcance	5
1.1.3 Referencias	5
1.2 Sello de Tiempo (TS).....	6
1.2.1 Uso	6
1.2.2 Usos prohibidos	6
1.2.3 Estructura de los sellos de tiempo	6
1.3 Definiciones y Acrónimos	6
1.3.1 Definiciones	6
1.3.2 Acrónimos	7
2. Obligaciones y responsabilidades	8
2.1 Obligaciones de la TSA	8
2.1.1 General	8
2.1.2 Obligaciones de la TSA hacia sus suscriptores.....	8
2.2 Obligaciones del suscriptor	8
2.3 Obligaciones de partes que confían	9

2.4 Responsabilidades

	9
2.4.1 Responsabilidades Legales	9
2.4.2 Responsabilidades Generales	9
2.4.3 Fuerza Mayor	9

3. Requerimientos en prácticas de la TSA 10

3.1 Declaración de Prácticas y de Divulgación	10
3.1.1 Declaración de prácticas de TSA	10
3.1.2 Declaración de divulgación de TSA	10
3.2 Gestión del ciclo de vida de las llaves	11
3.2.1 Generación de la llave de TSU.....	11
3.2.2 Protección de la llave privada de TSU	11
3.2.3 Distribución de la llave pública de TSU	11
3.2.4 Recambio de llaves de TSU.....	12
3.2.5 Terminación del ciclo de vida de la llave de TSU	12
3.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo.	12
3.2.7 Requerimientos para suspensión y revocación de los certificados de TSA.	13
3.3 Sello de tiempo	15
3.3.1 Token de sello de tiempo	15
3.3.2 Sincronización de los relojes con UTC.....	16
3.3.3 Procedimiento de registro del Suscriptor	16

3.4	Gestión y operación de la TSA	17
3.4.1	Gestión de la seguridad	17
3.4.2	Gestión y clasificación de activos	17
3.4.3	Seguridad del personal.....	17
3.4.4	Seguridad física y ambiental.....	19
3.4.5	Gestión de las operaciones	21
3.4.6	Gestión de acceso a los sistemas	21
3.4.7	Mantenimiento e Implementación de sistemas de confianza	22
3.4.8	Cumplimiento de requerimientos legales	22
3.4.9	Confidencialidad y Registro de información relativa a las operaciones del	22
	Servicio de sello de tiempo.....	22
3.5	Organización	23
4.	Consideraciones de seguridad	24
5.	Revisión y aprobación del documento	24
5.1	Revisión	24
5.2	Aprobación	24
6.	Normativa Técnica	24

Control de Cambios			
Registro de control de cambios sobre el Documento			
Versión	Fecha	Descripción	Responsable
1.0	29-11-2019	Creación de documento	Ronald Pérez
1.2	18-10-2022	Especificación de contenido en 3.2.3	Juan Pizarro
1.2	Oct 2023	Especificación de contenido en 3.2.7.7	Juan Pizarro
1.3	Abril 2024	Especificación contenida en 3.3.3	Oficial de seguridad

1. Introducción

1.1 Presentación

En este documento se presenta la Política de sello de tiempo asociada a la emisión de Certificado de Sello de tiempo de E-Sign. Esta es una definición de las reglas que rigen los procedimientos o prácticas que E-Sign declara convenir en la prestación de sus servicios de sello de tiempo. Lo anterior tanto al momento de emitir o gestionar la información usada en la solicitud del sello, durante la verificación de los token de time-stamping, al momento de la confirmación de vigencia de la llave privada de la TSA - a través de la CRL o servicio OCSP - así como ante el evento de que la llave de la TSA haya sido comprometida; todo lo cual se encuentra definido en esta política. Se define además los roles, responsabilidades y relaciones entre el usuario final y E-Sign, siendo la Declaración de Prácticas de Sello de Tiempo de nuestra empresa un complemento a este documento.

Esta Declaración de Política de sello de tiempo constituye el marco general de normas aplicables a toda la autoridad certificadora de E-Sign, cuando ella actúa como Autoridad de sello de tiempo (TSA).

1.1.1 Sobre las Políticas de Sello de Tiempo

Las políticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los sellos de tiempo que provee E-Sign, desde la gestión de la solicitud de un sello de tiempo, la obtención de un tiempo confiable, hasta la emisión del sello de tiempo requerido. Es decir, son aquellas políticas a nivel de sistemas como de personal, que en base a sus buenas prácticas dan seguridad y confianza a los sellos de tiempo y servicios de certificación provistos por E-Sign.

1.1.2 Alcance

Este documento de servicios que presta E-Sign para la emisión de los mismos en su actuar como TSA.

1.1.3 Referencias

La presente Política de Sello de Tiempo se ha generado en base a las especificaciones del documento RFC 3628 4, 5, 7.4.8 y 7.4.9 "Policy Requirements for Time-Stamping Authorities" así como también de las especificaciones técnicas definidas en el documento ETSI TS 102 023 "Electronic Signatures and infraestructures (ESI) Policy Requirements for Time-Stamping Authorities" y el documento RFC 3161 "Internet X.509 Public Key infrastructure Time-Stamping Protocol (TSP)".

De manera complementaria a los documentos indicados, se ha utilizado el documento de nombre "Guía de Evaluación Procedimiento de Acreditación Prestadores de Servicios de

Certificación, Servicios de Certificación de Sello de Tiempo, versión 1.0, entregados por el Ministerio de Economía del Gobierno de Chile, como parte del proceso de acreditación.

1.2 Sello de Tiempo (TS)

Instrumento utilizado para dar evidencia de la existencia de un documento firmado con firma electrónica avanzada, antes de cierto instante de tiempo. Se trata de un parámetro firmado por una Autoridad de Sellado de Tiempo (TSA) utilizado para dar evidencia de la existencia de un documento antes de cierto instante de tiempo.

Los sellos de tiempo emitidos por E-Sign se utilizarán únicamente conforme a la función y finalidad que tengan establecida en estas Políticas de Certificación de Sello de Tiempo y la Declaración de Prácticas de Sello de Tiempo, en concordancia con la normativa vigente para garantizar el no repudio.

1.2.1 Uso

El uso de los sellos de tiempo aquí descrito está acotado a demostrar que un dato dado ha existido y no ha sido alterado en un instante específico y confiable.

El conjunto de normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denomina "Política de Sello de Tiempo".

1.2.2 Usos prohibidos

Los sellos de tiempo emitidos por E-Sign, se utilizarán únicamente conforme a la función y finalidad que se tenga establecida en la presente Política de Sello de tTempo y de acuerdo a la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

1.2.3 Estructura de los sellos de tiempo

La estructura de los sellos de tiempo generados por E-Sign, se ajustan al documento RFC 3161 "Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)".

1.3 Definiciones y Acrónimos

1.3.1 Definiciones

Concepto	Descripción
Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés Time Stamping Authority)	Sistema de emisión y gestión de sello de tiempo basado en una firma digital acreditada dentro de la jerarquía nacional de certificadores registrados, encargada de proveer uno o más servicios de sellado de tiempo a través de unidades de sellado de tiempo (TSU).

Parte que confía	Receptor del token de sellado de tiempo que confía en este sello de tiempo, o cualquier entidad que quiera comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Puede ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.
Política de Sellado de Tiempo	Conjunto de reglas que indican la aplicabilidad de un token de sellado de tiempo para una comunidad particular y/o la clase de aplicación con requerimientos de seguridad comunes.
Sistema de TSA	Conjunto de elementos organizados para soportar los servicios de sellado de tiempo.
Suscriptor	Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sello de Tiempo. En un proceso de sellado de tiempo, es el solicitante que posee la información a la que quiere incluir un sello de tiempo para probar que los datos existían antes de un determinado instante.
Tiempo Universal Coordinado	(UTC por sus siglas en inglés Universal Time Coordinated): También conocido como tiempo civil, el cual es determinado por la referencia a una zona horaria. El tiempo coordinado UTC está basado en relojes atómicos que se sincronizan para obtener una alta precisión y es el sistema de tiempo utilizado como estándar por la World Wide Web.
Token de sellado de tiempo	Dispositivo de datos empleado en un proceso de creación de firma electrónica, que está asociado a una representación de un dato para un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los tokens de sellado de tiempo deben emitirse de acuerdo al RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
Unidad de Sellado de Tiempo (TSU por sus siglas en inglés, TimeStamping Unit)	Es el conjunto de hardware y software que es gestionado como una unidad y que tiene una llave privada de la TSA para firmar tokens de sellado de tiempo.

1.3.2 Acrónimos

- TSA: Autoridad de Sellado de Tiempo
- TSS: Servicio de Sellado de Tiempo
- TST: Token de Sellado de Tiempo •
- UTC: Tiempo Universal Coordinado
- TSU: Unidad de Sellado de Tiempo

2. Obligaciones y responsabilidades

2.1 Obligaciones de la TSA

2.1.1 General

E-Sign, en su calidad de Autoridad de Sello de Tiempo se obliga a:

- Realizar sus operaciones y proveer todos los servicios de Sello de Tiempo de acuerdo a lo dispuesto en ésta política, así como en la Declaración de Prácticas de Sello de Tiempo.
- En caso de subcontratar en el futuro alguno de los servicios, asegurar que los contratistas mantienen un fiel cumplimiento de esta política, así como de la Declaración de Prácticas de Sello de Tiempo.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sello de tiempo a los que sirven de soporte.

Las obligaciones específicas, pertinentes al sello de tiempo emitido detalladas en estas Políticas de sello de tiempo se encuentran disponible de manera pública en el sitio www.ESign.com.

2.1.2 Obligaciones de la TSA hacia sus suscriptores

- La TSA de E-Sign garantiza el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC, que está incluido en los sellos, se asegura con una desviación máxima 1 segundo.
- Además, garantiza que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo y se garantiza un nivel de servicio superior al 95% que permite dar el cumplimiento a las normas técnicas.

2.2 Obligaciones del suscriptor

- El suscriptor debe verificar que el token de Sellado de Tiempo se ha firmado de manera correcta y comprobar en la CRL el estado del certificado de la TSA, esta comprobación de validez se puede hacer también, utilizando el servicio OCSP.
- Además, el suscriptor debe asegurarse de conocer las normas estipuladas en las políticas y prácticas de certificación de sello de tiempo de E-Sign, así como el propósito y alcance de un sello de tiempo obtenido en E-Sign o en algún Prestador de Servicios de Sellos de Tiempo acreditado.

2.3 Obligaciones de partes que confían

Las partes que confían deben asegurarse de tener conocimiento tanto del alcance y uso del sello de tiempo recibido, como de las normas legales que sigue el Proveedor de Servicios de Certificación, además serán responsables de verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Adicionalmente deberán dar aviso a la TSA de cualquier situación anómala ya sea en el servicio o en los sellos de tiempo emitidos por la TSA.

2.4 Responsabilidades

2.4.1 Responsabilidades Legales

E-Sign no será responsable de cualquier perjuicio que derive de una utilización negligente o no acorde a las políticas y/o declaración de prácticas de sello de tiempo, por parte de los suscriptores o terceras partes que confían.

Las responsabilidades asumidas por E-Sign como TSA, se encuentran declaradas en sus prácticas de sello de tiempo y en los contratos o acuerdos de suscripción.

2.4.2 Responsabilidades Generales

E-Sign garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley N° 19.799, Ley 19.628 y Ley 19.496 de Chile, así como la Ley N° 27269, Ley 29733 y DECRETO SUPREMO 019 de Perú.

E-Sign, como proveedor de servicios de Sello de Tiempo, adhiere además a los estándares internacionales que rigen esta actividad, siendo ellos los documentos RFC 3628, RFC 3161 y su equivalente ETSI 102 023.

2.4.3 Fuerza Mayor

E-Sign queda exenta de responsabilidad en caso de pérdida o perjuicio, siendo esto el resultado de un evento de fuerza mayor que le impida proveer los servicios de TimeStamp.

3. Requerimientos en prácticas de la TSA

3.1 Declaración de Prácticas y de Divulgación

3.1.1 Declaración de prácticas de TSA

En particular E-Sign, como TSA establece que ha trabajado en:

- Una determinación de activos y riesgo asociado a cada uno de los activos relevantes que participan en los servicios de la TSA.
- Un SGSI para mitigar los riesgos detectados, el cual es controlado por un comité de seguridad, el que define los cursos de acción y aprueba las mejoras a los controles implantados.
- Una política y práctica que permita proveer los servicios de su TSA, así como las modificaciones a estos documentos que han sido formalmente aprobadas.
- La publicación hacia la comunidad de la información relevante asociada a este servicio tales como las condiciones bajo las que se provee los servicios de la TSA.

Además la Declaración de Prácticas de Sello de Tiempo de la TSA detalla los mecanismos y procedimientos establecidos para cumplir con las obligaciones y responsabilidades, control de seguridad, así como modificaciones y planes de mejora, elementos de información de contacto, características técnicas del servicio de sello, leyes y estándares, entre otros que constituyen el funcionamiento de la TSA, las que deben ser contempladas por todas las organizaciones externas que apoyan los servicios de la TSA incluyendo las políticas y prácticas de sello de tiempo aplicables.

3.1.2 Declaración de divulgación de TSA

LA TSA de E-Sign entrega como parte de estas políticas su información de contacto a los suscriptores y terceros, da a conocer la política que rige su operación(<https://firma.cl/privacidad>) , el algoritmo de hash utilizado, vigencia de la firma, la precisión del tiempo registrado en cada uno de los TST emitidos, responsabilidades y obligaciones de las partes que participan del proceso asociado al servicio de la TSA, información que permita verificar la validez del TST, el periodo de retención de los logs de eventos, normativa legal aplicada, limitación de responsabilidades, solución de conflicto entre las partes, resolución que aprueba la operación como Autoridad de sello de Tiempo emitida por el Ministerio de Economía.

3.2 Gestión del ciclo de vida de las llaves

3.2.1 Generación de la llave de TSU

Las llaves utilizadas por la TSU son generadas en módulos criptográficos que cumplen como mínimo con los requerimientos de FIPS 140-2 nivel 3 o Common Criteria EAL 4. El algoritmo de generación de llaves de TSU, el largo de estas llaves y el algoritmo de firma usado por TSU para firmar Tokens de sello de tiempo son apropiados para el propósito de firma de Tokens de sello de tiempo de acuerdo a estándares técnicos reconocidos por la industria, como se describe en la sección 3.2.1 de la Declaración de Prácticas de Sello de Tiempo. El proceso de generación de la llave de la TSU es llevado a cabo en un ambiente físicamente seguro, por parte de personal que cumple roles de confianza definidos, bajo un control a lo menos dual.

Para mayor detalle remítase a la Declaración de Prácticas de sello de tiempo de E-Sign, punto 3.1.1.

3.2.2 Protección de la llave privada de TSU

E-Sign cuenta con niveles de seguridad del HSM donde se almacena la clave bajo control, a fin de asegurar la confidencialidad e integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3.

En lo que respecta a la generación de la llave de la TSU, el módulo criptográfico utilizado por E-Sign mantiene la confidencialidad de la llave en su ciclo de tiempo completo, restringiendo el acceso a éste al personal autorizado solamente. De detectarse un acceso no autorizado, este se registra ya sea de manera física (tampering físico) o a través de log a ser usado durante la auditoría. Este equipo contempla además mecanismos de backup y respaldo de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos.

La TSA de E-Sign implementa prácticas para asegurar que las llaves de sus TSU mantienen su confidencialidad e integridad.

En particular,

- a) Las llaves utilizadas por la TSU para firmar sellos de tiempo son contenidas y utilizadas en módulos criptográficos que cumplen como mínimo con los requerimientos de FIPS 140-2 nivel 3 o Common Criteria EAL 4
- b) Las llaves utilizadas por la TSU para firmar sellos de tiempo no son respaldadas para así minimizar el riesgo de compromiso de las mismas.

3.2.3 Distribución de la llave pública de TSU

La TSA de E-Sign implementa prácticas para asegurar que las llaves públicas utilizadas para validar las firmas de sellos de tiempo emitidos por sus TSU, mantienen su integridad y autenticidad al ser distribuidas a terceras partes.

Las llaves públicas utilizadas para verificar firmas de la TSU son puestas a disposición de las terceras partes en un certificado de llave pública. Estos certificados son emitidos por Autoridades Certificadoras cuya Política de Certificación debe incluir como mínimo, requerimientos análogos a los especificados en 3.2.7.

El perfil de los certificados de Suscriptor debe incluir la extensión Extended Key Usage (2.5.29.37) y esta extensión debe incluir el valor `id-kp-timeStamping` (1.3.6.1.5.5.7.3.8).

3.2.4 Recambio de llaves de TSU

Por motivos de seguridad y para evitar el repudio a un certificado, E-Sign como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo a las políticas y prácticas que rigen la operación de su CA. Sin embargo, la llave privada de la TSU será reemplazada antes del fin de su periodo de validez.

3.2.5 Termina del ciclo de vida de la llave de TSU

Toda llave privada de la TSA de E-Sign debe ser reemplazada antes de su expiración. La TSA de E-Sign rechazará cualquier intento de emitir un sello de tiempo cuando la llave privada utilizada para la firma haya expirado. Después de expirada, toda llave privada de TSU es destruida al igual que sus copias de respaldo, si éstas existiesen, a fin de que tal llave privada no pueda ser recuperada.

3.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo.

Respecto al ciclo de vida del hardware criptográfico el personal de E-Sign y terceros involucrados deben cumplir la normativa de dicho ciclo que a continuación se detalla:

3.2.6.1 Hardware no es intervenido durante su viaje o almacenamiento

Los HSM de E-Sign cuentan con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión y en caso que ocurra esto en los HSM, cualquiera sea el motivo, las claves son borradas y destruidas, de acuerdo con los procedimientos del fabricante. Ante este tipo de eventos dichos equipos no entrarán a producción, previo a la reiniciación del equipamiento de acuerdo al quórum definido.

3.2.6.2 Administración del Hardware Criptográfico

El equipo HSM que será utilizado por E-Sign tanto para su PSC como TSA, implementa la seguridad de acceso a información criptográfica a través de diferentes niveles a fin de garantizar que los equipos no han sido manipulados y cumplen con los requisitos. Además E-Sign dispone de procedimientos asociados para el manejo de los HSM por el personal de confianza, utilizando tarjetas de administración y de operación. Lo anterior se encuentra clasificado de uso interno y revisado de forma periódica por el auditor.

Respecto a las características técnicas los equipos HSM de E-Sign cumplen con el estándar FIPS-140.

3.2.7 Requerimientos para el ciclo de vida de los certificados de TSA

Los certificados utilizados para autenticar las llaves de las TSU de la TSA son emitidos por Autoridades Certificadoras cuya Declaración de Prácticas de Certificación debe incluir como mínimo, requerimientos de ciclo de vida compatibles con los siguientes:

Nota: En esta sección el concepto Suscriptor hace referencia al suscriptor de certificado y no al Suscriptor del servicio TSA.

3.2.7.1 Solicitud de Certificados TSA

Un certificado de TSA puede ser solicitado por cualquier representante debidamente autorizado de una TSA.

Los Certificados de Organización son emitidos a organizaciones después de autenticar que la Organización tiene existencia legal y que otros atributos de la Organización – que sean incluidos en el Certificado - hayan sido autenticados.

3.2.7.2 Validación de Solicitudes de Certificados TSA

La identidad de la Organización e información de inscripción proporcionados por los solicitantes de Certificados (a excepción de la información del Suscriptor no verificada) debe ser confirmada, y la Solicitud de Certificado TSA sólo puede ser aprobada después de validar:

- a) La existencia de la organización mediante el uso de al menos una tercera parte proveedora de servicios de pruebas o base de datos, o, alternatively, la documentación de la organización emitida por o inscrita en el organismo de gobierno o autoridad reconocida competentes y que confirme la existencia de la organización.
- b) Que la Organización puede llevar a cabo las funciones de Autoridad de Sello de Tiempo, de acuerdo con los requisitos establecidos en los Procedimientos de Validación documentados por E-Sign.
- c) Que la Organización ha autorizado la Solicitud de Certificado de TSA.
- d) Que la persona que presenta la Solicitud de Certificado en nombre del Solicitante de Certificado, está autorizada para hacerlo y es empleado de la Organización.

3.2.7.3 Emisión de Certificados TSA

El Certificado es creado y entregado luego de la aprobación de la Solicitud de Certificado por la Autoridad Certificadora, o bien, luego de la recepción de un requerimiento de la RA, para que se emita el Certificado.

La Autoridad Certificadora crea y envía al Solicitante, o a la persona o entidad que éste haya indicado, su Certificado emitido basándose en la información contenida en la Solicitud de Certificado luego de la aprobación de tal Solicitud.

Los Certificados deberán estar disponibles para los Suscriptores, ya sea permitiéndoles descargarlos desde un sitio web, a través de un mensaje conteniendo el Certificado o a través de la entrega de los medios físicos en los cuales se almacena el certificado.

El perfil de los certificados de Suscriptor debe permitir el uso de la extensión Extended Key Usage (2.5.29.37) y esta extensión debe permitir incluir el valor id-kp-timeStamping (1.3.6.1.5.5.7.3.8).

3.2.7.4 Expiración de Certificados TSA

Los certificados de Suscriptor de Certificado están sujetos a un periodo de validez, el que corresponde al período de tiempo durante el cual la AC emisora garantiza que mantendrá información acerca del estado del certificado.

El período de validez que debe estar incorporado en el perfil del certificado, de acuerdo a las especificaciones de RFC 5280.

Un certificado expira al momento de finalizar el período de validez.

3.2.7.5 Recambio de Llaves de Certificados TSA

El recambio de llaves es realizado antes de la expiración del periodo de validez del Certificado de Suscriptor que las autentifica y en tal caso debe ser solicitado un nuevo certificado para la nueva llave pública.

Un Certificado no puede ser renovado después de su expiración.

3.2.7.6 Renovación de Certificados TSA

La renovación es funcionalmente equivalente al recambio de llaves.

La renovación del certificado es realizada antes de la expiración de su periodo de validez.

Un Certificado no puede ser renovado después de su expiración.

3.2.7.7 Revocación y Suspensión de Certificados TSA

Un Certificado de Suscriptor es revocado en cualquiera de los siguientes casos:

- Si el Suscriptor lo solicita,

- Si la Autoridad Certificadora toma conocimiento de y confirma el fallecimiento del Suscriptor,
- Si la Autoridad Certificadora es notificada de una resolución judicial ejecutoriada para revocar el certificado,
- Si la Autoridad Certificadora determina que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa,
- Si la Autoridad Certificadora determina que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del dispositivo que protege su llave privada,
- Si la información contenida en el Certificado, exceptuando la información no verificada del Suscriptor, es incorrecta o ha cambiado,
- Si la Autoridad Certificadora, una organización o un Suscriptor de Certificado tiene razones para creer o tiene fundadas sospechas de que ha habido un compromiso de la llave privada de un Suscriptor,
- Si la Autoridad Certificadora, o una organización tiene motivos para creer que el Suscriptor ha incumplido materialmente una obligación material, declaración o garantía de acuerdo al Acuerdo de Suscripción vigente,
- Si el Acuerdo de Suscriptor con el Suscriptor ha terminado su vigencia, por ejemplo por incumplimiento por parte del suscriptor de sus obligaciones.
- Si la relación entre una organización con un Suscriptor de Certificado se termina o simplemente finaliza de otra forma,
- Si a asociación entre una organización, que es un Suscriptor de un Certificado Organizacional y el representante de la Organización que tiene el control de la llave privada del Suscriptor se termina o simplemente finaliza de otra forma,
- Si la Autoridad Certificadora o una organización tiene motivos para creer que el Certificado fue emitido de manera que no está en concordancia con los procedimientos requeridos por la Política de Certificados, el Certificado fue emitido a una persona que no sea la que es Sujeto del Certificado o el certificado fue emitido sin la autorización de la persona que es Sujeto de dicho Certificado,
- Si la Autoridad Certificadora o una organización tiene motivos para creer que un hecho material en la Solicitud del Certificado es falso,
- Si la Autoridad Certificadora determina que un prerequisite material para la emisión del Certificado no estaba satisfecho.

Los participantes que pueden solicitar la revocación de un certificado Suscriptor son:

- Un representante debidamente autorizado de la organización tendrá derecho a solicitar la revocación de los Certificados emitidos a la organización,
- Un representante debidamente autorizado de la Autoridad Certificadora,
- La entidad que aprobó la solicitud del Suscriptor de Certificado.

La suspensión de certificados no es practicada por la Autoridad Certificadora, y en su lugar es llevada a cabo la revocación del Certificado.

3.3 Sello de tiempo

3.3.1 Token de sello de tiempo

La TSA de E-Sign implementa medidas para asegurar que los tokens de sellado de tiempo son emitidos en forma segura e incluyen un identificador único de política (OID), valores de fecha y hora proveniente de una fuente confiable de tiempo UTC sincronizado en la precisión definida en esta política.

Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el suscriptor para que sea sellado con el sello de tiempo
- Un identificador para la política de marca de tiempo
- Un número serial único que será usado para ordenar los TSTs así como para identificar un sello de tiempo específico.
- La firma electrónica que ha sido generada con una llave privada que es usada sólo para la firma de los sellos de tiempo.
- La identificación de la TSA y de la TSU.

La TSA de E-Sign define todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

3.3.2 Sincronización de los relojes con UTC

La TSA de E-Sign utiliza una fuente fiable de tiempo, mediante un servidor basado en el protocolo NTP que sincronice con el tiempo UTC a través de una red de satélites GPS o en caso excepcional contra múltiples fuentes que incluyen el "National Measurement Institute"; lo anterior con una desviación máxima de 1 segundo.

En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la TSA.

Cuando sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempo o por cualquiera de las fuentes fiables mencionadas anteriormente, el token de sello de tiempo no será emitido, hasta contar con un tiempo correcto. Además, Para la administración del reloj de la TSU requiere de un quórum de 3 de 8 tarjetas.

Para mayor detalle sobre la sincronización de los relojes, remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de E-Sign.

3.3.3 Procedimiento de registro del Suscriptor

Una Organización que contrata alguno de los servicios de firma de E-Sign puede optar a contratar también el servicio TSA E-Sign. De este modo E-Sign identifica y autentifica a la Organización como parte del proceso de contrato del servicio de firma y ésta se convierte en Suscriptor del servicio TSA.

Los usuarios finales autorizados por la Organización son registrados mediante un identificador de usuario y una contraseña que les permite el acceso al servicio de firma, y, a través de éste, al servicio de TSA.

Sólo las organizaciones usuarias de alguno de los servicios de firma de E-Sign pueden optar a ser Suscriptores del servicio de TSA.

3.3.4 Procedimiento de validación del Suscriptor

Una Organización que contrata alguno de los servicios de firma de E-Sign puede optar a contratar también el servicio TSA E-Sign. De este modo E-Sign identifica y autentifica a la Organización como parte del proceso de contrato del servicio de firma y ésta se convierte en Suscriptor del servicio TSA.

Para llevar a cabo la validación del suscriptor de nuestros servicios de TSA, la parte interesada deberá enviar la siguiente documentación:

- RUT de la empresa
- Razón social
- Nombre del representante legal
- RUT del representante legal

Con el fin de verificar la veracidad de esta información, los datos serán validados en los siguientes portales:

- Registro de Empresas y Sociedades
- Servicio de Impuestos Internos (SII)
- Registro Civil

Una vez validados los antecedentes, se procederá con la elaboración del contrato, el cual deberá ser firmado por el representante legal del suscriptor

3.4 Gestión y operación de la TSA

3.4.1 Gestión de la seguridad

La TSA de E-Sign desarrollará una administración activa de la seguridad a través de un Sistema de Gestión de Seguridad de la Información (SGSI), el que considera las mejores prácticas y estándares de la industria. El estándar que aplica la TSA de E-Sign como parte de

su SGSI es el estándar ISO 27001 así como los controles definidos en la ISO 27002. En particular:

- a) E-Sign declara que su TSA es responsable por todos los aspectos asociados a la provisión de servicios de sello de tiempo y no subcontrata los servicios de sello de tiempo.
- b) Todo su personal tiene acceso a sus prácticas y políticas de sello de tiempo.
- c) Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
- d) E-Sign cuenta con un Comité de seguridad de la información, un oficial de seguridad, un oficial adjunto y una oficina técnica, los que en su conjunto velan por el cumplimiento del plan anual definido por el SGSI.
- e) E-Sign define que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.
- f) E-Sign no subcontrata los servicios de sello de tiempo.

3.4.2 Gestión y clasificación de activos

Los activos de la TSA de E-Sign reciben un apropiado nivel de protección. Para ello la TSA de E-Sign realiza anualmente un análisis de riesgos siguiendo una metodología y herramientas basadas en la norma ISO 27001, para el cual se hace un levantamiento de los activos.

Todo lo anterior se encuentra documentado y clasificado de uso interno, siendo esta documentación revisada de forma periódica en auditorias.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de E-Sign.

3.4.3 Seguridad del personal

3.4.3.1 Requerimientos de antecedentes y experiencia

E-Sign requiere que todo el personal asociado a la TSA cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, lo cual incluye:

- Conocimientos y formación sobre entornos de certificación digital y sellos de tiempo.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la TSA.

3.4.3.2 Comprobación de antecedentes

En E-Sign se realiza una comprobación de los antecedentes, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign antes de asignar un rol de confianza.

3.4.3.3 Roles de confianza

E-Sign define que sus roles de confianza al cumplir su función de TSA corresponden a:

- ☐ Oficial de seguridad
- ☐ SysAdmin.
- ☐ Controller.

3.4.3.4 Requerimientos de formación y reentrenamiento

E-Sign considera para el personal asociado a la TSA, la formación y reentrenamiento a través de un plan anual de capacitación. Esto de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

3.4.3.5 Sanciones

E-Sign informa y entrega al momento del ingreso, a cada empleado el Reglamento Interno, el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones.

3.4.3.6 Requerimientos de contratación

Como parte de los requerimientos de contratación, todo trabajador de E-Sign debe firmar un acuerdo de confidencialidad (NDA), tal como es especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

3.4.3.7 Documentación entregada al personal

El personal de la TSA tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación.
- Políticas de certificación.
- Política de privacidad.
- Política de Seguridad de la Información.
- Organigrama y funciones del personal.

3.4.3.8 Finalización de contratos

La finalización de contratos cuenta con un procedimiento en el cual se suprimen los privilegios de acceso del individuo a las instalaciones e información de la organización, a excepción de

la considerada pública, una vez informado el individuo de su salida y de su pérdida de privilegios, se verifica la devolución del material entregado y se les informa al resto de la organización, a los proveedores y entidades externas a E-Sign de que el individuo ya no representa a la TSA de E-Sign.

3.4.4 Seguridad física y ambiental

La seguridad física y ambiental se detalla en la política de seguridad, dando cumplimiento a la norma ISO 27001 en la cual se basa. Los servicios de E-Sign están de acuerdo a las prácticas de certificación de Sello de tiempo, como también a la norma ETSI TS 102.023.

3.4.4.1 Emisión de sellos de tiempo, así como su administración

La Emisión de sellos de tiempo, es realizada por el personal autorizado, así como su administración será de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign, punto 3.1.1, ello a fin de evitar daños, perdidas, interrupción o compromiso de los activos críticos de la TSA.

3.4.4.2 Control de los módulos criptográficos

El control de los módulos criptográficos se llevarán a cabo para evitar la pérdida de información y están de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign, punto 3.1.1.

3.4.4.3 Controles físicos y ambientales

3.4.4.3.1 Data Center y Oficinas Centrales

Los sistemas e infraestructura del Servicio de Emisión de sellos, se encuentran alojados en un sitio principal y uno secundario. Las características generales comprenden una Zonificación en Alta Criticidad y una Zona de Media Criticidad.

Ambos cuentan con medidas que mantienen un perímetro de seguridad el cual restringe el acceso sólo a personal autorizado.

Respecto a la casa matriz de E-Sign ella cuenta con accesos vigilados, área de recepción así como control de visitas y acceso biométrico del personal.

a) **Seguridad Física Data Center**

E-Sign opera en dos Datacenter seguros y confiables que cuentan con niveles de protección y solidez de la construcción y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos Datacenter cuentan con controles definidos, para proteger los elementos que forman parte de la solución de E-Sign, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

b) **Sistema de Energía Eléctrica**

E-Sign cuenta en los sitios con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación, por largos periodos de tiempo. Para esto cuenta con energía redundante a través de UPS y grupos electrógenos.

Para un mayor detalle sobre el Sistema de Energía Eléctrica se encuentra especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

c) **Sistema de Climatización**

El Sistema Climatización en ambos sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos y en caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

Para mayor detalle sobre control ambiental remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

d) **Sistema de Extinción y Control de Incendios**

El Sistema de Extinción y Control de Incendios cuenta con el suministro e instalación de un sistema de protección contra incendios sobre la base de detección temprana, que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática.

e) **Telecomunicaciones**

Las especificaciones respecto a las Telecomunicaciones se basan en una plataforma robusta, segura y escalable, utilizando para ello los servicios WAN, estos servicios provistos por los principales carriers del país que nos aseguran redes confiables y con tecnología de última generación.

Para mayor información remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

3.4.5 Gestión de las operaciones

La TSA de E-Sign establece que su sistema y componentes son fiables, ya que se encuentran operados de manera correcta con un riesgo mínimo de falla en la emisión, el control de sellos de tiempo, el manejo correcto de los medios, el control y planificación de los sistemas, control y reporte de incidentes.

Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado. Respecto al manejo de medios y seguridad, E-Sign declara un apropiado tratamiento de sus activos a través de la realización de un análisis anual de riesgo riesgos basados en la norma ISO 27001, el cual genera como parte de su preparación la lista de activos de la TSA, su nivel de protección, así como los procedimientos adicionales a seguir para minimizar su riesgo.

Además, considera los siguientes roles de confianza que manejan las operaciones:

- SysAdmin.
- Oficial de Seguridad.
- Jefe PostVenta.
- Controller.

En cuanto a la Planificación de la capacidad, se debe mantener un manejo de la capacidad para la demanda, monitoreando y proyectando de acuerdo a los futuros requerimientos, de manera que la capacidad de proceso como de almacenamiento siempre sean las adecuadas. Para efectuar esto, E-Sign cuenta con un procedimiento formal de gestión de capacidad de sus instalaciones.

Respecto a los procedimientos operacionales y responsabilidades, E-Sign cuenta con la operación del servicio de Sello de Tiempo de la TSA; siendo éstas desarrolladas por el personal confiable.

3.4.6 Gestión de acceso a los sistemas

La TSA de E-Sign, asegura que el acceso a su sistema (hardware, software y datos) se encuentra protegido compartiendo las medidas de seguridad física que dan protección al sistema en un entorno de confianza y está limitado al personal autorizado.

Los administradores de E-Sign realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA. Es por ello que se cuenta con Cortafuegos, Administración de usuarios, Restricciones de acceso a la información y sistemas, un control apropiado del personal autorizado, Logs de las operaciones. Adicionalmente, los componentes de la red local se mantienen en Datacenters bajo ambiente seguro y con una auditoría periódica.

3.4.7 Mantenimiento e Implementación de sistemas de confianza

En la TSA de E-Sign se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello que establece el monitoreo y registrar cada cambio en los sistemas. Para cualquier cambio en los sistemas se lleva a cabo un análisis de requerimientos de seguridad, procedimientos de control de cambio para nuevas versiones y la generación de las llaves siempre se lleva a cabo dentro del entorno de confianza, por personal critico autorizado.

3.4.8 Cumplimiento de requerimientos legales

E-Sign como Autoridad de sello de tiempo, actúa en conformidad con la Ley N° 19.799 y su reglamento, así como la Ley N° 19.628 relativas a la protección de datos personales, la ley N° 19.496 sobre los derechos de los consumidores y las directrices técnicas establecidas por los organismos calificadores (ETSI, ISO, RFC, etc.). Además, su gestión y operación de servicios se encuentra regulada por la Entidad Acreditadora del Ministerio de Economía y sus Guías de Acreditación.

E-Sign cuenta con procedimientos de control y de seguridad de la información, a objeto de proteger la información personal de sus suscriptores de divulgación, todo ello ante un procesamiento no autorizado o ilegal, así como ante la destrucción o daño de dicha información ya sea de manera accidental o intencional. A menos que sea solicitada por él mismo o por orden judicial u otro requisito legal.

3.4.9 Confidencialidad y Registro de información relativa a las operaciones del Servicio de sello de tiempo

La TSA de E-Sign debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a registros de la actividad de la TSA que puedan ser utilizados como evidencia y se encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por E-Sign en su sitio web, tal como se detalla en la Declaración de Prácticas de Sello de Tiempo de E-Sign.

Todos los registros concernientes a la operación del servicio de sello de tiempo se encuentran disponibles sólo al suscriptor o en caso que lo solicite una corte a través de un requerimiento legal.

La integridad de esta información es mantenida por la PSC de E-Sign por un periodo de 5 años posterior a la expiración de la validez de la llave usada para la firma por parte de la TSU.

Estos registros incluyen:

- Requerimiento de sello de tiempo
- Sello de tiempo creado
- Eventos relacionados con la administración de la TSA, incluyendo:
 - Registros de eventos correspondientes al ciclo de vida de las llaves de la TSU
 - Registros de eventos correspondientes a los certificados de la TSU
 - Registros relacionados con la sincronización del reloj de usado por la TSU en sus TST
 - Registros asociados a eventos de detección de pérdida de sincronización

Los registros antes mencionados, son almacenados por E-Sign y no son de fácil eliminación o destrucción dentro del periodo de tiempo previamente declarado. A estos registros, sólo tiene acceso el personal autorizado por la TSA de E-Sign.

3.5 Organización

La Autoridad de Sellado de Tiempo es un servicio adicional que se encuentra soportada por la PSC de E-Sign, la cual se encuentra acreditada en su operación por la Entidad Acreditadora del Ministerio de Economía.

La TSA de E-Sign cumple con:

- Las políticas y los procedimientos bajo los que opera no incluyen cláusulas discriminatorias.
- E-Sign provee su servicio de sello de tiempo a cualquier suscriptor que cumpla y este de acuerdo con las obligaciones declaradas en las prácticas y políticas de sello de tiempo.
- para la provisión de sus servicios E-Sign cumple con la normativa legal vigente en Chile.
- Cuenta con un seguro de responsabilidad civil, de la Ley 19799, artículo 14, ante daños o perjuicios producto de su operación.
- E-Sign es anualmente auditada respecto sus estados financieros y el cumplimiento de la normativa vigente.
- E-Sign como PSC certificada por el Ministerio de Economía, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal.
- ante un conflicto con un cliente, el cual no pueda ser resuelto favorablemente por las partes, E-Sign acudirá a los Tribunales de Justicia a modo que ellos actúen como árbitro arbitrador del conflicto.
- E-Sign mantiene en su repositorio documental todo contrato, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

4. Consideraciones de seguridad

Se debe tener presente que, al momento del chequeo de validez de los TST, por parte de un tercero que confía, el certificado de firma de la TSU debe ser válido y no se encuentra revocado, ya que la validez del TST es cierta sólo para el momento en que se efectúa dicho chequeo, pues en un tiempo posterior puede existir un compromiso de la llave privada de la TSU de E-Sign que invalida la llave de firma y por ende al TST emitido.

5. Revisión y aprobación del documento

5.1 Revisión

Este documento es revisado anualmente a fin de verificar su validez y eficacia, o en un plazo menor en caso de producirse cambios significativos que ameriten su revisión de acuerdo al marco regulatorio, comercial, legal o técnico.

5.2 Aprobación

Este documento, así como las modificaciones que él sufra deben ser aprobados por el comité de seguridad, a fin de que sea incorporado como la nueva versión vigente al sistema de gestión documental y para posteriormente proceder a su difusión con los colaboradores y partes externas pertinentes.

6. Normativa Técnica

La normativa técnica que se tuvo a la vista para elaborar este documento, es la siguiente:

- Ley N°19.799 y su reglamento
- ISO/IEC 9594-8
- RFC 3161
- XadES
- ISO/IEC 27.001
- ISO/IEC 18014-1:2008
- ISO/IEC 18014-2:2009
- ISO/IEC 18014-3:2009
- FIPS 140-2
- ETSI TS 102 042
- ETSI TS 102 023
- ANSI X9.95-2012
- RFC 3628
- RFC 5816