

# **PRACTICAS DE CERTIFICACIÓN DE SELLO DE TIEMPO**

**E-SIGN S.A.**

Fecha: Mayo 2025

|                                                                                                                  |                                                                                  |                     |              |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|--------------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |              |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Octubre 2023 |
|                                                                                                                  |                                                                                  | Página              | 2 de 34      |

## Tabla de contenido

|       |                                                                          |    |
|-------|--------------------------------------------------------------------------|----|
| 1     | INTRODUCCIÓN.....                                                        | 4  |
| 1.1   | Alcance.....                                                             | 4  |
| 1.2   | Referencias .....                                                        | 4  |
| 1.3   | Organización que Administra el Documento .....                           | 4  |
| 1.4   | Contacto.....                                                            | 5  |
| 1.5   | Procedimiento de aprobación de las CPS.....                              | 5  |
| 1.6   | Identificación.....                                                      | 5  |
| 1.7   | Conceptos generales.....                                                 | 5  |
| 1.7.1 | Servicios de Sellado de Tiempo .....                                     | 5  |
| 1.7.2 | Autoridad de Sellado de Tiempo .....                                     | 5  |
| 1.7.3 | Suscriptores .....                                                       | 6  |
| 1.7.4 | Partes que confían.....                                                  | 6  |
| 1.7.5 | Otros participantes .....                                                | 6  |
| 1.7.6 | Entidad Acreditadora.....                                                | 6  |
| 1.7.7 | Uso de sellos de tiempo .....                                            | 7  |
| 1.8   | Política de sellado de tiempo y declaración de prácticas de la TSA ..... | 7  |
| 1.8.1 | Propósito .....                                                          | 7  |
| 1.8.2 | Nivel de especificidad.....                                              | 7  |
| 1.8.3 | Enfoque .....                                                            | 7  |
| 1.9   | Cumplimiento .....                                                       | 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 .....                      | 9  |
| 2.2   | Obligaciones del suscriptor .....                                        | 9  |
| 2.3   | Obligaciones de partes que confían.....                                  | 10 |
| 2.4   | Responsabilidades.....                                                   | 10 |
| 2.4.1 | Responsabilidades Legales .....                                          | 10 |
| 2.4.2 | Responsabilidades Generales .....                                        | 10 |
| 2.4.3 | Fuerza Mayor.....                                                        | 11 |
| 2.4.4 | Resolución de Conflictos.....                                            | 11 |
| 3     | Requerimientos en prácticas de la TSA .....                              | 12 |
| 3.1   | Declaraciones de Prácticas y de divulgación .....                        | 12 |
| 3.1.1 | Declaración de prácticas de TSA.....                                     | 12 |

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |              |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|--------------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |              |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Octubre 2023 |
|                                                                                                                  |                                                                                  | Página              | 3 de 34      |

|        |                                                                                                        |    |
|--------|--------------------------------------------------------------------------------------------------------|----|
| 3.1.2  | Declaración de divulgación de TSA.....                                                                 | 12 |
| 3.2    | Gestión del ciclo de vida de las llaves .....                                                          | 12 |
| 3.2.1  | Generación de la llave de la TSU .....                                                                 | 12 |
| 3.2.2  | Protección de la llave privada de la TSU.....                                                          | 13 |
| 3.2.3  | Distribución de la llave pública.....                                                                  | 13 |
| 3.2.4  | Reemisión de llaves de la TSU .....                                                                    | 14 |
| 3.2.5  | Termino del ciclo de vida de la llave del TSU.....                                                     | 14 |
| 3.2.6  | Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo..... | 15 |
| 3.2.7  | Requerimientos para el ciclo de vida de los certificados de TSA .....                                  | 16 |
| 3.3    | Sello de tiempo .....                                                                                  | 21 |
| 3.3.1  | Sincronización de los relojes con UTC.....                                                             | 21 |
| 3.4    | Gestión de la TSA y operaciones .....                                                                  | 22 |
| 3.4.1  | Gestión de la seguridad .....                                                                          | 22 |
| 3.4.2  | Gestión y clasificación de activos.....                                                                | 22 |
| 3.4.3  | Seguridad del personal.....                                                                            | 22 |
| 3.4.4  | Seguridad física y ambiental .....                                                                     | 24 |
| 3.4.5  | Gestión de las operaciones.....                                                                        | 27 |
| 3.4.6  | Gestión de acceso a los sistemas.....                                                                  | 28 |
| 3.4.7  | Mantenimiento e implementación de sistemas de confianza .....                                          | 29 |
| 3.4.8  | Compromiso de los servicios de TSA .....                                                               | 29 |
| 3.4.9  | Cese de la TSA .....                                                                                   | 30 |
| 3.4.10 | Cumplimiento de requerimientos legales.....                                                            | 30 |
| 3.4.11 | Registro de información concerniente a las operaciones del servicio de sello de tiempo.....            | 31 |
| 3.5    | Organización .....                                                                                     | 31 |
| 4      | Control de Documento.....                                                                              | 32 |
| 5      | Apéndice Tabla de siglas y definiciones .....                                                          | 32 |

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 4 de 34   |

# 1 INTRODUCCIÓN

En el siguiente documento se presenta la declaración de “Prácticas de sello de tiempo” para la emisión de sello de tiempo de E-Sign, la cual se encuentra publicada en la página web de E-Sign. Estas son una descripción de los procedimientos o prácticas que E-Sign declara convenir en la prestación de sus servicios de sello de tiempo, cuando emite y gestiona en su rol de Autoridad de sello de tiempo (TSA).

Es así como la presente Declaración de Prácticas de sello de tiempo, detalla las normas y condiciones de los servicios de sello de tiempo, que están relacionados con requisitos para la sincronización del tiempo, el sistema de emisión de los sellos de tiempo y otros requerimientos específicos para el proceso. También se describen las medidas de seguridad técnica, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados de sello de tiempo, así como el asegurar que el proceso de certificación es llevado a cabo en un ambiente seguro y que puede dar total confianza a los usuarios de la calidad de los sellos de tiempo y servicios anexos proporcionados por E-Sign.

Esta Declaración de Prácticas de sello de tiempo constituye el marco general de normas aplicables a toda la actividad certificadora E-Sign, actuando como Autoridad de sello de tiempo (TSA), siendo este documento un complemento a las Políticas de Sello de Tiempo de E-Sign.

Cabe indicar que la presente Declaración de Prácticas de sello de tiempo, se ha generado siguiendo 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) Policy Requirements for Time-Stamping Authorities*” y el documento RFC 3161 “*Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)*”.

## 1.1 Alcance

El alcance de la Declaración de Prácticas de Sello de Tiempo detalla las normas y condiciones de los servicios que presta E-Sign para la emisión de los mismos.

## 1.2 Referencias

Los siguientes documentos contienen disposiciones que son relevantes para la Declaración de Prácticas de Sellado de Tiempo de E-Sign:

- IETF RFC 3628 (2003): "Policy Requirements for Time-Stamping Authorities (TSAs)".
- ETSI TS 102 023: “Electronic Signatures and infraestructures (ESI) Policy Requirements for Time-Stamping Authorities”
- IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
- FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

## 1.3 Organización que Administra el Documento

E-Sign S.A.  
Avenida Apoquindo 6550, oficina 501  
Las Condes  
Santiago  
Chile

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> |  | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  |  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  |  | Página              | 5 de 34   |

## 1.4 Contacto

Oficial de Seguridad E-Sign S.A.  
Avenida Apoquindo 6550, Oficina 501  
Las Condes  
Santiago  
Chile  
+56 (2) 24331500  
+56 (2) 24331501  
practicas@esign-la.com

## 1.5 Procedimiento de aprobación de las CPS.

Cualquier nueva versión de una PCST estará sujeta a un procedimiento de aprobación que considera:

Elaboración y aprobación interna de la nueva.

Presentación de las PCST al Directorio de E-SIGN S.A.

Una vez pasada las aprobaciones anteriores, se publicarán las nuevas PCST indicando la fecha de entrada en vigor.

Una vez publicadas las PCST se informará de estas a la Entidad Acreditadora.

## 1.6 Identificación

El presente documento se denomina “Prácticas de Sello de Tiempo de E-Sign”, las que internamente se citan como Prácticas de Sello de Tiempo y están registradas con el Identificador de Objeto (OID) 1.3.6.1.4.1.42346.1.4.3.1. Este documento se encuentra disponible, en forma pública, en [www.esign-la.com/cps](http://www.esign-la.com/cps).

E-Sign tiene el identificador (OID) 1.3.6.1.4.1.42346 el cual está registrado en la Internet Assigned Number Authority (IANA).

## 1.7 Conceptos generales

### 1.7.1 Servicios de Sellado de Tiempo

Los Servicios de Sellado de Tiempo Calificados de E-Sign (TSS) consisten en la administración de la infraestructura y el aprovisionamiento de Tokens de Sellado de Tiempo. Estos servicios son proporcionados por la Autoridad de Sellado de Tiempo de E-Sign (TSA) a los Suscriptores y son una parte integral de la Infraestructura de Clave Pública de E-Sign (PKI). E-Sign ofrece servicios de sellado de tiempo mediante el protocolo de sello de tiempo RFC 3161 a través del transporte HTTP. Cada TST contiene un identificador de política de sellado de tiempo, un número de serie único y un certificado TSU que contiene información de identificación la TSA E-Sign El TSS asegura el uso de una fuente de tiempo confiable y una gestión adecuada de todos los componentes del sistema.

### 1.7.2 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo de E-Sign (TSA) es responsable de la provisión de Servicios de Sellado de Tiempo como se describe en este documento. Tiene la responsabilidad de la operación de las

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 6 de 34   |

Unidades de Sellado de Tiempo (TSU) relevantes que se crean y firman en nombre de la TSA. La entidad legal responsable de la TSA es E-Sign S.A. actuando como Proveedor de Servicios de Sellado de Tiempo. E-Sign emite Sellos de tiempo calificados bajo la siguiente jerarquía:

#### **AC Raíz**

CN = Esign CA Class 3 Root CA  
 OU = Terms of use at [www.esign-la.com/acuerdoterceros](http://www.esign-la.com/acuerdoterceros)  
 O = E-Sign S.A.  
 C = CL

#### **AC de la Autoridad de Sellado de Tiempo**

E = e-sign@esign-la.com  
 CN = E-Sign Class 3 Time Stamping Authority CA  
 OU = Terms of use at [www.esign-la.com/acuerdoterceros](http://www.esign-la.com/acuerdoterceros)  
 O = E-Sign S.A.  
 C = CL

### **1.7.3 Suscriptores**

El Suscriptor es el solicitante, persona física o jurídica, a quien se le proporciona el sello de tiempo y que celebra el contrato con E-Sign.

El suscriptor puede ser una organización que comprende varios usuarios finales o un usuario final individual.

Cuando el suscriptor es una organización, algunas de las obligaciones que se aplican a esa organización tendrán que aplicarse también a los usuarios finales. En cualquier caso, la organización será responsable si las obligaciones de los usuarios finales no se cumplen correctamente y, por lo tanto, dicha organización deberá notificar debidamente a sus usuarios finales.

Cuando el Suscriptor es un usuario final, el usuario final será el responsable directo si sus obligaciones no se cumplen correctamente.

### **1.7.4 Partes que confían**

Una Parte que Confía es una persona o entidad que recibe un documento digital con sello de tiempo y actúa en base a un certificado y / o una firma digital emitida bajo la TSA. Una parte que confía debe evaluar la corrección y validez del documento en sí en los contextos donde se utiliza.

### **1.7.5 Otros participantes**

No aplica.

### **1.7.6 Entidad Acreditadora**

La comunidad de usuarios requiere de un organismo independiente y de confianza que acredite que las políticas y prácticas de la TSA, son coherentes con las necesidades del sello de tiempo y que la TSA cumple cabalmente con dichas políticas y prácticas, en el caso de Chile la entidad acreditadora es el Ministerio de Economía.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 7 de 34   |

### 1.7.7 Uso de sellos de tiempo

Los Sellos de Tiempo se utilizarán únicamente en la medida en que el uso sea compatible con la ley aplicable y dentro de los límites y contextos especificados en el presente documento. Está prohibido cualquier uso fuera de los límites y contextos especificados en este documento o con fines ilícitos, contrarios al interés público o que puedan dañar el negocio o la reputación de E-Sign. A título indicativo, el uso de Sellos de tiempo está prohibido para cualquiera de los siguientes propósitos:

- actividades ilegales (incluyendo ciberataques);
- emisión de nuevos sellos de tiempo e información sobre la validez del sello de tiempo;
- permitir que otras partes utilicen el TST del suscriptor;
- utilizar el sello de tiempo emitido para sellar documentos que pueden tener consecuencias no deseadas (incluido el sello de tiempo en dichos documentos con fines de prueba).

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)".

## 1.8 Política de sellado de tiempo y declaración de prácticas de la TSA

### 1.8.1 Propósito

El presente documento especifica los requisitos de política y seguridad relacionados con las prácticas de operación y gestión de E-Sign como Autoridad de Sellado de Tiempo (TSA) para la emisión de Sellos de Tiempo. Estos se pueden usar para respaldar firmas electrónicas o para cualquier aplicación que requiera probar que un dato existió antes de un tiempo específico. El presente documento puede ser utilizado por entidades independientes como base para confirmar que la TSA E-Sign es una entidad confiable para la emisión de Sellos de Tiempo. El presente documento está a disposición del público. La distribución de este documento está restringida según se describe en la sección "Derechos de propiedad intelectual".

### 1.8.2 Nivel de especificidad

El presente documento describe solo las reglas generales de emisión y gestión de TST. La descripción detallada de la infraestructura y los procedimientos operativos relacionados se describen en documentos adicionales que no se ponen a disposición del público. Estos documentos adicionales solo están disponibles para el personal autorizado de E-Sign y, si es necesario, para los auditores del TSS.

### 1.8.3 Enfoque

El presente documento se define con los detalles específicos del entorno operativo, estructura organizativa, procedimientos operativos, instalaciones y entorno informático de la TSA E-Sign.

## 1.9 Cumplimiento

La TSA referencia las políticas de sello de tiempo, definidas por E-Sign, en cada uno de los sellos de tiempo emitidos. E-Sign es periódicamente inspeccionada por la Entidad Acreditadora a fin de asegurar

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 8 de 34   |

la correcta implantación de las prácticas de certificación definidas para la TSA, del cumplimiento de las obligaciones descritas en este documento para cada una de las partes, así como el haber cumplido con la implementación de los controles y procedimientos identificados en la política para garantizar la confianza en los sellos de tiempo que emite.

## 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 todo el servicio de Time-Stamping de acuerdo a lo dispuesto en la política, así como en la presente Declaración de Prácticas de sello de tiempo.
- Definir en sus prácticas y política de sello de tiempo las obligaciones de los distintos actores del proceso.
- Realizar una revisión periódica de las prácticas aquí descritas.
- Mantener actualizada estas prácticas y contar con la aprobación formal, ante cambios en las mismas, por parte del Comité de Seguridad.
- Proveer a todos los suscriptores y terceros de confianza, por medio de su sitio web [www.esign-la.com](http://www.esign-la.com) de:
  - ✓ La información de contacto.
  - ✓ La política, la declaración de prácticas y los documentos relacionados a los servicios de sello de tiempo, garantizando el acceso a la versión final de los documentos mencionados.
  - ✓ El algoritmo de hash utilizado como parte de las mismas políticas y prácticas publicadas. o La vigencia de la raíz utilizada para la firma de sus sellos de tiempo.
  - ✓ La precisión del tiempo utilizado como parte de las mismas políticas y prácticas publicadas.
  - ✓ Las prohibiciones de uso de sus sellos de tiempo, como parte de las mismas políticas y prácticas publicadas.
  - ✓ Las obligaciones tanto de los suscriptores como de los terceros de confianza, información contenida en las políticas y prácticas publicadas.
  - ✓ Los mecanismos de verificación de los tokens emitidos por E-Sign.
  - ✓ El periodo de permanencia de los log que maneja la TSA.
  - ✓ Las leyes, reglamentos y estándares bajo los cuales se regula la actividad de la TSA.
  - ✓ Un punto de contacto para presentar sus reclamos o no conformidades al servicio.
  - ✓ La resolución de funcionamiento, emitida por la Entidad Acreditadora.
- Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, tal como se indica en el punto “Administración del ciclo de vida de la llave”, incluida en este mismo documento.
- Mantener sincronizado el reloj de la TSU con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.
- Contar con la infraestructura requerida para prestar el servicio de sello de tiempo conforme al nivel de calidad comprometido.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 9 de 34   |

- Mantener los controles de seguridad física, de procedimiento y personales definidos para estos servicios, de acuerdo a lo comprometido en este documento.
- Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de E-Sign de acuerdo con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- 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.
- Garantizar mediante revisiones y auditorias que todos los requerimientos de la TSA cumplen con los controles requeridos por la legislación aplicable, las políticas, prácticas y procedimientos internos.
- Garantizar la seguridad de hardware criptográfico usado para firmar sello de tiempo a lo largo de su ciclo de vida.

Las obligaciones específicas, pertinentes al certificado de sello de tiempo emitido se detallan en las “Políticas de sello de tiempo” correspondiente y se encuentran disponible de manera pública en el sitio [www.esign-la.com/cps](http://www.esign-la.com/cps).

### 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 para el tiempo UTC que está incluido en los sellos se asegura una desviación máxima 1 segundo.
- La TSA de E-Sign garantiza un nivel de servicio superior al 95%, sin considerar los procesos de mantenimiento de sistemas y equipos. Los procesos de mantenimiento técnicos son planificados anticipadamente, teniendo una duración determinada y se debe dar aviso a los suscriptores del servicio, utilizando los medios de difusión disponibles.
- La TSA de E-Sign garantiza que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo (TSA), a través de su política de privacidad de datos personales disponible en su sitio web.
- Es política de E-Sign, sólo reembolsar al solicitante la tasa respectiva por la emisión de sus sellos de tiempo, en caso su solicitud no hubiese sido atendida por responsabilidad atribuible a E-Sign.

## 2.2 Obligaciones del suscriptor

- El suscriptor debe verificar que el token de time-stamping se ha firmado de manera correcta, confirmando que la llave privada de la TSA que firma dicho token se encuentra vigente – a través de la CRL o servicio OCSP - y que no ha sido comprometida.
- Conocer las normas estipuladas en las políticas y prácticas de certificación de sello de tiempo de E-Sign, y asentir lo que allí se estipule en forma previa a la emisión de un sello de tiempo.
- Conocer y aceptar el propósito y alcance de un sello de tiempo obtenido en E-Sign o en algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por E-Sign.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 10 de 34  |

## 2.3 Obligaciones de partes que confían

- Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Deberá verificar que la llave de la TSA no ha sido comprometida hasta el momento de la verificación, utilizando para ello la CRL publicada por E-Sign.

En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la TSA, se debe verificar que el número de serie del certificado de la TSA no se encuentra en la CRL, o determinar la validez del certificado de la TSA en el momento que se generó el sello.

- Conocer y Aceptar el propósito y alcance de un sello de tiempo emitidos por E-Sign o algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por E-Sign.
- Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado, y/o a los sellos de tiempo emitidos, lo cual puede ser considerado como causa de revocación del mismo.

## 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.

Los servicios de sellado de tiempo de E-Sign no han sido diseñados, autorizados o destinados para su aplicación en transacciones relacionadas con actividades que requieran funcionamiento a prueba de errores, como es el caso de instalaciones nucleares, sistemas de navegación o tráfico aéreo, sistemas de comunicación o de control de armamento, sistemas de equipos médicos o de todo otro sistema digital en que un error pueda conducir a la muerte, a las lesiones de personas, o a daños ambientales. E-Sign no será responsable en caso de producirse daños por el uso de sus servicios de sello de tiempo en ámbitos como los indicados en esta cláusula.

E-Sign declara que las responsabilidades por ella asumidas en esta declaración de prácticas y en los contratos o acuerdos de suscripción que a ellas se remitan serán aseguradas y reaseguradas conforme a las prácticas que habitualmente se aplican para los seguros de responsabilidad civil (Remítase a RG01), y en concordancia con lo estipulado por la legislación que exista o llegare a existir. En particular la TSA de E-Sign cuenta con un seguro en conformidad al artículo 14 de Ley 19799 para Chile. La cobertura señalada no podrá ser invocada directamente por el suscriptor o signatario titular de los sellos de tiempo, a menos que este sea la parte perjudicada. Los límites de responsabilidad a aplicar en cada sello se señalan en las políticas y prácticas de sello de tiempo correspondientes.

### 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, y en virtud de esto, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, así como por el incumplimiento de las prescripciones contenidas en la Ley N° 19.628 relativas a la protección de datos personales o en la

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 11 de 34  |

Ley 19.496 (Chile), sobre protección de los derechos de los consumidores. En ningún caso será responsable de cualquier perjuicio que derive de una utilización negligente, por parte de los suscriptores o terceras partes interesadas, o no acorde con las políticas y prácticas establecidas por la TSA de E-Sign.

E-Sign, como proveedor de servicios de Sello de Tiempo, adhiere 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, en los servicios que presta, producto de:

- Guerra, desastres naturales o cualquier otro caso de fuerza mayor.

Los cuales le hagan imposible proveer los servicios de *time-stamping* de acuerdo a lo definido y publicado en sus políticas y prácticas de certificación.

### 2.4.4 Resolución de Conflictos

Cualquier diferencia, dificultad, problema o controversia que pueda surgir entre E-Sign y los suscriptores o signatarios que suscriban él (los) respectivo(s) contrato(s) de sellos de tiempo, o con los terceros interesados que adhieran a las CPS de E-Sign con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de estas CPS o de la actividad de certificación de sellos de tiempo será resuelta definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que, en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El arbitraje se llevará a cabo en la ciudad de Santiago. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse en conformidad a las reglas establecidas para dichas resoluciones en el Título Sexto, del Libro Primero, del Código de Procedimiento Civil. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualquiera de las Partes presentare ante el sustituto. La evidencia de haberse ausentado del país el árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro deberá ser designado de común acuerdo por las Partes, dentro del plazo máximo de 15 días hábiles. A falta de acuerdo respecto de la persona que actuará en el cargo, el árbitro deberá tener el carácter de mixto y su designación será efectuada, a solicitud escrita de cualquiera de las Partes por la Justicia Ordinaria, debiendo recaer la designación en una persona que haya sido Ministro o Abogado Integrante de la Excelentísima Corte Suprema de Justicia, o bien, Profesor de las cátedras de Derecho

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> |  | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  |  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  |  | Página              | 12 de 34  |

Civil o Comercial de las Facultades de Derecho de las Universidades de Chile, Católica de Santiago o Católica de Valparaíso, excluidos quienes hubieren asesorado o prestado servicios a cualquier título a alguna de las partes en el bienio inmediatamente anterior.

## 3 Requerimientos en prácticas de la TSA

### 3.1 Declaraciones de Prácticas y de divulgación

#### 3.1.1 Declaración de prácticas de TSA

La TSA de E-Sign, a partir del análisis de riesgo aplicado al servicio de la TSA, ha generado una planificación orientada a mitigar los riesgos detectados. Esta planificación se encuentra alineada con las políticas y prácticas que detallan el servicio prestado desde el punto de vista de los actores participantes del proceso, sus obligaciones, del personal a cargo de la prestación del servicio, de los aspectos técnico asociados a dicha prestación, de los aspectos documentales y organizativos, así como de los cumplimientos legales que rige la actividad de E-Sign como TSA.

#### 3.1.2 Declaración de divulgación de TSA

La presente declaración de prácticas de sello de tiempo detalla la implementación de los controles que son necesarios para cumplir con la política de sellado de tiempo, garantizando fiabilidad y confianza del servicio de sellos. Entre los elementos más relevantes que considera este documento se encuentran:

- La información de contacto.
- Características del servicio de sello de tiempo
- El algoritmo de hash
- La precisión del tiempo
- Las prohibiciones de uso de sus sellos de tiempo
- Las obligaciones tanto de los suscriptores como de los terceros de confianza
- Los mecanismos de verificación de los *tokens* emitidos por E-Sign.
- El periodo de permanencia de los log que maneja la TSA.
- Las leyes, reglamentos y estándares bajo los cuales se regula la actividad de la TSA.
- Un punto de contacto para presentar sus reclamos o no conformidades al servicio.
- La resolución de funcionamiento, emitida por la Entidad Acreditadora.

E-Sign declara que tendrá a disposición pública, a través de su sitio web, la información relativa a los servicios prestados y formalizados en la Política y declaración de práctica de la TSA.

### 3.2 Gestión del ciclo de vida de las llaves

#### 3.2.1 Generación de la llave de la TSU

El módulo criptográfico adoptado por E-Sign, es capaz de generar llaves en base al algoritmo de encriptación de llave publica SHA2RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS\_COP.1; así mismo cuenta con capacidad de firmar, cifrar y distribuir las llaves tal como se solicita en el criterio común de distribución de llaves criptográficas CC P2 FCS\_CKM.2.

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                              |                                                                          |  |                     |           |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN DE SELLO DE TIEMPO (PCSTS)</b> |  | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                          |  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                          |  | Página              | 13 de 34  |

La llave usada por la TSU de E-Sign son generadas de acuerdo a las Políticas y Prácticas definidas para el proceso de Firma Electrónica Avanzada; utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la TSA de E-Sign utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, el cual sólo puede ser accedido por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de llaves del equipo HSM.

### 3.2.2 Protección de la llave privada de la TSU

E-Sign lleva a cabo un conjunto de acciones de manera tal de asegurar que la llave privada de la TSU, usada para firmar los sellos de tiempo, permanece de manera confidencial y mantenga su integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3. Cuando la llave privada es respaldada, ellas son copiadas, almacenadas y recuperadas sólo por el personal con roles de confianza y bajo un ambiente seguro.

Así, E-Sign realiza la protección de las llaves a través de:

- **Módulos criptográficos:** El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los HSM de E-Sign cumplan el criterio FIPS 140-2 Nivel 3 o equivalente.
- **Depósito de la llave privada:** La clave privada está cifrada y queda contenida en el repositorio implementado por el dispositivo HSM.
- **Copia de respaldo de la llave privada:** Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la AC (raíz o intermedias) que se puede aplicar en caso de contingencia para la TSA. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- **Introducción de la llave privada en el módulo criptográfico:** Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las TSU que hacen uso de dichos módulos.

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* de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos.

### 3.2.3 Distribución de la llave pública

Las llaves públicas utilizadas por las TSU de E-Sign son distribuidas en certificados digitales emitidos por una CA cuya Declaración de Prácticas de Certificación debe incluir como mínimo las prácticas especificadas en 3.2.7.

El mecanismo mediante el cual es establecida la confianza en la TSA por parte de un tercero que desee confiar está basado en la instalación del certificado raíz bajo cuya jerarquía fue emitido el certificado que autentifica la llave pública de la TSU respecto a la cual se desea confiar. E-Sign publica en su sitio

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PÚBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                              |                                                                                  |                     |           |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                                  | Página              | 14 de 34  |

web tanto los certificados raíz bajo cuya jerarquía emite sus propios certificados para autenticación de TSA, como certificados raíz de otros PSC acreditados por el Ministerio de Economía de Chile, bajo cuya jerarquía son emitidos certificados para autenticación de TSA. Estos certificados, se encuentran disponibles en el sitio web de E-Sign, a través de una conexión segura (https).

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido firmado por la TSA podrá ser validado por el cliente, ya que el certificado raíz contiene la llave pública que permitirá verificar la validez de la cadena de certificación en la cual encaja el certificado que, a su vez, autentifica el sello emitido.

A continuación, se presenta la secuencia general del modelo de confianza:

- Se descarga certificado raíz de la AC que ha emitido el certificado utilizado para autenticar la firma del sello de tiempo. Este certificado debe ser descargado a través de un canal seguro, que debe tener habilitado el sitio de descarga de dicha raíz.
- Descargado el certificado raíz, este se procede a instalar en el repositorio de entidades emisoras raíz de confianza del equipo cliente.
- El sistema indicará si la importación e instalación del certificado ha sido correcta. De ser así, cualquier sello de tiempo que sea firmado con un certificado de sello de tiempo, que ha sido emitido y firmado bajo esta raíz, podrá ser validado automáticamente en el equipo cliente.

### 3.2.4 Reemisión de llaves de la TSU

Por motivo de seguridad y 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, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

### 3.2.5 Terminación del ciclo de vida de la llave del TSU

La llave privada de la TSU será reemplazada al momento de su expiración y/o compromiso de la llave privada de firma. La TSU rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida.

El tiempo de vigencia del certificado de la TSU no es mayor que el periodo de vigencia de los algoritmos y tamaño de llave declarado en estas prácticas.

La TSA de E-Sign tiene la capacidad de revocar el certificado raíz activa de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que E-Sign vaya a discontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo: suscriptores, terceros de confianza y autoridades de sello de tiempo.

E-Sign comunicará a cada uno de sus suscriptores del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los suscriptores,

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PÚBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                              |                                                                                  |                     |           |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                                  | Página              | 15 de 34  |

los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

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

La gestión de ciclo de vida del hardware criptográfico usado por la TSA de E-Sign para la firma de sellos de tiempo tiene como objetivo garantizar la seguridad de este hardware a lo largo de su ciclo de vida. Para cumplir con este objetivo están contempladas las siguientes las medidas de seguridad señaladas a continuación.

- Los equipos criptográficos utilizados por la TSA de E-Sign para firmar los sellos de tiempo, deben contar con certificación FIPS 140-2 nivel 2 como mínimo.
- Los equipos criptográficos deben estar instalados en las dependencias identificadas en 3.4.4 que también describe las medidas de seguridad física y ambiental implementadas en tales dependencias
- El acceso a los equipos criptográficos está restringido a personal con roles específicos que cumplen con los requerimientos descritos en 3.4.3.

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 equipos HSM con que cuenta E-Sign y que son usados para firmar los sellos de tiempo, cuentan con la detección de intrusión a los equipos mediante detectores de intrusión. En caso de detección de una intrusión el equipo HSM reinicia automáticamente su memoria a sus condiciones de salida de fábrica. Los eventos antes mencionados son registrados en el registro de auditoría del equipo.

Ante la detección de un incidente de detección de intrusión, el equipo no debe ser puesto en producción, ya sea que el incidente se haya ocurrido durante el almacenamiento o transporte del equipo. El administrador del equipo debe proceder a reiniciar el equipo a sus condiciones de salida de fábrica y reportar el incidente al Oficial de Seguridad.

Si el incidente registrado, ocurre durante el transito del equipo desde las dependencias de su fabricante, el Oficial de Seguridad debe contactarse inmediatamente con este fabricante. En cambio, de ocurrir este evento posterior a la instalación, adicionalmente se deben revisar eventuales brechas en las políticas y procedimientos de seguridad que permitieron la ocurrencia dicho incidente.

Las revisiones que deben realizarse como mínimo al equipo, tanto posterior a su transporte o durante su almacenamiento es:

- Controlar que los sellos de seguridad no han sido alterados.
- Verificar que no se presentan daños visibles a la estructura general del equipo.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PÚBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 16 de 34  |

- Verificar que el registro de auditoría del equipo no contenga alarmas o registro de incidentes.

### 3.2.6.2 Administración del Hardware Criptográfico

El equipo HSM utilizado por E-Sign tanto para su PSC como TSA, implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

Para acceder a funcionalidades del HSM, sobre el que se ejecutan las operaciones de instalación, respaldo y recuperación, se utilizan estos medios físicos de protección lógica, los que controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la Autoridad Certificadora, utilizada para la generación del certificado de la TSU, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar.

Finalmente, en caso de requerir mover el equipo a otra instalación o el envío del mismo a la fábrica por motivos de garantía, E-Sign ha definido que la memoria del dispositivo debe ser restablecida al estado de salida de fábrica, eliminado así todo su contenido.

#### 3.2.6.2.1 Token de sello de tiempo

E-Sign cuenta con procedimientos técnicos para garantizar que los TST sean emitidos de forma segura e incluyan la hora correcta. Cada TST incluye:

- una representación del datum con sello de tiempo proporcionado por el solicitante
- un número de serie único para identificar un TST específico
- una firma electrónica generada con una clave utilizada exclusivamente para Sellado de tiempo
- un identificador único de la política de seguridad bajo la cual fue creado el token.
- un identificador para la TSA y la TSU.
- valor de fecha y hora trazable al valor de la hora UTC real
- algoritmo de firma utilizado en TST

### 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 descritos en los apartados siguientes, sin embargo, a la fecha de publicación de esta Declaración de Prácticas de Certificación de Sellado de Tiempo, los certificados utilizados para autenticar las llaves de las TSU de la TSA son emitidos por la Autoridad Certificadora de E-Sign exclusivamente, y, a su vez, la Autoridad Certificadora de E-Sign sólo emite certificados de TSA para la Autoridad de Sellado de Tiempo de E-Sign.

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 17 de 34  |

*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 Certificado TSA

Un certificado de TSA puede ser solicitado por cualquier representante debidamente autorizado de la Autoridad de Sellado de Tiempo de E-Sign.

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:

- La existencia de la organización mediante el uso de al menos una tercera parte proveedora de servicios de pruebas o base de datos, o, alternativamente, 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.
- 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.
- Que la Organización ha autorizado la Solicitud de Certificado de TSA.
- 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.

En el caso de que la organización solicitante y la Autoridad Certificadora sean E-Sign, los requerimientos en a), b) y c) son considerados cumplidos y sólo es validado el requerimiento en d).

### 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 AR, 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).

Descripción del procedimiento de emisión

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 18 de 34  |

El proceso de emisión de un certificado de TSA comprende los siguientes eventos:

a) Generación de Llaves

Representante de TSA solicita a operador de TSU la habilitación de certificado TSA  
Operador TSU genera llaves y CSR en servidor TSA.  
Operador TSU envía CSR a Representante de TSA.

b) Solicitud de Certificado TSA

Representante de TSA genera ticket con solicitud de certificado TSA en Sistema de Atención.  
Responsable del área a la cual pertenece el solicitante autoriza ticket en Sistema de Atención.  
Responsable del área a la cual pertenece el Administrador de la Autoridad Certificadora (AC) autoriza ticket en Sistema de Atención.

c) Emisión de Certificado TSA

Administrador de la AC valida autorizaciones en ticket en Sistema de Atención.  
Administrador de la AC accede a sistema de Administración de la AC y emite certificado TSA.  
Administrador de la AC carga el certificado TSA en ticket en Sistema de Atención

d) Instalación de Certificado TSA.

Representante de TSA descarga certificado TSA desde ticket en Sistema de Atención  
Representante de TSA envía certificado TSA a Operador TSU.  
Operador TSU instala certificado TSA en servidor TSA.

### 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 periodo 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.

Descripción del procedimiento de recambio de llaves

El proceso de recambio de llaves de un certificado de TSA comprende los siguientes eventos:

a) Generación de Llaves

Representante de TSA solicita a operador de TSU la habilitación de certificado TSA.  
Operador TSU genera llaves y CSR en servidor TSA.  
Operador TSU envía CSR a Representante de TSA.

b) Solicitud de Certificado TSA

Representante de TSA genera ticket con solicitud de certificado TSA en Sistema de Atención.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 19 de 34  |

Responsable del área a la cual pertenece el solicitante autoriza ticket en Sistema de Atención.

Responsable del área a la cual pertenece el Administrador de la Autoridad Certificadora (AC) autoriza ticket en Sistema de Atención.

c) Emisión de Certificado TSA

Administrador de la AC valida autorizaciones en ticket en Sistema de Atención.

Administrador de la AC accede a sistema de Administración de la AC y emite certificado TSA.

Administrador de la AC carga el certificado TSA en ticket en Sistema de Atención.

d) Instalación de Certificado TSA

Representante de TSA descarga certificado TSA desde ticket en Sistema de Atención.

Representante de TSA envía certificado TSA a Operador TSU.

Operador TSU instala certificado TSA en servidor TSA.

### 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.

Descripción del procedimiento de renovación de certificado

El proceso de renovación de un certificado de TSA comprende los siguientes eventos:

a) Generación de CSR

Representante de TSA solicita a operador de TSU la renovación de certificado TSA.

Operador TSU genera CSR en servidor TSA.

Operador TSU envía CSR a Representante de TSA.

b) Solicitud de Certificado TSA

Representante de TSA genera ticket con solicitud de certificado TSA en Sistema de Atención.

Responsable del área a la cual pertenece el solicitante autoriza ticket en Sistema de Atención.

Responsable del área a la cual pertenece el Administrador de la Autoridad Certificadora (AC) autoriza ticket en Sistema de Atención.

c) Emisión de Certificado TSA

Administrador de la AC valida autorizaciones en ticket en Sistema de Atención.

Administrador de la AC accede a sistema de Administración de la AC y emite certificado TSA.

Administrador de la AC carga el certificado TSA en ticket en Sistema de Atención.

d) Instalación de Certificado TSA

Representante de TSA descarga certificado TSA desde ticket en Sistema de Atención.

Representante de TSA envía certificado TSA a Operador TSU.

Operador TSU instala certificado TSA en servidor TSA.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 20 de 34  |

### 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 la 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 prerrequisito 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 también tendrá derecho a revocar o solicitar la revocación del Certificado del Suscriptor.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                              |                                                                                  |  |                     |           |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> |  | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                                  |  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                                  |  | Página              | 21 de 34  |

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

Descripción del procedimiento de revocación

El proceso de revocación de un certificado de TSA comprende los siguientes eventos:

a) Producción de Carta de Revocación

Representante de TSA completa Carta de Revocación de certificado TSA.  
Representante de TSA genera ticket con Carta de Revocación de certificado TSA en Sistema de Atención.

b) Procesamiento de Carta de Revocación de Certificado TSA

Responsable del área a la cual pertenece el solicitante valida Carta de Revocación y autoriza ticket en Sistema de Atención.  
Responsable del área a la cual pertenece el Administrador de la Autoridad Certificadora (AC) valida Carta de Revocación y autoriza ticket en Sistema de Atención.

c) Revocación de Certificado TSA

Administrador de la AC valida autorizaciones en ticket en Sistema de Atención.  
Administrador de la AC accede a sistema de Administración de la AC y revoca el certificado TSA.  
Administrador de la AC informa revocación del certificado TSA en ticket en Sistema de Atención.

## 3.3 Sello de tiempo

### 3.3.1 Sincronización de los relojes con UTC

En E-Sign la TSA utiliza una fuente fiable de tiempo, mediante un servidor NTP que se sincroniza 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*”, el cual provee tiempo UTC(k); lo anterior con una desviación máxima de 1 segundo. Esta fuente de tiempo está basada en el protocolo NTP (*Network Time Protocol*) haciendo que la exactitud no disminuya por debajo de los requerimientos.

De manera más específica:

- La calibración de la TSU es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la TSU se encuentra protegido contra amenazas ambientales que puedan afectar su precisión fuera del rango declarado.
- 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.
- En caso de detectarse una desviación más allá de la precisión declarada, la TSU no generará nuevos TST hasta que el tiempo correcto es restaurado.
- E-Sign declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el TST.

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PÚBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 22 de 34  |

## 3.4 Gestión de la TSA y operaciones

### 3.4.1 Gestión de la seguridad

La TSA de E-Sign desarrolla una administración activa de la seguridad (Remítase a PS01), que considera las mejores prácticas y estándares de la industria. Este Sistema de Gestión se basa en un análisis de riesgo desarrollado por la TSA de E-Sign, a fin de detectar sus brechas de seguridad y planificar las mitigaciones de las mismas a través de un plan de trabajo que incluye medidas documentales, técnicas y organizativas.

En particular:

- E-Sign declara que su TSA es responsable por todo el aspecto asociado a la provisión de servicios de sello de tiempo
- Todo su personal tiene acceso a sus prácticas y políticas de sello de tiempo.
- E-Sign cuenta con un Comité de seguridad de la información, un oficial de seguridad y privacidad, los que en su conjunto velan por el cumplimiento del plan anual definido; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación.
- E-Sign declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados anualmente por la Entidad Acreditadora del Ministerio de Economía de Chile.
- La TSA de 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. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA de E-Sign generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente. Para el cumplimiento de este plan, así como su seguimiento, E-Sign cuenta con un Comité de seguridad de la información, un oficial de seguridad, los que en su conjunto velan por el su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.

### 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

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 23 de 34  |

- 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

Mediante CV y entrevistas realizadas al momento de la vinculación.

### 3.4.3.3 Roles de confianza

- **Oficial de seguridad y privacidad:** es responsable de la administración e implementación de las prácticas de seguridad y políticas y plan de privacidad.
- **Administrador de Sistemas:** está autorizado a instalar, configurar y mantener los sistemas de confianza de la TSA, para la administración de sello de tiempo, Además es responsable por la operación de los sistemas y autorizado para realizar el respaldo y recuperación.
- **Administrador de Seguridad:** Es el encargado de verificar la mantención de los sistemas de confianza de la TSA.
- **Auditor:** es el encargado de revisar archivos y log de auditoría de la TSA.

### 3.4.3.4 Frecuencia de rotación de tareas

No es aplicable para E-Sign, ya que las personas mantienen su cargo.

### 3.4.3.5 Sanciones

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

### 3.4.3.6 Requerimientos de contratación

Como parte del contrato, todo trabajador de la PSC, firma un acuerdo de confidencialidad.

### 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

Adicionalmente, se facilitará el acceso a la documentación técnica necesaria para llevar a cabo sus funciones.

### 3.4.3.8 Control de cumplimiento

De acuerdo al Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 24 de 34  |

### 3.4.3.9 Finalización de contratos

El oficial de seguridad con el apoyo del área de sistemas y RRHH, procederá a:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización
- Suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización
- Supresión de acceso a toda información, a excepción de la considerada PÚBLICA
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios.
- Informar a los proveedores y entidades externas a E-Sign la marcha de individuo y de que ya no representa a la TSA de E-Sign.
- Verificar la devolución del material proporcionado por la E-Sign. Por ejemplo:
  - ✓ Equipo computacional
  - ✓ Llaves mobiliario oficinas
  - ✓ Teléfono móvil, etc.

## 3.4.4 Seguridad física y ambiental

E-Sign en su calidad de PSC y TSA, opera en dos Centros de Datos seguros y confiables bajo certificación Tier III y Tier II, estando sus servicios en acuerdo a estas prácticas de certificación como también de acuerdo a la norma ETSI TS 102 023.

Específicamente la TSA de E-Sign cumple con los puntos más abajo indicados

### 3.4.4.1 Emisión de sellos de tiempo, así como su administración

- a) Los accesos físicos solo son limitados al personal autorizado y relacionados al servicio de sello de tiempo.
- b) E-Sign cuenta con un plan de continuidad operacional tanto para su PSC con TSA, los cuales son probados periódicamente a fin de verificar su operación, así como para realizar mejoras que podrían resultar de estos simulacros.
- c) E-Sign implementa controles a fin de evitar la pérdida de información de la TSA.

### 3.4.4.2 Control de los módulos criptográficos

E-Sign mantiene los controles de sus módulos criptográficos tanto para la generación de la llave, así como la protección de las mismas tal como se indican en la “Gestión del ciclo de vida de las llaves” de este mismo documento.

### 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 Certificados, se encuentra alojado en un Sitio Principal y uno secundario. Las características generales del recinto Principal comprenden una Zonificación en Alta Criticidad (Sitio de Producción) y una Zona de Media Criticidad.

- Zona Alta Criticidad: Sitio de Producción:
  - ✓ El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 25 de 34  |

- ✓ Acceso restringido.
- ✓ Sistema de video vigilancia.
- ✓ Piso falso de 30cm de altura con cámara plena para distribución de aire para climatización de todos los equipos de la sala.
- ✓ Acceso por rutas físicas redundantes para fibras ópticas carriers.
- ✓ Equipos de Climatización precisa redundantes en configuración 1+1.
- ✓ Equipos de energía ininterrumpida UPS redundantes en configuración 1+1. La iluminación de la sala se encuentra respaldada por el sistema UPS y el grupo electrógeno.
- ✓ Sistema autónomo de detección y extinción de incendios.
- ✓ Soporte generación autónoma de energía de emergencia mediante Grupo Electrónico de operación continua. Todos los equipos están respaldados.
- Zona Criticidad Media: Operaciones:
  - ✓ Espacio cerrado de oficinas dotado de puestos de trabajo para personal operación y administración.
  - ✓ Acceso restringido mediante tarjeta magnética u botonera con clave.
  - ✓ Sistema de Video Vigilancia.
  - ✓ Iluminación y puestos de trabajo respaldados por el grupo electrógeno.

Respecto al sitio secundario sus principales características son:

- ✓ Acceso restringido y controlado.
- ✓ Climatización full redundante calculada de acuerdo a la carga térmica de la sala.
- ✓ Alimentación del sistema eléctrico independiente de otros consumos propios del lugar en que se encuentra ubicado el sitio secundario.
- ✓ Sistema de respaldados con UPS redundante y grupo electrógeno.
- ✓ Sistema de detección temprana de incendio y extinción vía agente limpio FM-200.
- ✓ Sistema de detección de sobre temperatura para monitorear permanentemente el funcionamiento del sistema de Aire Acondicionado.
- ✓ Sistema de detección de intrusos.
- ✓ Acceso por rutas físicas redundantes para fibras ópticas carriers.
- ✓ Acceso a través de una puerta cortafuego.
- ✓ Sistemas de Circuito Cerrado de Televisión.

Por otra parte, el edificio donde se encuentran la Casa Matriz de E-Sign, cuenta con accesos vigilados por un circuito cerrado de cámaras de seguridad, sensores de intrusión para controlar y detectar el acceso a áreas restringidas y guardias en la entrada del edificio, con lo cual se pretende mantener un control de acceso mínimo a las instalaciones.

Adicionalmente, en estas dependencias podemos encontrar:

- Entradas cerradas con un sistema de control de acceso vía tarjeta.
- Área de recepción atendida por personal.
- Control de acceso a visitas.

A través de estas medidas se mantiene un perímetro de seguridad que restringe el acceso sólo a personal autorizado.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 26 de 34  |

#### 3.4.4.3.1.1 Seguridad Física Data Center

Los sistemas de E-Sign, como Entidad de Certificación, se encuentran alojados en un Sitio Principal y uno secundario. Ambos sitios cuentan con niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos sitios cuentan con diversos perímetros de seguridad, diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico, sistemas de video vigilancia y de grabación, de detección de intrusiones entre otros.

Los sitios además cuentan con un sistema central de vigilancia mediante circuito cerrado de televisión, distribuidas en lugares estratégicos del piso, las que permanentemente están grabando las actividades y registrando los accesos de personas a lugares que requieren acceso restringido. El centro de control es monitoreado por guardias de seguridad las 24 horas del día, todos los días de la semana, lo que permite llevar un registro y control total de acceso.

#### 3.4.4.3.1.2 Sistema de Energía Eléctrica

El suministro eléctrico para el sitio principal está garantizado a través de diversas alternativas que operan en forma concurrente. Adicional a esto, se han incorporado la instalación de un grupo electrógeno dimensionado para proporcionar energía eléctrica a todas las instalaciones del sitio ante fallas de los proveedores de energía. Todo el sistema de suministro eléctrico está reforzado por una serie de UPS's instaladas en cascada, que garantizan la operación por un tiempo más que suficiente para activar el generador y asegurar la continuidad del servicio. También se cuenta con tableros eléctricos redundantes de modo de asegurar el funcionamiento antes fallas de la distribución de los equipos.

Respecto al sitio secundario, sus instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. En resumen, ambos sitios cuentan con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación por largos periodos de tiempo.

#### 3.4.4.3.1.3 Sistema de Control Ambiental

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. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Ambos cuentan con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 27 de 34  |

#### 3.4.4.3.1.4 Sistema de Extinción y Control de Incendios

Dado los riesgos de incendio a que pueden estar sujetos los sitios, es que tanto el sitio principal como el secundario cuentan 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 con FM-200.

#### 3.4.4.3.1.5 Telecomunicaciones

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de E-Sign, es que se ha diseñado en ambos sitios una plataforma robusta, segura y escalable, utilizando como base para ello los servicios WAN, estos servicios provistos por los principales portadores del país, nos aseguran, redes confiables y con tecnología de última generación.

El objetivo principal de este diseño es cumplir con los niveles de servicio comprometidos por E-Sign, por lo que se contempla respaldos en todos los puntos críticos. Adicionalmente, cabe destacar que las redes de transporte del portador están diseñadas para entregar una alta disponibilidad, comuna arquitectura redundante interna, lo cual permite garantizar el servicio de conectividad sobre su red.

#### 3.4.4.3.1.6 Seguridad Lógica Data Center

Ambos sitios cuentan los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

### 3.4.5 Gestión de las operaciones

La TSA de E-Sign asegura que su sistema y componentes son seguros y se encuentran operados de manera correcta, con un riesgo mínimo de falla.

Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado. Lo anterior a través de la aplicación de normativas de desarrollo de aplicaciones, protección de malware, adquisición de nuevos componentes y procedimiento de paso a producción.

- **Manejo de medios y seguridad:** 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. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA de E-Sign generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente. Para el cumplimiento de este plan, así como su seguimiento, E-Sign cuenta con un Comité de seguridad de la información, un oficial de seguridad, los que en su conjunto velan por el su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Ministerio de Economía de Chile.

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                              |                                                                          |  |                     |           |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE CERTIFICACIÓN DE SELLO DE TIEMPO (PCSTS)</b> |  | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                          |  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                          |  | Página              | 28 de 34  |

- **Planificación de la capacidad:** El manejo de la capacidad para la demanda es monitoreado y proyectado de acuerdo a los futuros requerimientos, de manera que la capacidad de proceso como de almacenamiento siempre sean las adecuadas. E-Sign cuenta con un documento de Gestión de Capacidad, cuyo objetivo es definir la provisión de recursos y servicios de manera óptima y efectiva en costos de manera de que ellos calcen con la demanda de los clientes presentes y futuros que E-Sign atiende. Este proceso ayuda a identificar y reducir las ineficiencias asociadas con la sub utilización de los recursos, niveles de demanda no satisfechas por E-Sign así como el proveer los niveles de servicio comprometidos de una manera eficiente en costos.
- **Manejo de incidentes y su respuesta:** E-Sign cuenta con un sistema de gestión de incidentes que asegura que los eventos y debilidades de la seguridad de la información, asociados con los sistemas de información de los procesos de la PSC y su TSA, son comunicados a los roles encargados de la gestión de los incidentes, de una manera que permite el que se realicen las acciones correctivas oportunas, documentadas y estructuradas para resolver estos incidentes en el menor tiempo posible.

La gestión de incidentes en E-Sign, a través de su área de Postventa, proporciona el punto único de contacto entre E-Sign y sus clientes, actuando como interfaz entre los usuarios y las funciones de TI y también como filtro para asegurar que todos los miembros de los equipos de E-Sign puedan completar su trabajo en una forma estructurada.

El sistema de gestión de incidentes, adicional a los incidentes de seguridad, permite la recepción de los reportes de fallas y consultas que afectan el normal funcionamiento de los servicios asociados al proceso de emisión de certificados, así como el canal para la recepción de solicitudes de mantenimiento correctivo, preventivo y perfectivo de las aplicaciones, y también la creación, modificación y eliminación de cuentas de usuarios para las aplicaciones, etc.

- **Procedimientos operacionales y responsabilidades:** La operación del servicio de Sello de Tiempo de la TSA de E-Sign opera de manera independiente de otros servicios provistos por la PSC: estas operaciones son desarrolladas por personal confiable definida en la estructura de la PSC de E-Sign y sus Prácticas de Certificación.

### 3.4.6 Gestión de acceso a los sistemas

La TSA de E-Sign, declara y asegura que el acceso a su sistema (hardware, software y datos) sólo está limitado al personal autorizado. En particular, la PSC de E-Sign cuenta con:

- Firewall Perimetral en Alta disponibilidad con licenciamiento UTM, apropiado para proteger la red interna de accesos no autorizados incluyendo a suscriptores y terceros que confían. El documento guía para este compromiso son la “Normativa de uso de los servicios de red”.
- Administración de usuarios, para mantener la seguridad de los sistemas, incluyendo administración de cuentas, logs y modificación o eliminación de accesos.
- Restricciones de acceso a la información y sistemas de aplicación de acuerdo a la política de control de acceso, así como desagregación de funciones en los roles de confianza definidos.
- Un control apropiado del personal autorizado tanto en su identificación como autenticación, previo a tener acceso a las aplicaciones relacionadas con los sellos de

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PÚBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 29 de 34  |

tiempo. En particular E-Sign cuenta con un inventario de activos, incluyendo los roles y personas que cubren cada rol.

Adicionalmente, los componentes de la red local se mantienen en *Datacenters* bajo ambiente seguro y con una auditoría periódica.

Los administradores de E-Sign realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA.

### 3.4.7 Mantenimiento e implementación de sistemas de confianza

La TSA asegura que sus sistemas y productos están protegidos contra modificaciones no autorizadas.

Para ello, la TSA de E-Sign y su PSC previo a cualquier cambio en sus sistemas o productos lleva a cabo:

- Un análisis de requerimientos de seguridad es llevado a cabo durante el diseño y especificación de requerimientos. Es así como, cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente las actividades para determinar e implementar los requerimientos de seguridad necesarios. Esto ocurrirá tanto cuando se vaya a adquirir un producto o cuando este se desarrolle internamente; estableciendo igualmente los requerimientos de seguridad que debe cumplir y revisando dicho cumplimiento antes de su compra o desarrollo.
- Un procedimiento de control de cambio para nuevas versiones, modificaciones y/o correcciones de emergencia al software. El propósito de este Procedimiento es establecer las actividades necesarias para llevar a cabo los cambios y actualizaciones en los sistemas de una manera eficiente, incluido las nuevas versiones y los pasos a producción, minimizando el impacto y las incidencias que se puedan producir debido a ellos.
- Respecto a la generación de la llave de la TSA, utilizada por la TSU en la entrega de sus sellos de tiempo TST, siempre es creada en un ambiente seguro.

### 3.4.8 Compromiso de los servicios de TSA

La TSA de E-Sign declara que ante cualquier evento de seguridad que afecte sus servicios, incluyendo compromiso de la llave de firma de la TSU o pérdida de precisión declarada de su reloj, esto es informado directamente o a través de su sitio web a sus suscriptores y terceros que en ella confía. El PSC de E-Sign y en particular su TSA ha:

- Desarrollado un Plan de continuidad operacional, el cual incluye los escenarios de compromiso de llave, pérdida de la precisión declarada del reloj de la TSA o falla de componentes que afecten directamente la operación del sitio principal de la TSA. Para estos escenarios E-Sign ha definido un plan que permite la recuperación de servicios frente a estos eventos.
- Ante los eventos antes mencionados, la TSA de E-Sign no emitirá nuevos TST hasta superar el compromiso declarado.
- Ante pérdida de la precisión, compromiso del mismo o sospecha de compromiso en el tiempo de la TSA; E-Sign dejará esta información a los suscriptores y terceros que confían indicando la descripción del evento. Esta comunicación será directa o a través de su sitio web

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 30 de 34  |

- En caso de comprometerse ya sea la llave o la precisión declarada, se informará a los suscriptores y terceros que confían de aquella información que permite detectar los sellos de tiempo afectados, a menos que esta información vulnere su política de privacidad de datos personales - disponible en su sitio web - de sus usuarios o la seguridad del servicio de la TSA de E-Sign.

### 3.4.9 Cese de la TSA

La TSA de E-Sign tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que E-Sign vaya a discontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo: suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas.

E-Sign comunicará a cada uno de sus suscriptores del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los suscriptores, los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

### 3.4.10 Cumplimiento de requerimientos legales

E-Sign como Autoridad de sello de tiempo, actúa en conformidad con la Ley N° 19.799, 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 calificadoros (ETSI, ISO, RFC, etc.). Además, su operación se encuentra regulada por la Entidad Acreditadora del Ministerio de Economía de Chile 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, manteniendo la confidencialidad y la integridad de los datos; 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. E-Sign usa esta información sólo para los fines que fueron entregados por parte del suscriptor.

La información con data del suscriptor es protegida de divulgación, a menos que sea solicitada por él mismo o por orden judicial u otro requisito legal.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                              |                                                                                  |                     |           |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                                  | Página              | 31 de 34  |

### 3.4.11 Registro de información concerniente a las operaciones del servicio de sello de tiempo

La TSA de E-Sign mantiene registros de la información relevante, concerniente a su operación. La información personal de los suscriptores, que ha recolectado la PSC de E-Sign como parte de su operación, está protegida de acuerdo con la Política de Privacidad de datos personales publicados por E-Sign en su sitio web.

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. Lo anterior a fin de proteger la confidencialidad de dichos datos. 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 PSC de E-Sign.

## 3.5 Organización

La Autoridad de Sellado de Tiempo 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 de Chile. En particular la TSA de E-Sign cumple con:

- Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias que contravengan la Ley N° 19.496 sobre los derechos de los consumidores para Chile.
- 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.
- E-Sign para la provisión de sus servicios cumple con la normativa legal vigente en Chile, respecto a la formación y operación de empresas y personas jurídicas.
- E-Sign como parte de su cumplimiento de la Ley 19799 (Chile), artículo 14, cuenta con un seguro de responsabilidad civil, 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 en Chile, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal a través de sus planes anuales de capacitación.

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PÚBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 32 de 34  |

- E-Sign 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-Sign mantiene un su repositorio documental todo contrato, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

## 4 Control de Documento

| Nº  | Motivo                                                                          | Fecha Modificación | Página            | Realizado por | Fecha Aprobación | Revisado y aprobado |
|-----|---------------------------------------------------------------------------------|--------------------|-------------------|---------------|------------------|---------------------|
| 1.0 | Creación de documento                                                           | 10/02/2020         | Todo              |               | 10/02/2018       | Comité de Seguridad |
| 2.3 | Se actualiza formato                                                            | Marzo 2020         | Todo              | Ronald Pérez  | Noviembre 2020   | Comité de Seguridad |
| 2.4 | Actualización de contenido en 3.2.3                                             | Octubre 2022       | 14-15             | Juan Pizarro  | Octubre 2022     | Comité de Seguridad |
| 2.5 | Actualización de contenido en 2.1.1, 3.2.6 y 3.2.7                              | Octubre 2023       | 8-9, 15-16, 16-21 | Juan Pizarro  | Octubre 2023     | Comité de Seguridad |
| 2.6 | Se añadió la url <a href="http://www.esign-la.com/cps">www.esign-la.com/cps</a> | Mayo 2025          | Punto 1.6         | Jorge Silva   | Mayo 2025        | Comité de seguridad |

## 5 Apéndice Tabla de siglas y definiciones

**Tabla de siglas**

| Plazo | Definición                                                                         |
|-------|------------------------------------------------------------------------------------|
| 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 Sellado de Tiempo                                                        |
| CP    | Certificate Policy, o Políticas de Certificado                                     |
| CPS   | Certificate Practice Statement, o Declaración de Prácticas de Certificación.       |
| CRL   | Certificate Revocation List, o Lista de revocación de Certificados.                |
| FIPS  | Federal Information Processing Standards.                                          |
| OCSP  | Online Certificate Status Protocol, o Protocolo de estado en línea de Certificado. |
| PKI   | Public Key Infrastructure, o Infraestructura de Llave Pública.                     |
| RFC   | Request for Comments, o Solicitud de comentarios.                                  |

### Definiciones

| Término | Definición |
|---------|------------|
|---------|------------|

| Elaborado por: | Aprobado por:       | Lugar de Archivo            | USO PUBLICO |
|----------------|---------------------|-----------------------------|-------------|
| CISO           | COMITÉ DE SEGURIDAD | Redmine – Proyecto Webtrust |             |

|                                                                                                              |                                                                                  |                     |           |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO PÚBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                              |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                              |                                                                                  | Página              | 33 de 34  |

| Término                                               | Definición                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificado                                           | Un mensaje que, al menos, establece un nombre o identifica a la entidad emisora, identifica al Suscriptor, contiene la llave pública del Suscriptor, identifica el Período Operativo del Certificado, contiene un número de serie del Certificado y está firmado digitalmente por la CA.                                                                                                     |
| Políticas de certificación (CP)                       | Conjunto ordenado de reglas que indica la aplicabilidad de un certificado a una comunidad particular y/o a una clase de aplicación con requerimientos de seguridad comunes                                                                                                                                                                                                                   |
| Lista de revocación de Certificados (CRL)             | Listado, firmado digitalmente por una CA, de los Certificados que han sido identificados como revocados antes de su fecha de vencimiento. La lista generalmente indica el nombre del emisor de CRL, la fecha de emisión, la fecha programada de la siguiente emisión de CRL, los números de serie de los Certificados revocados, y los tiempos específicos y las razones para la revocación. |
| Autoridad Certificadora (CA)                          | Una entidad autorizada para emitir, gestionar, revocar y renovar Certificados                                                                                                                                                                                                                                                                                                                |
| Declaración de Prácticas de Certificación (CPS)       | Una declaración de las prácticas que una Autoridad Certificadora emplea al aprobar o rechazar Solicitudes de Certificados y al emitir, administrar y revocar Certificados-                                                                                                                                                                                                                   |
| Compromiso                                            | Una violación (o supuesta violación) de una política de seguridad, en el que una divulgación no autorizada de, o la pérdida de control sobre, la información puede haber ocurrido. Con respecto a las llaves privadas, un compromiso es una pérdida, robo, divulgación, modificación, uso no autorizado, u otro compromiso de la seguridad de la llave privada.                              |
| Autoridad Intermedia de certificación (CA intermedia) | Una Autoridad Certificadora, cuyo Certificado se encuentra dentro de una cadena de Certificados entre el Certificado de la CA raíz y el Certificado de la Autoridad Certificadora que emitió el Certificado del Suscriptor usuario final.                                                                                                                                                    |
| Período operacional                                   | Período que comienza con la fecha y hora en que se emite un Certificado (o en una fecha y hora posterior confirmadas en el Certificado) y termina con la fecha y la hora en que dicho Certificado expira o se revoca prematuramente.                                                                                                                                                         |
| Infraestructura de Llave Pública (PKI)                | La arquitectura, organización, técnicas, prácticas y procedimientos que, en conjunto soportan la implementación y operación de un sistema criptográfico de llave pública basado en Certificados.                                                                                                                                                                                             |
| Tercera Parte que Confía                              | Una persona u organización que actúa confiando en un Certificado y/o en una firma digital.                                                                                                                                                                                                                                                                                                   |
| Suscriptor                                            | Entidad que requiere los servicios prestados una TSA y que ha aceptado explícita o implícitamente sus términos y condiciones                                                                                                                                                                                                                                                                 |

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PÚBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |

|                                                                                                                  |                                                                                  |                     |           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------|-----------|
| <br><b>DOCUMENTO<br/>PUBLICO</b> | <b>DECLARACIÓN PRÁCTICAS DE<br/>CERTIFICACIÓN DE SELLO DE TIEMPO<br/>(PCSTS)</b> | <b>CPSTS</b>        |           |
|                                                                                                                  |                                                                                  | Fecha de Aprobación | Mayo 2025 |
|                                                                                                                  |                                                                                  | Página              | 34 de 34  |

| Término                              | Definición                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-Sign                               | E-Sign S.A., empresa con domicilio en la República de Chile y/o cualquier subsidiaria de propiedad de E-Sign responsable de las operaciones concretas en cuestión.                                                                                                                                                                                                                                                                             |
| Persona de confianza                 | Un empleado, contratista o consultor de una entidad dentro de E-Sign responsable de la gestión de confiabilidad de la infraestructura de la entidad, sus productos, sus servicios, sus instalaciones y/o sus prácticas.                                                                                                                                                                                                                        |
| Posición de confianza                | Una posición dentro de una entidad E-SIGN que debe ser ejercido por una persona de confianza.                                                                                                                                                                                                                                                                                                                                                  |
| Sistema de confianza                 | Hardware, software y procedimientos que están razonablemente a salvo de intrusos y mal uso, proporcionan un nivel razonable de disponibilidad, confiabilidad y buen funcionamiento, son razonablemente adecuados para el desempeño de sus funciones previstas y hacen cumplir la política de seguridad aplicable. Un sistema confiable no es necesariamente un "sistema fiable" como se reconoce en la nomenclatura gubernamental clasificada. |
| Token de sellado de tiempo (TST)     | Objeto de datos que vincula una representación de un dato a un momento en particular, estableciendo así evidencia de que el dato existió antes de ese momento.                                                                                                                                                                                                                                                                                 |
| Autoridad de Sellado de Tiempo (TSA) | La Autoridad de los Servicios de Sellado de Tiempo, que emite Tokens de Sellado de Tiempo.                                                                                                                                                                                                                                                                                                                                                     |
| Unidad de Sellado de Tiempo (TSU)    | Conjunto de hardware y software que se gestiona como una unidad y tiene una única llave para firma de tokens de sellado de tiempo activa a la vez.                                                                                                                                                                                                                                                                                             |
| Declaración de divulgación de la TSA | Conjunto de declaraciones sobre las políticas y prácticas de una TSA que particularmente requieren énfasis o divulgación a los suscriptores y partes que confían                                                                                                                                                                                                                                                                               |
| Declaración de práctica de la TSA    | Declaración de las prácticas que emplea una TSA para emitir tokens de sellado de tiempo                                                                                                                                                                                                                                                                                                                                                        |
| Sistema TSA                          | Conjunto de productos y componentes de TI organizados para implementar la prestación de Servicios de Sellado de Tiempo                                                                                                                                                                                                                                                                                                                         |

|                       |                      |                             |                    |
|-----------------------|----------------------|-----------------------------|--------------------|
| <b>Elaborado por:</b> | <b>Aprobado por:</b> | <b>Lugar de Archivo</b>     | <b>USO PUBLICO</b> |
| CISO                  | COMITÉ DE SEGURIDAD  | Redmine – Proyecto Webtrust |                    |