POLÍTICA DE SELLO DE TIEMPO

e-certchile

CAMARA DE COMERCIO DE SANTIAGO

ÍNDICE

1. Introducción

En este documento se presenta la Política de Sello de Tiempo asociada a la emisión de sellos de tiempo del PSC. Estas son una definición de las reglas a las que se deben ajustar los procedimientos o prácticas que nuestro PSC declara cumplir en la presentación 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 time-stamping, al momento de la confirmación de vigencia de la llave privada de la TSA, que es a través de la CRL o 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 definen además los roles, responsabilidades y relaciones entre el usuario final y nuestro PSC, siendo la declaración de Prácticas de Sello de Tiempo un complemento a este documento.

Esta declaración de Políticas de Sello de Tiempo constituye el marco general de normas aplicables a toda la autoridad certificadora, cuando ella actúa como autoridad de sello de tiempo (TSA). Sin embargo, el detalle aplicable a cada sello que se emita, se establece en este documento y se encuentra disponible, en forma pública, en nuestra página www.e-certchile.cl .

Cabe señalar que la presente Política de Sello de Tiempo, se ha generado siguiendo las especificaciones del documento RFC 3628 “Policiy 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 eldocumento RFC 3161 “Internet X.509 Public Key Infraestructure Time-Stamping Protocol (TSP)”

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 el PSC, desde la gestión de la solicitud de un sello de tiempo, la obtención de un sello de 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 nuestro PSC.

1.2. Alcance

El alcance de la Política de Sello de Tiempo define las normas y condiciones de los servicios que se prestan para la emisión de los mismos en su actuar como TSA.

1.3. Referencias

La presente Política de Sello de tiempo se ha generado en base a las especificaciones del documento RFC 3628 “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) Policiy Requirements for Time-Stamping Authorities” y el documento RFC 3161 “Internet X.509 Public Key Infraestructure Time-Stamping Protocol (TSP)”.

De manera complementaria a los documentos indicados, se ha utilizado el documento de nombre “Guías de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo” en su versión 1.0, entregados por el Ministerio de Economía, Fomento y Turismo del Gobierno de Chile, como parte del proceso de acreditación de Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo.

1.4. Identificación

El presente documento se denomina “Políticas de Sello de Tiempo”, las que internamente se citan como Políticas de Sello de Tiempo y están registradas con el número único (OID) 31725. Este número identifica únicamente a nuestro PSC en un contexto global, el cual está registrado en la Internet Assigned Number Authority (IANA).

1.5. Comunidad de usuarios y aplicabilidad

Esta Política se aplica a todos los sellos de tiempo emitidos por e-certchile.

Entidades.

- Certificador. Son las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorgan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. En caso de que deseen acreditarse deberán encontrarse domiciliadas en Chile y seguir el procedimiento de acreditación que señala el Título V de la ley y desarrolla el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.
- e-certchile se encuentra acreditado por la Entidad Acreditadora desde el año 2003, mediante la Resolución Exenta Nº 317, de la Subsecretaría de Economía.

- Autoridad de Sellado de Tiempo. Es la organización que opera y controla el funcionamiento de la sincronización del tiempo, emisión y otros procesos específicos de sellado de tiempo de un documento o datos, teniendo como principal obligación la provisión de los servicios de sellado de tiempo.
- e-certchile se encuentra acreditado por la Entidad Acreditadora desde el año 2016, mediante la Resolución Exenta Nº 3779, de la Subsecretaría de Economía.
- Suscriptor. Son entidades que pueden ser individuos, empresas, sistemas y otro tipo, que solicitan la emisión del sello de tiempo.
- Tercera Parte que Confía. Son entidades que pueden ser individuos, empresas, sistemas u otro tipo, que son receptores de un sello de tiempo generado por la autoridad de sellado de tiempo.
- Una tercera parte que confía no es necesariamente un suscriptor, puede ser cualquier individuo, empresas, sistemas y otro tipo que libre y voluntariamente decide confiar en un sello de tiempo.
- Para realizar la verificación de los sellos de tiempo emitidos por la autoridad de sellado de tiempo la parte que confía debe contar con mecanismos que le permitan validar si se trata de un sello de tiempo auténtico.
- Entidad Acreditadora: La Subsecretaría de Economía y Empresas de Menor Tamaño en virtud de lo dispuesto en la Ley 19.799.

1.6. Procedimiento de registro

Los usuarios que utilizan el servicio de TSA, se controlan a través de su ip pública, por lo que el procedimiento de registro conta de lo siguiente:

- Validación del usuario en la plataforma
- Notificación de ip pública
- Seguimiento de las transacciones

1.7. Aplicabilidad de los sellos de tiempo.

Los sellos de tiempo emitidos por la autoridad de sellado de tiempo se utilizarán únicamente conforme a la función y finalidad que están establecidas en esta Práctica de Sellado de Tiempo e-certchile (CPST e-certhile), en concordancia con la normativa vigente para garantizar el no repudio.

El uso de los sellos de tiempo está limitado a demostrar que un documento o una serie de datos han existido y no han sido modificados desde un instante de tiempo específico y confiable.

Usos prohibidos. Los sellos de tiempo emitidos por autoridad se dé sellado de tiempo se utilizarán únicamente conforme a la función y finalidad que se tenga establecida en la presente Práctica de Sellado e-certchile (CPST e-certchile) de tiempo y de acuerdo con la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

1.8. Estructuras de los sellos de tiempo

La estructura de los sellos de tiempo generados, se ajustan al documento RFC 3161 “Internet

La estructura de los sellos de tiempo generados por autoridad de sellado de tiempo se ajusta al documento RFC 3161 “Internet X.509 Public Key Insfraestcruture Time Stamping Protocol (TSP)”.

La certificadora referencia el OID de la Práctica de Sellado de Tiempo e-certchile (CPST e-certchile) en cada uno de los sellos de tiempo.

1.9. Detalles de contacto.

Dirección postal: Monjitas 392 Piso 17, comuna y ciudad de Santiago de Chile.

Correo electrónico: sclientes@e-certchile.cl

Teléfono: (+56 2) 2360 7175

Mesa ayuda certificación: (+56 2) 2818 5760

Sucursales:

- Enrique Mac-Iver 410, Local 1 comuna y ciudad de Santiago de Chile:

Lunes a Jueves: 09:00 – 17:30 hrs.

Viernes 09:00 – 14:30 hrs.

- Av. Nueva Providencia 2260, Local 81, comuna de Providencia y ciudad de Santiago de Chile

Lunes a Jueves: 09:00 – 17:30 hrs.

Viernes 09:00 – 14:30 hrs.

a) Definiciones y Acrónimos

El alcance de las definiciones del documento de Prácticas de Certificación de sello de tiempo se entenderá como:

- Parte que confía: Receptor del token o firma 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.
- Subscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de
- Sello de Tiempo y el cual implícita o explícitamente e-certchile las políticas de uso de este servicio. 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 en un determinado instante.
- Token de sellado de tiempo: Dispositivo de datos empleado a 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 token de sellado de tiempo deben emitirse de acuerdo al RFC 3161 “Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)”.
- Autoridad de Sellado 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).
- Sistema de TSA: Conjunto de elementos organizados para soportar los servicios de sellado de tiempo.
- 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.
- Unidad de sellado de tiempo (TSU por sus siglas en inglés, “time-stamping unit”): Es el conjunto de hardware y software que es gestionado como una unidad y que tiene un token de sellado de tiempo firmado por una llave privada de la TSA.
- Tiempo Universal Coordinado (UTC por sus siglas en inglés Universal Time Coordinated): 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.

- Declaración de Prácticas de sellado de tiempo: Declaración de las Prácticas que una autoridad de sellado de tiempo emplea en la emisión de los tokens de sellado de tiempo.

b) Acrónimos

- TSA: Autoridad de sellado de tiempo
- TSS: Servicio de sellado de tiempo
- TST: Token de sello de tiempo
- UTC: Tiempo universal coordinado
- TSU: Unidad de sello de tiempo

2. Obligaciones y Responsabilidades

2.1. Obligaciones de la TSA

e-certchile.

e-certchile en su calidad de autoridad de sellado de tiempo se obliga a:

- Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los sellos de tiempo en los términos establecidos en la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.
- Cumplir y respetar los procedimientos establecidos en esta “CPST e-certchile”.
- Cumplir con todas las otras obligaciones establecidas en la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éste.
- Garantizar el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC puede tener una desviación máxima de 1 segundo.
- Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, así como, también del hardware criptográfico.
- Mantener un identificador único para cada sello de tiempo emitido, así como incluir una referencia a la política bajo la cual fue emitido.
- Mantener sincronizado el reloj de la unidad de sellado de tiempo con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.
- Mantener los controles de seguridad física, de procedimiento y personales definidos para el sellado de tiempo.

- Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de acuerdo con la información conocida en el momento de su emisión.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.
- Garantizar mediante revisiones y auditorias que todos los requerimientos de la autoridad de sellado de tiempo cumplen con los controles requeridos por la legislación aplicable, la Práctica de Sellado de Tiempo (CPST e-certchile) y los procedimientos internos.
- Informar:
- El algoritmo de hash utilizado en lo sellos de tiempo.
- La precisión del tiempo utilizado como parte del proceso de certificación de los sellos de tiempo.
- Los mecanismos de verificación de los tokens emitidos por e-certchile.
- El período de permanencia de los logs que maneja la autoridad de sellado de tiempo.
- Mantener www.e-certchile.cl con información para el público sobre los servicios de e-certchile.

Obligaciones del suscriptor.

- Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la autoridad de sellado de tiempo y su periodo de validez.
- Verificar que la llave de la autoridad de sellado de tiempo no ha sido comprometida hasta el momento de la verificación, utilizando para ello la CRL publicada por e- certchile.
- En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la autoridad de sellado de tiempo verificar que el número de serie del certificado no se encuentra en la CRL y que era válido al momento en que se generó el sello de tiempo.
- Conocer el propósito y alcance de los sellos de tiempo emitidos por e-certchile.
- Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado o a los sellos de tiempo emitidos, lo cual debe ser considerado como causa de revocación de éste.
- Conocer y aceptar los términos, condiciones y límites contenidos en estas “CPST e-certchile”.

2.2. Responsabilidades

e-certchile.

- Emitir los certificados de sellado de tiempo cumpliendo todas las exigencias establecidas en estas “CPST e-certchile”.
- Que la información incluida o incorporada por referencia en el sello de tiempo sea exacta.
- La aplicación correcta del procedimiento empleado.
- e-certchile no será responsable por ningún daño o perjuicio actual o futuro, directo o indirecto, previsto o imprevisto, emergente o lucro cesante, pérdida de datos u otros, debidos, ocasionados o conectados con el uso indebido, no uso, uso tardío de certificados, aun cuando e-certchile hubiera sido advertido de la posibilidad de producción de tales daños.
- Limitación de responsabilidad de e-certchile.
- Las responsabilidades que afectan la operación de la autoridad de sellado de tiempo se encuentran limitadas a lo establecido en el artículo 14 de la Ley 19.799.
- En todo caso, la responsabilidad de autoridad de sellado de tiempo cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a e-certchile, quedará limitada como máximo al monto correspondiente a UF 5.000 (cinco mil unidades de fomento), monto asegurado de conformidad con lo dispuesto en el artículo 14 de la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.
- La actividad de la autoridad de sellado de tiempo se encuentra limitada al ciclo de vida del certificado de sellado de tiempo.

2.3. Fuerza mayor

e-certchile no será responsable por daños, pérdidas o perjuicios que provengan de incumplimientos en el desarrollo de la actividad de certificación de firma electrónica y que sean atribuibles a circunstancias constitutivas de caso fortuito o fuerza mayor.

Las obligaciones de e-certchile afectadas por el caso fortuito o la fuerza mayor se suspenderán por el período de tiempo que dure el hecho que lo motivó.

Para los efectos de esta “CPST e-certchile” se entenderá por caso fortuito o fuerza mayor lo dispuesto en el artículo 45 del Código Civil, lo que incluye guerras, desastres naturales, paros,

huelgas o suspensión de laborales del personal de e-certchile o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

3. Requerimientos en prácticas de la TSA

3.1. Prácticas y declaraciones de divulgación

a) Declaraciones de prácticas de TSA

La información establecida en este documento se completa con el documento de prácticas de sello de tiempo que detalla la implementación de los controles que son necesarios para cumplir con esta política de sellado de tiempo, así como políticas, normativas, procedimientos, ya sean estos operacionales y/o técnicos para uso interno de e-certchile, que garantizan la fiabilidad y la confianza del servicio de sellos de tiempo.

En particular e-certchile, como TSA establece que ha trabajado en:

Una determinación de activos y riesgo asociado a c/u 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, se detallan 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 incluyendo las políticas y prácticas de sello de tiempo aplicables.

Para un mayor detalle, remítase a lo especificado en la Prácticas de sello de tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

b) Declaración de divulgación de TSA

Nuestra TSA entrega como parte de estas políticas su información de contacto a los suscriptores y terceros, da a conocer la política que rige su operación incluyendo en esta última: 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 participen 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, Fomento y Turismo.

3.2. Gestión de ciclo de vida de las llaves

a) Generación de llave de la TSU

El módulo criptográfico adoptado por e-certchile, es capaz de generar llaves en base al algoritmo de encriptación de llave pública SHA2RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS_COP.1 y que se evidencia en el documento asociado al proceso TB01. La TSA cuenta para la generación de los TST solicitados, con un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3.

Respecto al personal que participa en la generación de la llave, por parte de la CA, y que es usada por la TSU, se declara que ellos pertenecen a los roles de confianza definidos y cualquier actividad a realizar sobre el módulo HSM requiere de un quórum 2 de 4 personas. Se declara que satisface los requerimientos identificados en CEN Workshop Agreement 14167-2 [CWA 14167-2] o ISO 15408 al cumplir con la ETSI TS 102 042 que fue la que dio origen al ciclo de vida de la llave aquí descrito. Para mayor detalle remítase a la Declaración de Prácticas de sello de tiempo.

b) Protección de la llave privada de la TSU

Nuestro PSC 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 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. Declaramos cumplir con el documento "CEN Workshop Agreement 14167-2 [CWA 14167-2]" o ISO 15408 en lo correspondiente al ciclo de vida de su llave criptográfica, realizando la implantación de estos controles de acuerdo con la norma ETSI TS 102042. En cuanto a los respaldos, ellos sólo son recuperados por el personal con roles de confianza y bajo un ambiente seguro, de acuerdo a lo especificado en la Declaración de Prácticas de sello de tiempo.

c) Distribución de la llave pública

El certificado de la TSA incluye su clave pública, la cual se distribuye a través de la página web de e-certchile. Este certificado digital utilizado por la TSA es generado por la PSC de e-certchile, de acuerdo a las políticas y prácticas de certificación inspeccionadas por el Ministerio de Economía, Fomento y Turismo para esta PKI, La distribución se basa en establecer la confianza con la TSA de acuerdo al modelo de confianza definido por e-certchile asegurando la integridad y autenticidad de la firma de la TSU. El modelo de confianza definido puede ser revisado en mayor detalle en el documento asociado al proceso TB04 del proceso de firma electrónica avanzada.

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de sello de tiempo.

d) Remisión de llaves de la TSU

Por motivo de seguridad y evitar el repudio a un certificado, e-certchile como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo con 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, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

e) Término del ciclo de vida de la llave del TSU

La llave privada de la TSU debe ser reemplazada al momento de su expiración o ante un evento de seguridad que vulnere dicha llave. La TSU de e-certchile rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida al igual que sus copias de respaldo, a fin de que su clave privada no pueda ser recuperada.

Detalle del proceso de término del ciclo de vida de la llave de la TSU se encuentra especificado en la Declaración de Prácticas de sello de tiempo.

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-certchile y terceros involucrados deben cumplir la normativa de dicho ciclo que a continuación se detalla:

- El Hardware no es intervenido durante su viaje o almacenamiento: Los HSM del PSC cuentan con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión y en caso de 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 con el quórum definido.

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

- Administración del Hardware Criptográfico: El equipo HSM que será utilizado por e-certchile 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, se dispone de procedimientos asociados para el manejo de los HSM por el personal de confianza, utilizando tarjetas de administración y de operación, como también definiendo un quórum 2 de 4 para la administración del ambiente completo y seguro. Lo anterior se encuentra clasificado de uso interno y revisado de forma periódica por el auditor. Respecto a las características técnicas los equipos HSM cumplen con el estándar FIPS-140 2 nivel 3. Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo.

4. Sello de tiempo

4.1. Token de Sello de Tiempo

La TSA garantiza 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.

4.2. Sincronización de los relojes con UTC

La TSA de e-certchile declara utilizar 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 SHOA.

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

5. Gestión de la TSA y operaciones

5.1. Gestión de la Seguridad

La TSA 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. En particular:

- e-certchile 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.
- Todo su personal tiene acceso a sus prácticas y políticas de sello de tiempo.
- Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
- e-certchile cuenta con un Comité de seguridad de la información, un oficial de seguridad, y apoyo técnico de una empresa dedicada a la Seguridad de la Información, los que en su conjunto velan por el cumplimiento del plan anual definido por el SGSI.
- e-certchile declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.
- e-certchile no subcontrata los servicios de sello de tiempo.
- Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo.

6. Gestión y clasificación de activos

Los activos de la TSA de e-certchile reciben un apropiado nivel de protección. Para ello la TSA de e-certchile realiza anualmente un análisis de riesgos 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-certchile.

7. Seguridad del personal

7.1. Requerimientos de antecedentes y experiencia

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.2. Comprobación de antecedentes

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.3. Roles de Confianza

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.4. Requerimientos de formación y reentrenamiento

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.5. Frecuencia de rotación de tareas

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.6. Sanciones

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.7. Requerimientos de contratación

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.8. Documentación entregada al personal

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.9. Control de Cumplimiento

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

7.10. Finalización de Contratos

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

8. Seguridad Física y ambiental

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

9. 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-certchile, ello a fin de evitar daños, pérdidas, interrupción o compromiso de los activos críticos de la TSA.

10. Control de módulos criptográficos

El control de los módulos criptográficos se llevará a cabo para evitar la pérdida de información y están de acuerdo a lo especificado en la Prácticas de Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo y el documento de “Gestión del ciclo de vida de las llaves”.

11. Controles físicos y ambientales

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

12. Gestión de las operaciones

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo

13. Gestión de acceso a los sistemas

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

Los administradores de e-certchile 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 Data Centers bajo ambiente seguro y con una auditoría periódica.

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo.

14. Mantenimiento e implementación de sistemas de confianza

En la TSA de e-certchile se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello que se establece monitorear 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.

15. Compromiso de los servicios de TSA

La TSA de e-certchile declara que ante cualquier compromiso de los servicios de sello de tiempo, se harán efectivos los procedimientos correspondientes al plan de continuidad de e-certchile. Si este compromiso afecta a la llave de firma de la TSU o pérdida de precisión de su reloj, se declarará un evento de seguridad y se informará directamente o a través de su sitio web a sus suscriptores y terceros que en ella confía, dicha información del evento. Ante los eventos antes mencionados, la TSA de e-certchile no emitirá nuevos TST hasta superar el compromiso declarado Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo.

16. Cese de una TSA

En el momento en que e-certchile vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a comunicar del cese de sus funciones con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo ya sean suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas. Además, la TSA procederá revocar los certificados de la TSU y transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. En el caso de las claves y copias de respaldo de la TSA de e- certchile, estas deben ser borradas y destruidas, de manera que operaciones. Adicionalmente, los componentes de la red local se mantienen en Data Centers bajo ambiente seguro y con una auditoría periódica estas no puedan ser recuperadas, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo.

En el procedimiento para el término de actividades, se dispondrá de los costos necesarios para los requerimientos indicados.

17. Cumplimiento de requerimientos legales

De conformidad con la Práctica Sellado de Tiempo CPST e-certchile 000T-PO-02-I3-D1 Práctica de Sellado de Tiempo.

18. Registro de información relativa a las operaciones del servicio de sello de tiempo

La TSA de e-certchile debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a la información personal de los suscriptores que se ha recolectado y se encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por e- certchile en su sitio web, tal como se detalla en la Declaración de Prácticas de Sello de Tiempo de e-certchile.

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

Los registros antes mencionados, son almacenados por e-certchile 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 PSC.

19. Organización

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

La TSA de e-certchile cumple con: Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias. e-certchile 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. e- certchile para la provisión de sus servicios cumple con la normativa legal vigente en Chile. Cuenta con un seguro de responsabilidad civil, de la Ley N°19.799, articulo 14, ante daños o perjuicios producto de su operación. e-certchile es anualmente auditada respecto sus estados financieros y el cumplimiento de la normativa vigente. e-certchile como PSC certificada por el Ministerio de Economía, Fomento y Turismo, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal.

e-certchile ante un conflicto con un cliente, el cual no pueda ser resuelto favorablemente por las partes, utilizará los Tribunales de Justicia a modo que ellos actúen como árbitro arbitrador del

conflicto. e-certchile mantiene en su repositorio documental todo contrato, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

20. 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-certchile que invalida la llave de firma y por ende al TST emitido. La TSA de e-certchile asegura que hash incluido en su TST corresponde al enviado por el suscriptor en su request.

Para mayor detalle de las consideraciones de seguridad, remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo.

NORMA(S) QUE APLICA(N)	
Norma	**Referencia Normativa**
ISO 9001:2015	5.2 Política | 8.2.2 Determinación de los requisitos relacionados con los productos y servicios
ISO 27001:2013	5.2 Política
Guía de Acreditación (Minecon) FEA	N/A
Guía de Acreditación (Minecon) BIO	N/A
Guía de Acreditación (Minecon) TSA	PO01 Política de certificados de Sello de tiempo / PO02 Declaración de prácticas de Sello de tiempo

CONTROL DE CAMBIOS		
N° DE VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIOS**
0	2020 /07	Creación del documento, se recomienda su lectura completa.