Declaración de Prácticas de Sellado de Tiempo

(DPST ECERT)

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
G.A.M. TSA	4.13 Requisito PO02 - Declaración de prácticas de sello de tiempo	TSA: Servicio de Certificación de Sello de Tiempo	PC-TSA-0001
		TSA: Servicio de Certificación de Sello de Tiempo	

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	15-09-2025	25-09-2025	25-09-2025	6	22-03-2021

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Product Owner	Chief Technology Officer	Gerente General	Gerente de Cumplimiento y Consultoría	Público

CONTENIDO

1 INTRODUCCIÓN

EMPRESA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA SpA, en adelante “ECERT", es una filial de la Cámara de Comercio de Santiago (CCS) fundada en el año 2000, cuyo enfoque es ser un aliado estratégico para todos nuestros clientes, brindándoles servicios basados en soluciones de firma electrónica e identidad digital en Latinoamérica.

El propósito de la presente Declaración de Práctica de Sellado de Tiempo es establecer y definir las normas, procedimientos y prácticas que la Autoridad de Sellado de Tiempo ECERT deberá seguir en la prestación de servicios de sellado de tiempo. Este documento establece un marco normativo que garantiza la confianza, integridad y seguridad de los sellos de tiempo emitidos, así como el cumplimiento riguroso de las normativas y estándares vigentes en el ámbito de la firma electrónica y la seguridad informática, conforme a lo dispuesto en la Ley N° 19.799 y su normativa complementaria

La Declaración de Prácticas de Sello de Tiempo descrita a continuación establecen el ciclo de vida de los sellos de tiempo. Esto abarca desde la gestión de la solicitud de un sello de tiempo y la obtención de un tiempo confiable, hasta la emisión del sello solicitado. Estas políticas se basan en buenas prácticas que brindan seguridad y confianza en los sellos de tiempo y servicios de certificación proporcionados por ECERT.

Este documento está dirigido a:

- Solicitantes del sello de tiempo: Es la persona, entidad u organización que solicita un sello de tiempo a la TSA para aplicarlo a un documento o a un conjunto de datos.
- Auditores y reguladores: Quienes supervisan las actividades de la TSA para asegurarse de que cumpla con las políticas, normativas y estándares establecidos.

La “Declaración de Prácticas de Sello de Tiempo de ECERT “(PC-TSA-0001) se ha preparado de conformidad con el artículo 6 del Decreto 181 de 2002: Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma. De manera complementaria se han utilizado los siguientes documentos:

- Guías de Evaluación “Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo”, entregado por el Ministerio de Economía, Fomento y Turismo.
- RFC 3628 “Policy Requirements for Time-Stamping Authorities” ETSI TS 102 023 “Electronic Signatures and infraestructures (ESI) Policy Requirements for Time-Stamping Authorities”.
- La estructura de los sellos de tiempo generados se ajusta al documento RFC 3161 “Internet X.509 Public Key Infraestructure Time Stamping Protocol (TSP) y con el Decreto Supremo 181 de 2002, del Ministerio de Economía, Fomento y Turismo.

1.1 Presentación

La presente declaración de prácticas de Sellado de Tiempo ECERT (PC-TSA-0001) en adelante “DPST de ECERT”, describe la forma en que se cumplen estos requisitos relacionados con el ciclo de vida del Sello de Tiempo en base a la Ley 19.799.

ECERT ha establecido una Política General de Seguridad de la Información (PO-GER-0003) acorde con el modelo de confianza requerido.

La actividad de Certificación de Sellado de Tiempo que realiza ECERT se encuentra acreditada por la Entidad Acreditadora desde el año 2016, mediante la Resolución Exenta Nº 3779, de la Subsecretaría de Economía del Gobierno de Chile.

1.2 Identificación

El presente documento establece la Declaración de Prácticas de Certificación de Sello de Tiempo (PC-TSA-0001) de la EMPRESA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA SpA, en adelante “DPST de ECERT".

Esta “DPST de ECERT” está registrada con el número único (OID) 31725 el que identifica únicamente a ECERT en un contexto global, según registro en la Internet Assigned Number Authority (IANA).

1.3 Comunidad de Usuarios y aplicabilidad

1.3.1 Comunidad de usuarios

1.3.1.1 Autoridad de Sellado de tiempo (TSA)

Corresponde a las entidades que están autorizados para emitir sellos de tiempo. ECERT está constituido como Autoridad de Certificación de Sello de Tiempo de conformidad con la ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma y su Reglamento, Decreto Supremo Nº 181, de 2002, del Ministerio de Economía, Fomento y Turismo, según da cuenta la R.A. Exenta No. 3779, de 24 de noviembre de 2016, de la Subsecretaría de Economía, Fomento y Reconstrucción.

1.3.1.2 Autoridad de Certificación (CA)

Corresponde las entidades que emiten certificados digitales, en algunos casos una CA puede operar una TSA como parte de sus servicios de infraestructura de clave pública (PKI), por tanto, una CA puede emitir tanto, certificados digitales para la firma digital como, sellos de tiempo para garantizar la integridad temporal de los documentos.

1.3.1.3 Solicitante del sello de tiempo

Entidad u organización que solicita un sello de tiempo a la TSA para aplicarlo a un documento o a un conjunto de datos. Puede ser un usuario final, una empresa o una aplicación que necesita asegurar la autenticidad y la integridad temporal de la información.

1.3.1.4 Partes que Confían

Entidad u organización que solicita un sello de tiempo a la TSA para entidades que pueden ser individuos, empresas, sistemas u otro tipo, que son receptores de un sello de tiempo generado por la autoridad de sellado de tiempo.

Una parte que confía no es necesariamente un titular, puede ser cualquier individuo, empresas, sistemas y otro tipo que libre y voluntariamente decide confiar en un sello de tiempo.

1.3.1.5 Otros Participantes

Entidad Acreditadora: Es la Subsecretaría de Economía y Empresas de Menor Tamaño. Su misión es acreditar y supervisar a las certificadoras.

Certificado de la TSA (TSA certificate): Este certificado es utilizado por la TSA para firmar digitalmente los sellos de tiempo que emite. Garantiza que los sellos de tiempo son auténticos y no han sido alterados desde su emisión.

Verificador del sello de tiempo: Es la entidad o el software que verifica la validez y la integridad de un sello de tiempo emitido por la TSA. Puede ser parte del proceso de autenticación de documentos digitales o sistemas que utilizan sellos de tiempo para asegurar la trazabilidad y la no repudiación de eventos.

1.3.2 Aplicabilidad de los certificados

1.3.2.1 Usos apropiados del certificado

La Ley N°19.799 regula la firma electrónica en Chile y establece disposiciones sobre los documentos electrónicos y su valor legal. En el contexto de la Autoridad de Sellado de Tiempo (TSA), su uso apropiado según esta ley se centra en asegurar la integridad, la autenticidad temporal y no repudio de los documentos electrónicos.

El uso de los sellos de tiempo está limitado a demostrar que un documento o una serie de datos han existido y asegura que el evento quede registrado con una marca temporal precisa de fecha y hora en la que ocurrió.

Por tanto, sus principales usos incluyen la garantía de la integridad y la autenticidad temporal de los documentos electrónicos, asegurando que sean válidos y confiables en el ámbito legal, financiero y comercial.

1.3.2.2 Usos prohibidos de los certificados

Tenga en consideración que la Ley N°19.799 no enumera específicamente los usos prohibidos de la TSA, sin embargo, su operación y utilización deben alinearse con los principios de integridad, autenticidad y cumplimiento normativo. Cualquier uso que vaya en

contra de estos principios podría considerarse inapropiado y estar sujeto a acciones legales o regulatorias correspondientes.

1.4 Cumplimiento

La TSA de ECERT hace referencia a la Política de sellado de tiempo (MI-TSA-0037) establecida por ECERT en cada uno de los sellos emitidos. La Entidad Acreditadora lleva a cabo una inspección anual ordinaria de la TSA de ECERT para garantizar la correcta aplicación de la Declaración de Prácticas de TSA (PC-TSA-0001) y Política de sellado de tiempo (MI-TSA-0037). Además, se verifica la implementación de los controles y procedimientos definidos en las practicas, con el objetivo de asegurar la confianza en los sellos de tiempo emitidos.

1.5 Detalles de contacto y Administración de la TSA

1.5.1 Organización que administra el documento

Razón social: EMPRESA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA SpA.
Dirección social: Monjitas 392 Piso 17, comuna y ciudad de Santiago de Chile.

1.5.2 Contacto

Página Web: www.ecertla.com
Teléfono: 6003620400
Mail: mesasoporte@ecertchile.cl

1.5.3 Procedimiento de aprobación de la DPST

Cualquier nueva versión de esta “DPST de ECERT” estará sujeta a un procedimiento de aprobación que incluye los siguientes pasos:

1) Elaboración y aprobación interna de la nueva versión.
2) Presentación de esta "DPST de ECERT" al Comité de Sistema de Gestión de ECERT.
3) Después de obtener las aprobaciones mencionadas, se publicará la nueva versión de esta "DPST de ECERT", en la página web de ECERT, indicando la fecha de entrada en vigor.

Una vez que se publique la nueva "DPST de ECERT", se informará a la Entidad Acreditadora sobre los cambios realizados en caso de corresponder a cambios Materiales y en conformidad al inciso tercero del artículo 18° de la ley 19.799.

1.6 Definiciones y acrónimos

Para facilitar la comprensión de las definiciones y acrónimos empleados en este documento, consulte la siguiente tabla:

Definiciones	Acrónimos
Autoridad de Sellado de Tiempo	TSA
Servicio de sellado de tiempo	TSS
Token de sello de tiempo	TST
Tiempo universal coordinado	UTC
Unidad de sello de tiempo.	TSU
Declaración de Prácticas de Sellado de Tiempo	DPST
Política de Sellado de Tiempo	PST
Centro de Procesamiento de Datos	CPD
Public Key Infrastructure (Infraestructura de clave pública)	PKI

2 OBLIGACIONES Y RESPONSABILIDADES

2.1 Obligaciones

2.1.1 Obligaciones de la TSA ECERT

En su calidad de autoridad de sellado de tiempo se obliga a:

a) Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los sellos de tiempo en los términos establecidos en la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

b) Cumplir y respetar los procedimientos establecidos en las Prácticas de Certificación de Sellado de Tiempo "DPST DE ECERT" (PC-TSA-0001).

c) Cumplir con todas las otras obligaciones establecidas en la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éste.

d) Garantizar el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC puede tener una desviación máxima de 1 segundo.

e) Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, así como, también del hardware criptográfico.

f) Mantener un identificador único para cada sello de tiempo emitido, así como incluir una referencia a la política bajo la cual fue emitido.

g) Mantener sincronizado el reloj de la unidad de sellado de tiempo con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.

h) Mantener los controles de seguridad física, de procedimiento y personales definidos para el sellado de tiempo.

i) Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de acuerdo con la información conocida en el momento de su emisión.

j) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.

k) Garantizar mediante revisiones y auditorias que todos los requerimientos de la autoridad de sellado de tiempo cumplen con los controles requeridos por la legislación aplicable, Práctica de Certificación de Sellado de Tiempo "DPST DE ECERT" (PC-TSA-0001). y los procedimientos internos de ECERT.

l) Informar.

m) El algoritmo de hash utilizado en lo sellos de tiempo.

n) La precisión del tiempo utilizado como parte del proceso de certificación de los sellos de tiempo.

o) Los mecanismos de verificación de los tokens emitidos por ECERT.

p) El período de permanencia de los logs que maneja la autoridad de sellado de tiempo.

q) Mantener www.ecertla.com con información para el público sobre los servicios de ECERT.

2.1.2 Obligaciones del titular

El titular se obliga a:

a) Conocer y aceptar las normas establecidas en la Declaración de Prácticas de TSA (PC-TSA-0001) y Política de sellado de tiempo (MI-TSA-0037), antes de proceder con la emisión del sello de tiempo.

b) Verificar que el token de time-stamping se ha firmado correctamente, confirmando la validez de la clave privada de la TSA que firma dicho token mediante la consulta a la Lista de Revocación de Certificados (CRL) o el servicio OCSP, y asegurando que no ha sido comprometida.

c) Pagar la tarifa asociada al servicio de Sellado de Tiempo.

d) Conocer el propósito y alcance de los sellos de tiempo emitidos por ECERT.

e) Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado o a los sellos de tiempo emitidos, lo cual debe ser considerado como causa de revocación de éste.

f) Conocer y aceptar los términos, condiciones y límites contenidos en DPST de ECERT.

2.1.3 Obligaciones de la parte que confía

Las partes que confían se obligan a:

a) Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la autoridad de sellado de tiempo y su periodo de validez.
b) Conocer el propósito y alcance de los sellos de tiempo emitidos por ECERT.

2.2 Responsabilidades

2.2.1 Responsabilidades Legales

ECERT cumple con la normativa vigente y cuenta con un seguro de responsabilidad civil adecuado garantizando así una cobertura suficiente de su responsabilidad. De este modo, sólo responderá por los daños y perjuicios que en el ejercicio de su actividad se ocasionen por la certificación u homologación de certificados de firmas electrónicas, en el artículo 14 de la Ley 19.799 y el Decreto supremo 181 de 2002, del Ministerio de Economía, Fomento y Turismo.

ECERT nunca responderá por los daños y perjuicios que tengan su origen en el uso indebido o fraudulento del servicio de sellado de tiempo.

2.2.2 Responsabilidades generales

ECERT como prestador de servicios de certificación ciñe sus responsabilidades legales de acuerdo a las siguientes leyes chilenas:

- Ley 19.799 “Ley sobre Documentos Electrónicos, Firmas Electrónicas y Servicios de Certificación de Firmas Electrónicas".
- Ley 19.628 "Ley sobre Protección de la Vida Privada".
- Ley 19.496 “Ley de protección de los derechos de los consumidores”

2.2.3 Fuerza mayor

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

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

Para los efectos de esta "DPST de ECERT" se entenderá por caso fortuito o fuerza mayor lo dispuesto en el artículo 45 del Código Civil, lo que incluye guerras, desastres naturales, estallidos sociales, pandemias, paros, huelgas o suspensión de laborales del personal de ECERT o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

2.2.4 Disposiciones de resolución de disputas

Cualquier duda, conflicto, diferencia o dificultad que surja entre las partes con motivo de la aplicación, extensión interpretación, vigencia, cumplimiento, terminación o resolución de esta Declaración será conocida por un mediador designado de común acuerdo por las partes, el que deberá ser un profesional de reconocido prestigio.

En caso de que no se llegue acuerdo en el nombre del mediador o habiéndose designado, éste no haya solucionado la diferencia, dificultad, problema o controversia en el plazo de 30 días hábiles, contados desde la fecha de aceptación del encargo, ésta será resuelta definitivamente por un árbitro, quien tendrá la calidad de arbitrador en cuanto al procedimiento y de derecho en cuanto al fallo. El arbitraje se llevará a cabo en la ciudad de Santiago.

El árbitro deberá ser designado de común acuerdo por las partes. A falta de acuerdo respecto de la persona del árbitro, éste deberá ser designado, a solicitud escrita de cualquiera de las partes, por cualquier juzgado con competencia en el territorio jurisdiccional de la Corte de Apelaciones de Santiago que esté de turno al momento de solicitarse el nombramiento, pero en este último caso, el nombramiento deberá recaer necesariamente en algún abogado que se desempeñe o se haya desempeñado como profesor de Derecho y Tecnología de las Facultades de Derecho de las Universidades acreditadas ante el Consejo de Rectores. Las Partes establecen que el árbitro queda especialmente facultado para resolver todo asunto relacionado con su competencia y/o jurisdicción.

El árbitro aplicará las normas establecidas en el Código de Procedimiento Civil, en el Código Orgánico de Tribunales y en la Ley N°20.886 sobre Tramitación Electrónica. Se hace expresa mención por las partes que, el árbitro al momento de proponer sus honorarios éstos habrán sido establecidos siguiendo la tabla de aranceles del CAM Santiago.

Se entenderá que no se ha llegado a acuerdo en el nombramiento del mediador o árbitro, según sea el caso, si es que cualquiera de las partes requiere a su contraparte por escrito, en el plazo de 15 días corridos, el nombramiento de un mediador y/o árbitro y no hubiere respuesta o constancia de ese nombramiento de común acuerdo.

2.2.4.1 Separación y divisibilidad de cláusulas

En el evento que alguna disposición contenida en las "DPST de ECERT" sea declarada nula, inoponible o cualquier otra causa de ineficacia jurídica, se deja constancia que dicha declaración solo afecta la norma en particular, dejando vigente en su integridad el resto del documento.

2.2.4.2 Conflicto de normas

En caso de producirse un conflicto de normas, se seguirá el siguiente orden de precedencia:

a) Ley 19.799.
b) Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo que reglamenta la Ley 19.799.
c) "CPST ECERT" vigente.
d) Otros documentos relacionados con la prestación de servicios de certificación.

2.3 Tarifas

El Solicitante deberá pagar las tarifas correspondientes al servicio de Sellado de Tiempo. Estas tarifas cubren las actividades que ECERT realiza para gestionar el ciclo de vida de la TSA contratada bajo el modelo de compra por volumen de certificados de sellos de tiempo, adquiridos por una empresa o institución para sus clientes o colaboradores. Las tarifas y condiciones específicas se acordarán de manera individual en cada caso y estarán

debidamente establecidas en el contrato correspondiente, reflejando los términos y acuerdos alcanzados entre las partes.

2.3.1 Política de reembolso

Según lo dispuesto en el artículo 3 bis, letra b) de la Ley 19.496 sobre derechos de los consumidores, el derecho de retracto no procede, dado el servicio de sellado de tiempo es un complemento de los certificados, los que son elaborados por la Autoridad de Certificación conforme a las especificaciones proporcionadas por el Solicitante.

2.4 Publicaciones y repositorios

El repositorio que alberga las políticas, prácticas y documentación asociadas al Servicio de Sellado de Tiempo será ahora parte del Sistema de Gestión Integrado (SGI) de ECERT. Esta plataforma centralizada permitirá el acceso interno al personal corporativo, asegurando la trazabilidad y gestión adecuada de la información. Aquellos documentos que corresponda disponibilizar de forma pública estarán accesibles a través del sitio web institucional.

2.4.1 Publicación de información de certificación

ECERT realiza la publicación de la información relativa a Sellado de Tiempo a través de la página web https://www.ecertla.com sección “Políticas y Prácticas de ecert”. Las partes que confían pueden encontrar la siguiente información:

a) Declaración de Prácticas de Sellado de tiempo (PC-TSA-0001).
b) Política de Sellado de Tiempo (MI-TSA-0037).
c) Política General de Seguridad de la Información (PO-GER-0003).

2.4.2 Tiempo o frecuencia de publicación

La publicación de la información de ECERT, que incluye la Declaración de Prácticas de TSA (PC-TSA-0001) y Política de sellado de tiempo (MI-TSA-0037), se debe realizar tan pronto como esté disponible. Los cambios en la Declaración de Prácticas de Sellado de Tiempo se rigen por lo dispuesto en el punto 1.5 de este documento.

2.4.3 Controles de acceso a los repositorios

ECERT no restringe el acceso de lectura a la información definida en el punto 2.2; no obstante, implementa controles para evitar que personas no autorizadas puedan agregar, modificar o eliminar registros publicados. Esto se hace para salvaguardar la integridad y autenticidad de la información.

Por ello, se utilizan sistemas confiables para el repositorio con el fin de:

a) Permitir únicamente a personas autorizadas realizar anotaciones y modificaciones.
b) Verificar la autenticidad de la información.
c) Detectar cualquier cambio técnico que afecte los requisitos de seguridad.

2.4.4 Plazo

Esta “DPST de ECERT” puede modificarse según sea necesario para garantizar su actualización tecnológica y para mejorar la forma en que se lleva a cabo la actividad, ya sea mediante la introducción de mejoras en las instalaciones, sistemas, programas informáticos o recursos humanos utilizados. Estas actualizaciones o revisión se realizarán, a lo menos, una vez al año.

Toda modificación realizada a esta “DPST de ECERT” debe entrar en vigencia a partir de la fecha en que se publica en www.ecertla.com.

2.5 Auditorias de Cumplimiento

ECERT, en su calidad de certificador acreditado en Sellado de Tiempo, es inspeccionado anualmente por la Entidad Acreditadora para mantener vigente la acreditación obtenida en el año 2016.

Adicionalmente, realiza auditorías a su instalaciones y sistemas como parte de sus certificaciones ISO 9001 y ISO/IEC 27001, comprometiéndose a corregir dentro de un plazo razonable, las eventuales deficiencias que se puedan encontrar.

Además, ECERT audita periódicamente, ya sea directamente o a través de empresas especialmente contratadas, a nuestras Autoridades de Registro, asegurando así la máxima confianza y seguridad en nuestros servicios.

2.6 Privacidad de la información personal

La privacidad de la información es fundamental y con el objetivo de protegerla adecuadamente ECERT, ha desarrollado una Política de Tratamiento de Datos (PO-GER-0008) que detalla cómo gestiona los datos personales, cumpliendo con el marco legal establecido por la Ley 19.799 y en los términos definidos por la Ley 19.628 y que pueden ser consultados en la página web https://www.ecertla.com sección “Políticas y Prácticas de ecert”.

Los datos personales que ECERT trata son antecedentes personales, antecedentes demográficos y datos recolectados a través de tecnologías de cookies a través de su sitio Web.

Para el caso del servicio de Sellado de Tiempo, la información que se procesa no corresponde datos personales establecidos en la Ley 19.628.

2.7 Derechos de propiedad intelectual

ECERT reconoce y protege los derechos de propiedad intelectual e industrial en el ámbito de la tecnología, derechos que son fundamentales para fomentar la innovación, asegurar competitividad y mantener la posición de liderazgo del servicio.

Es por ello que ECERT es el Titular exclusivo de todos los derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas en el marco de la prestación de los servicios de certificación. Ningún derecho de propiedad intelectual o industrial preexistente o adquirido por ECERT será transferido a las entidades mencionadas en el punto 1.5 Entidades.

Los Solicitantes y Partes que confían no podrán utilizar el nombre, marca o logo de ECERT para publicidad o cualquier otro propósito sin el consentimiento expreso y por escrito de

ECERT. Cualquier uso deberá ser previamente acordado mediante un acuerdo escrito que defina el alcance y las condiciones específicas de dicho uso.

3 REQUERIMIENTOS EN PRÁCTICAS DE LA TSA

3.1 Declaración de Prácticas y de divulgación

3.1.1 Declaración de Prácticas de TSA

La Autoridad de Sellado de Tiempo (TSA) ECERT ha desarrollado una planificación orientada a mitigar los riesgos identificados durante el proceso de evaluación y análisis de riesgos. Esta planificación está alineada con las políticas y prácticas que regulan el servicio, considerando los roles y responsabilidades de los actores involucrados, el personal encargado de la prestación del servicio, así como los aspectos técnicos, documentales y organizativos. Se ha establecido el Comité de Sistema de Gestión Integrado (CSGI) como mecanismo de control, el cual también garantiza el cumplimiento de las normativas legales que rigen la actividad de la TSA.

3.1.2 Declaración de divulgación de TSA

La presente declaración de prácticas de sello de tiempo describe los controles que ECERT ha implementado para cumplir con la Política de sellado de tiempo (MI-TSA-0037), garantizando fiabilidad y confianza del servicio de sellos. Los objetivos de la Declaración de Practica son:

- Establecer estándares y procedimientos: Definir claramente los estándares técnicos y los procedimientos operativos que la TSA debe seguir al emitir sellos de tiempo. Esto garantiza consistencia y calidad en el servicio.
- Garantizar la precisión temporal: Especificar métodos para asegurar que los sellos de tiempo reflejen de manera precisa y confiable el momento en que se aplican a los datos o documentos.
- Seguridad y protección: Establecer medidas de seguridad adecuadas para proteger la infraestructura y las claves criptográficas utilizadas en la generación de sellos de tiempo, asegurando la confidencialidad e integridad de la información.
- Responsabilidades y roles: Definir claramente las responsabilidades y obligaciones de la TSA, así como los derechos y deberes de los usuarios de los sellos de tiempo.
- Cumplimiento normativo: Asegurar que la TSA cumpla con las normativas legales, regulaciones y estándares relevantes relacionados con la emisión de sellos de tiempo.
- Auditoría y revisión: Establecer requisitos para la auditoría y revisión periódica de las operaciones de la TSA para garantizar el cumplimiento de las políticas y estándares establecidos.
- Gestión de incidentes: Definir procedimientos claros para manejar y responder a incidentes de seguridad que puedan comprometer la integridad de los sellos de tiempo emitidos.
- Un punto de contacto para presentar reclamos al servicio.
- Transparencia y confianza pública: Promover la transparencia en las operaciones de la TSA para construir y mantener la confianza pública en los sellos de tiempo emitidos y en la autoridad que los emite.

ECERT realiza la publicación de la información relativa a Sellado de Tiempo a través de la página web https://www.ecertla.com/. Las partes que confían pueden encontrar la siguiente información:

- Declaración de Prácticas de Sellado de tiempo (PC-BIO-0001).
- Política de Sellado de Tiempo (MI-TSA-0037).
- Política General de Seguridad de la Información (PO-GER-0003).

3.2 Ciclo de vida del Sellado de tiempo

3.2.1 Generación de la llave Unidad de Sellado de Tiempo (TSU)

El módulo criptográfico de ECERT es capaz de generar llaves en base al algoritmo de encriptación de llave publica SHA1RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS_COP.1.

Para acceder a funcionalidades del equipo HSM Cryptosec TSA sobre el que se ejecutan las operaciones se utilizan estos medios físicos de protección lógica (ACS y OCS). Ellos 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 certificadora, bajo las ACS y OCS, 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. Con respecto a este quórum se establece una cantidad de token físicos para poder realizar tareas sobre el material criptográfico en el equipo HSM Cryptosec TSA, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso de que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 2 de 4 token.

La llave usada por la unidad de sellado de tiempo es generada de acuerdo con la Práctica de Sellado de Tiempo ECERT (DPST de ECERT) definidas para el proceso de sellado de tiempo, utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la autoridad de sellado de tiempo 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 acezado por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de Llaves del equipo HSM.

ECERT declara que satisface los requerimientos identificados en CEN Workshop Agreement 14167-2 [CWA 14167-2] o ISO 15408 al cumplir con la ETSI TS 102 042 que fue la que dio origen al ciclo de vida de la llave aquí descrito.

3.2.2 Protección de la llave privada de la Unidad de Sellado de Tiempo (TSU)

La autoridad de sellado de tiempo lleva a cabo un conjunto de acciones de manera tal de asegurar que la llave privada de la unidad de sellado de tiempo usada para firmar los sellos de tiempo permanezca 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, ella es copiada, almacenada y recuperada sólo por el personal con roles de confianza y bajo un ambiente seguro.

La autoridad de sellado de tiempo 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 ECERT cumplen el estándar FIPS 140-2 Nivel 3.
- Control de la llave privada: Las claves privadas utilizadas por la autoridad de sellado de tiempo y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 2 personas de un total de 6 para modificar el ambiente criptográfico.
- Depósito de la llave privada: La clave privada está cifrada y queda contenida en el repositorio asociado a 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 certificadora. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- Introducción de la clave 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 entidades de ECERT que hacen uso de dichos módulos.
- Método de activación de la clave privada: Las claves privadas de la autoridad de sellado de tiempo y que componen sus jerarquías, se activan mediante la inicialización del software de la certificadora y la activación del hardware criptográfico que contiene las claves.
- Método de desactivación de la clave privada: Un Administrador puede proceder a la desactivación de la clave privada de las certificadora o de sus claves intermedias (Clave de la autoridad de sellado de tiempo), mediante la detención del software de la certificadora.
- Método de destrucción de la clave privada: Existe un procedimiento de destrucción de claves de la autoridad de sellado de tiempo, así como de las claves intermedias de la jerarquía.

En lo que respecta a la generación de la llave de la unidad de sellado de tiempo, el módulo criptográfico utilizado mantiene la confidencialidad de la llave en su ciclo de tiempo completo, restringiendo el acceso a éste al personal autorizado solamente. De detectarse un acceso no autorizado, este se registra ya sea de manera física (tampering físico) o a través de log a ser usado durante la auditoría. Este equipo contempla además mecanismos de backup y respaldo de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos. ECERT declara cumplir con el documento "CEN Workshop Agreement 14167- 2 [CWA 14167- 2]" o ISO 15408 en lo correspondiente al ciclo de vida de su llave criptográfica, realizando la implantación de estos controles de acuerdo a la norma ETSI TS 102 042.

3.2.3 Distribución de la llave Pública

El certificado digital utilizado por la autoridad de sellado de tiempo es generado por la certificadora de acuerdo a las Prácticas de Certificación de Sellado de Tiempo ECERT (DPST ECERT) auditadas por la Entidad Acreditadora.

La confianza en una certificadora se establece mediante la instalación del certificado raíz de la unidad de sellado de tiempo en la cual se desea confiar. ECERT, como parte de los servicios que provee a sus clientes y terceros, publica en su sitio web los certificados raíces necesarios para la validación del sellado de tiempo.

Estos certificados están disponibles en el sitio web de ECERT y pueden ser descargados a través de una conexión segura (HTTPS). Una vez descargados, deben ser instalados en el repositorio de confianza del tercero que confía. Esto permitirá validar cualquier sello emitido por la certificadora, ya que el certificado raíz contiene la llave pública necesaria para verificar la autenticidad del sello.

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

- Se descarga certificado raíz de la autoridad de sellado de tiempo que ha emitido el sello a validar. Este certificado debe ser descargado a través de un canal seguro, que debe poseer el sitio de descarga de dicha raíz. Descargado el certificado raíz, este se procede a instalar en las emisoras raíz de confianza del equipo cliente.
- El sistema indicará si la importación e instalación del certificado ha sido correcta. De ser así, cualquier mensaje que sea firmado con un certificado de sello de tiempo, que ha sido emitido y firmado con esta raíz, podrá ser validado automáticamente en el equipo cliente. Una forma de validación adicional a esta instalación es verificar si el almacén de raíces de confianza incluye a este certificado recién instalado.

Al estar el certificado de la autoridad de sellado de tiempo instalado en el repositorio de confianza del cliente, cualquier sello que haya sido emitido y firmado por esta autoridad de sellado de tiempo podrá ser validado por el cliente, ya que el certificado raíz de la autoridad de sellado de tiempo contiene la llave pública que permitirá verificar el certificado emitido. Una forma de complementar esta cadena de confianza es instalar además del certificado raíz de la unidad de sello de tiempo (raíz intermedia de la certificadora), el certificado raíz de la certificadora utilizado para firmar el certificado de la unidad de sello de tiempo.

3.2.4 Reemisión de llaves de la TSU

Por motivo de seguridad y evitar el repudio a un certificado, ECERT como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo con las políticas y prácticas que rigen la operación de su CA. Sin embargo, la llave privada de la TSU será reemplazada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

3.2.5 Término del ciclo de vida de la llave del TSU

La llave privada de la unidad de sellado de tiempo será reemplazada al momento de su expiración. La unidad de sello de tiempo rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida.

ECERT tiene la capacidad de revocar el certificado raíz activo de la unidad de sello de tiempo, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por cese de actividades.

En el evento que ECERT vaya a descontinuar sus operaciones como autoridad de sellado de tiempo procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sellado de tiempo: titulares, terceros que confían y autoridades de sello de tiempo acreditadas.

ECERT comunicará a cada uno de sus titulares 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.

ECERT 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 los certificados de la unidad de sellado de tiempo 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 unidad de sello de tiempo, así como sus respaldos son destruidos inmediatamente al momento del cese de la actividad de la autoridad de sellado de tiempo.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, se realizará en conformidad con la ley chilena.

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

Los equipos HSM de ECERT, utilizados para firmar los certificados emitidos por la unidad de sellado de tiempo y para la firma de los propios sellos de tiempo, están equipados con sistemas de detección de intrusiones, que pueden incluir sellos holográficos y/o detectores de intrusión. Para prevenir la inserción no autorizada de dispositivos en el hardware del módulo de seguridad, este dispositivo se coloca detrás de los ventiladores del HSM.

El equipo HSM cuenta con múltiples niveles de detección de intrusión física que afectan la funcionalidad criptográfica, informando de estos eventos al administrador y, en última instancia, obligando a reiniciar el equipo a su configuración de fábrica. Todos los eventos de intrusión se despliegan en la pantalla del dispositivo.

Ante la detección de cualquier evento mencionado, el equipo no debe ser puesto en producción, ya sea que los incidentes hayan ocurrido durante su almacenamiento o transporte. El administrador del equipo debe reiniciarlo a su configuración de fábrica. Posteriormente, se debe reconectar el equipo y recuperar la información clave, utilizando el quórum proporcionado por el conjunto de tarjetas de administración definidas.

En particular si se ha detectado apertura de la tapa del equipo, este genera un evento indicando dicha intrusión, lo que implica que la seguridad del equipo se ha comprometido. Bajo este escenario no se debe pasar a producción dicho equipamiento bajo motivo alguno.

Si el evento indicado, se produce durante el tránsito del equipo desde el fabricante de dicho equipo, el administrador debe contactarse inmediatamente con el fabricante. En cambio, de ocurrir este evento posterior a la instalación, adicionalmente se deben revisar las políticas y procedimientos de seguridad que permitieron dicho incidente.

Entre las revisiones que deben realizarse al equipo, tanto posterior a su transporte o durante su almacenamiento es:

- Controlar que los sellos de seguridad no han sido alterados.
- Que las tapas permanecen completamente ajustadas al chasis del equipo.
- Que no se presentan daños aparentes a la estructura general del equipo.
- Que no se detecten daños evidentes en ventilaciones del equipo o que se haya intentado
- introducir algún componente a través de estos espacios.

El equipo HSM utilizado por ECERT tanto para su certificadora como para su autoridad de sellado de tiempo implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

Para acceder a funcionalidades del equipo HSM, sobre el que se ejecutan las operaciones de instalación, respaldo y recuperación, 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 certificadora para la generación del certificado de la unidad de sello de tiempo, 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. Con respecto a este quórum se establece una cantidad de tarjetas físicas para poder realizar tareas en el equipo HSM sobre el material criptográfico, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso de que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 2 de 4 token.

Una vez instalado de manera exitosa el hardware y software asociado al HSM, ECERT ha definido como criterio de verificación del correcto funcionamiento de los equipos, la emisión de un certificado de prueba, partiendo desde su solicitud hasta su emisión y a continuación la revocación del mismo. Con este ciclo se probará la correcta generación de claves, servicios OCSP y listas de revocación de certificados. Una vez desarrollada esta actividad, se podrá proceder a generar las llaves intermedias utilizadas por los distintos servicios de la PSC, en particular para este caso, la llave de la unidad de sello de tiempo utilizada para la firma de los sellos de tiempo a emitir.

Finalmente, en caso de requerir mover el equipo a otra instalación o el envío del mismo a la fábrica por motivos de garantía, ECERT ha definido que se debe dejar el equipo a sus condiciones originales que tenía a la salida de fábrica, borrando con ello todo su contenido de configuraciones interna del equipo HSM. En particular, para el caso de equipos, esto se puede realizar a través del menú de opciones de administración, opción “factory state”. Esto llevará a que el equipo borre todo su contenido. Lo anterior no afectará el “Security Word”

data almacenada en el RFS, por tanto, en caso de no existir intrusión, el contenido de dicho equipo puede ser restaurado a partir de esta data más las llaves ACS y el quórum definido.

3.2.7 Deberes y procedimientos asociados al ciclo de vida de los Sello de Tiempo

A continuación, se definen los deberes y procedimientos asociados al ciclo de vida de los sellos de tiempo:

- Emisión: El solicitante presenta una solicitud para obtener un certificado de firma electrónica, el cual se genera una vez que la Autoridad de Registro ha realizado de manera satisfactoria la validación fehaciente de su identidad. En consecuencia, solicita a la Autoridad de Certificación que emita y entregue el certificado al solicitante, basándose en la información contenida en la solicitud previamente presentada.

  Además, dado que el servicio de Sello de Tiempo complementa el servicio de Firma Electrónica Avanzada, los procedimientos de identificación y autenticación (descritos en el anterior párrafo) de los solicitantes de Sello de Tiempo son idénticos a los detallados en la Declaración de Prácticas de Certificación (PC-FEA-0001) y en las Políticas de Certificación de Firma Electrónica Avanzada (MI-FEA-0029).

- Revocación: La llave privada de la TSU debe ser reemplazada antes de su expiración o ante un evento de seguridad que vulnere dicha llave, lo que lleva a una revocación de esta. La TSU rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada se haya revocado. Después de revocada, la llave privada es destruida al igual que sus copias de respaldo, a fin de que su clave privada no pueda ser recuperada.
- Suspensión: La suspensión de certificados no aplica para TSA.
- Renovación: Por motivos de seguridad y para evitar el repudio de un certificado, ECERT, como Prestador de Servicios de Certificación (PSC), no realiza la reemisión de llaves una vez que se ha generado el certificado de la Tarjeta de Suscriptor Único (TSU), de acuerdo con las políticas y prácticas que rigen la operación de su Autoridad de Certificación (CA). Sin embargo, la llave privada de la TSU será renovada antes de que finalice su periodo de validez en caso de que se determine que el algoritmo o la longitud de la llave son potencialmente vulnerables, o si el certificado ha sido comprometido.

3.2.8 Expiración de los certificados

El certificado TSU utilizado para la firma con sello de tiempo tiene una vigencia de 7 años a partir de su emisión. Sin embargo, puede ser revocado anticipadamente antes de que finalice su periodo de validez en caso de que se determine que el algoritmo o la longitud de la clave son potencialmente vulnerables, o si el certificado ha sido comprometido. Al revocarse este certificado de firma de sellos de tiempo, todos los sellos de tiempo emitidos con dicho certificado se vuelven inválidos.

3.3 Sello de Tiempo

3.3.1 Token de sello de tiempo

ECERT garantiza que los tokens de sellado de tiempo son emitidos en forma segura e incluyen un identificador único de política (OID), valores de fecha y hora proveniente de una fuente confiable de tiempo UTC sincronizado en la precisión definida en esta política.

Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el titular para que sea sellado con el sello de tiempo.
- Un identificador para la política de marca de tiempo
- Un número serial único que será usado para ordenar los TST's así como para identificar un sello de tiempo específico.
- El Token de Sello de Tiempo calibrado a 1 segundo de la UTC, indicando la fuente de tiempo confiable.
- La firma electrónica que ha sido generada usando una llave que es sólo usada para la firma de los sellos de tiempo.
- La identificación de la autoridad de sellado de tiempo y de la unidad de sellado de tiempo.
- La autoridad de sellado de tiempo establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC 3161.

3.3.2 Sincronización de los relojes con UTC

La ECERT declara utilizar una fuente fiable de tiempo, mediante un servidor basado en el protocolo NTP que sincronice con el tiempo UTC a través de una red de satélites GPS o en caso excepcional contra múltiples fuentes que incluyen el "National Measurenment 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 unidad de sellado de tiempo es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la unidad de sellado de tiempo 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 certificadora.
- En caso de detectarse una desviación más allá de la precisión declarada, la unidad de sellado de tiempo no generará nuevos sellados de tiempo hasta que el tiempo correcto es restaurado.
- ECERT declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el sellado de tiempo.

3.3.3 Procedimiento de registro

Los sellos de tiempo, al formar parte del Proceso de Acreditación definido por el Regulador, implican que el procedimiento de registro de los solicitantes, que incluye su autenticación y verificación de identidad, se lleva a cabo de manera adecuada y de acuerdo con los niveles de protección requeridos, tal como se detalla en el capítulo 4 de la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada (PC-FEA-0001).

3.4 Gestión de la TSA y operaciones

3.4.1 Gestión de Seguridad

ECERT cuenta con una Política General de seguridad (PO-GER-0003), además de la certificación ISO 27001 con el objetivo de establecer buenas prácticas para la implementación de los controles técnicos específicos de seguridad de la información.

3.4.2 Gestión y clasificación de activos

ECERT ha desarrollado una Política Gestión Integral de Riesgos y Oportunidades (PO-GER-0001) y un Procedimiento Gestión de Riesgos y Oportunidades (PR-SGI-0001) los cuales son fundamentales en nuestro SGSI, los que están orientados a gestionar los riesgos identificados durante el proceso de evaluación y análisis de riesgos de los activos de la información. Esta planificación está alineada con la Política de sellado de tiempo (MI-TSA-0037) y la Declaración de Prácticas de TSA (PC-TSA-0001) que regulan el servicio de TSA, considerando los roles y responsabilidades de los actores involucrados, el personal encargado de la prestación del servicio, así como los aspectos técnicos, documentales y organizativos.

Adicionalmente, ECERT cuenta con una Política de clasificación de la información (PO-GSI-0004) que establece:

La información debe ser clasificada respecto de su confidencialidad, para ello se consideran los siguientes niveles de clasificación:

a) Confidencial (Alta): La información está restringida para ser conocida solamente por un ámbito de personas acotado al interior de la empresa, el acceso está limitado a las personas y a las acciones definidas.
b) Uso Interno (Media): La información no tiene restricciones para ser conocida al interior de la empresa, todos los empleados podrían acceder a ella, si esto es necesario para el correcto desempeño de sus funciones.
c) Público (Baja): La información no tiene restricciones para su divulgación en todo ámbito, tanto interno como externo.

3.4.3 Seguridad del Personal

3.4.3.1 Requisitos de cualificación, experiencia y autorización

Todo el personal de ECERT está adecuadamente calificado y/o instruido para desempeñar las operaciones asignadas. Aquellos en puestos de confianza no tienen intereses personales que puedan entrar en conflicto con sus responsabilidades. ECERT asegura que los

Operadores de Registro sean confiables para llevar a cabo las tareas de registro, proporcionándoles formación para ejecutar correctamente los procesos de validación de identidad de los solicitantes.

En general, ECERT removerá a cualquier colaborador de sus funciones de confianza si se detectan conflictos de interés o se cometen actos delictivos que puedan afectar su desempeño. ECERT no asignará roles de confianza o gestión a individuos no idóneos, especialmente aquellos cuya falta de competencia afecte su capacidad para el puesto. Por lo tanto, se realiza una investigación previa a la contratación según lo permita la legislación aplicable, que abarca:

a) Nivel de educación completado.
b) Experiencia laboral previa.
c) Verificación de antecedentes.

Con todo, las Autoridades de Registro pueden establecer procedimientos adicionales de verificación de antecedentes, siempre que se alineen con la legislación vigente, las políticas de ECERT, y son responsables por las acciones de las personas a las que autoricen en sus operaciones.

3.4.3.2 Roles de confianza

Para la prestación de los servicios y administración de la infraestructura se han identificado, las siguientes funciones o roles con la condición de fiables:

a) Auditor Interno: responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Operaciones TI. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la Gerencia de cumplimiento.
b) Ingeniero de Sistemas: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación, también es responsable de las operaciones de copia de respaldo y mantenimiento de la Autoridad de Certificación.
c) Jefe de Seguridad de la información: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por la Política General de Seguridad de la Información (PO-GER-0003). Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se han implementado de acuerdo con la Política de organización interna la respectiva segregación de funciones, como medida de prevención de actividades fraudulentas.

3.4.3.3 Requisitos de formación

ECERT forma al personal en roles de confianza y gestión hasta que alcancen la competencia necesaria, manteniendo un registro de esta formación.

Los programas de formación se revisan periódicamente y se actualizan para mejorarlos de manera continua.

La formación incluye, al menos, los siguientes contenidos:

a) Descripción detallada de las tareas que la persona debe llevar a cabo.
b) Políticas y procedimientos de seguridad de la información de ECERT, incluyendo el uso y operación de equipos y aplicaciones instaladas.
c) Gestión y manejo de incidentes y compromisos de seguridad de la información.
d) Procedimientos de continuidad de negocio y de emergencia.
e) Procedimientos de gestión y seguridad relacionados con el tratamiento de datos personales.

3.4.3.4 Frecuencia y requisitos de reentrenamiento

ECERT actualiza la formación del personal según las necesidades y con la frecuencia adecuada para que puedan desempeñar sus funciones de manera competente y satisfactoria. Esto se realiza especialmente cuando se introducen modificaciones significativas en las tareas de certificación.

3.4.3.5 Sanciones por acciones no autorizadas

El Reglamento Interno de Orden, Higiene y Seguridad de ECERT considera las sanciones a las que se pueden ver expuestas las personas que laboran en la certificadora.

3.4.3.6 Requisitos del contratista independiente

ECERT puede contratar a terceros para desempeñar tareas de confianza, quienes previamente deben firmar las cláusulas de confidencialidad y cumplir con los requisitos operativos establecidos por ECERT. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, resultar en la terminación del contrato.

En el caso de que todas o parte de las operaciones de certificación sean realizadas por un tercero, dicho tercero debe aplicar y cumplir con los controles y disposiciones establecidos en esta sección u otras partes de la Declaración de Prácticas de Certificación. Sin embargo, ECERT sigue siendo responsable de asegurar la ejecución efectiva de estas medidas.

Estos aspectos están formalizados en el acuerdo legal utilizado para establecer la prestación de servicios de certificación por un tercero con ECERT.

3.4.4 Seguridad física y ambiental

ECERT presta servicios de certificación a través de su infraestructura de llave pública, la cual cuenta con controles de seguridad física y ambiental. Estos controles protegen los recursos de las instalaciones, los sistemas y el equipamiento utilizado para las operaciones de servicios electrónicos de confianza.

En concreto, la Política General de Seguridad de la Información (PO-GER-0003) de ECERT aplicable a los servicios de certificación digital establece lo siguiente:

a) Controles de acceso físico.
b) Protección frente a desastres naturales.
c) Medidas de protección frente a incendios.
d) Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
e) Protección antirrobo.
f) Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios de certificación digital, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias.

3.4.4.1 Ubicación del sitio y construcción

Las operaciones de ECERT se llevan a cabo en un entorno físicamente seguro, diseñado para disuadir, prevenir y detectar cualquier uso, acceso o divulgación no autorizados de información sensible.

El centro de datos en donde se realizan las operaciones criptográficas cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia. La calidad y solidez de los materiales de construcción de las instalaciones garantiza adecuados niveles de protección.

3.4.4.2 Acceso físico

Se dispone de cuatro niveles de seguridad física (Entrada al perímetro de la instalación, entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles externos a los niveles internos.

El acceso físico a las dependencias donde se llevan a cabo los procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

a) Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
b) El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
c) Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de ECERT a los administradores del servicio de hospedaje que disponen de la llave para abrir el rack.

3.4.4.3 Energía y aire acondicionado

Las instalaciones cuentan con equipos estabilizadores de corriente, un sistema de alimentación eléctrica y el respaldo es un grupo electrógeno.

Además, las salas que albergan equipos informáticos están equipadas con sistemas de control de temperatura que incluyen aire acondicionado.

3.4.4.4 Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

3.4.4.5 Prevención y protección contra incendios

Las instalaciones y activos cuentan con sistemas automáticos de detección y extinción de incendios, cumpliendo con las regulaciones de seguridad aplicables.

3.4.4.6 Eliminación de residuos

En el caso de desechos magnéticos, estos son destruidos físicamente después de un proceso de borrado permanente o formateo seguro.

3.4.4.7 Copia de seguridad externa

La copia de seguridad se encuentra externa al data center donde se genera el respaldo.

3.4.5 Gestión de las operaciones

3.4.5.1 Manejo de medios

El manejo de medios es un componente crítico de la gestión de la seguridad de la información y ayuda a proteger los activos de información, es por eso que ECERT ha implementado controles de seguridad en base a la norma ISO 27002 contra accesos no autorizados, divulgaciones, alteraciones o pérdidas de información.

3.4.5.2 Controles de procedimiento

ECERT asegura que los sistemas de la infraestructura tecnológica operen de manera segura mediante procedimientos específicos para las funciones que afectan la provisión de servicios de certificación.

El personal responsable de la prestación del servicio sigue los procedimientos administrativos y de gestión conforme a la Política General de Seguridad de la Información (PO-GER-0003) de ECERT.

3.4.5.3 Funciones que requiere separación de funciones

Los roles que requieren Segregación de Funciones incluyen:

a) Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de confianza.
b) La administración de los sistemas, así como la activación de una CA en un ambiente de producción es incompatible con las funciones del Auditor.

3.4.5.4 Tipos de eventos registrados

ECERT produce y mantiene registros de al menos los siguientes eventos relacionados con la seguridad de la información:

a) Encendido y apagado del sistema.
b) Intentos de creación, borrado, establecimiento de contraseñas.
c) Intentos de inicio y fin de sesión.
d) Intentos de accesos no autorizados al sistema de ECERT a través de la red.
e) Intentos de accesos no autorizados al sistema de archivos.
f) Cambios en la configuración y mantenimiento del sistema.
g) Registros de las aplicaciones de la Autoridad de Certificación.
h) Encendido y apagado de la aplicación de la Autoridad de Certificación.
i) Cambios en la creación de políticas de certificados.
j) Generación de claves propias.
k) Creación y revocación de certificados.
l) Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
m) La ceremonia de generación de claves.
n) Registros de acceso físico.
o) Cambios en el personal.
p) Posesión de datos de activación, para operaciones con la clave pública y privada de la Autoridad de Certificación.

Frecuencia de procesamiento del registro de auditoria

ECERT revisa los registros cuando se genera una alerta del sistema debido a un incidente.

El procesamiento de los registros de auditoría implica una revisión para asegurar que no hayan sido manipulados, una inspección rápida de todas las entradas de registro, y una investigación detallada de cualquier alerta o irregularidad encontrada. Todas las acciones tomadas como resultado de la revisión de auditoría se deben documentar en cumplimiento con el proceso de gestión de incidentes.

Periodo de conservación del registro de auditoria

ECERT almacena la información de los registros durante un periodo que varía entre 1 y 6 años, dependiendo del tipo de información registrada.

Protección del registro de auditoria

Los registros de auditoría estarán protegidos mediante medios electrónicos para garantizar la integridad, la identificación temporal y el seguimiento de las actividades. Esto incluye la implementación de mecanismos para proteger los archivos de registro contra modificaciones, eliminaciones no autorizadas u otros tipos de manipulación.

Procedimiento de copias de seguridad del registro de auditoria

Dispone de un procedimiento de respaldo adecuado para asegurar que, en caso de pérdida o destrucción de archivos relevantes, las copias de respaldo correspondientes de los registros estén disponibles en un período corto de tiempo.

Evaluaciones de vulnerabilidades

ECERT cuenta con un Procedimiento de gestión de vulnerabilidades técnicas, en base al que se realizan las evaluaciones.

3.4.5.5 Procedimiento de manejo de incidentes y respuesta

ECERT ha desarrollado la Política General de Seguridad (PO-GER-0003), Política Gestión de Incidentes (PO-GER-0006) y la Política de Continuidad del Negocio (PO-GER-0007) que le permiten gestionar y recuperar los sistemas en caso de incidentes y compromisos de sus operaciones, asegurando la disponibilidad de los servicios críticos de revocación y publicación del estado de los certificados.

Estas políticas incluyen el escalamiento, investigación y respuesta al incidente de continuidad de negocio.

3.4.5.6 Capacidades de continuidad del negocio después de un desastre

Se restablecerán los servicios críticos conforme al plan de continuidad de negocio existente, asegurando la recuperación de las operaciones normales dentro de las 24 horas siguientes al desastre. ECERT cuenta con un centro alternativo disponible para poner en marcha los sistemas de certificación según lo establecido en el plan de continuidad de negocio.

3.4.6 Gestión de acceso a los sistemas

ECERT declara y asegura que el acceso a su sistema (hardware, software y datos) está restringido exclusivamente al personal autorizado. En particular se implementan las siguientes medidas:

- Cortafuegos: Se utilizan cortafuegos adecuados para proteger la red interna de accesos no autorizados.
- Administración de usuarios: Se lleva a cabo una gestión de usuarios para mantener la seguridad de los sistemas, lo que incluye la administración de cuentas, registros (logs) y la modificación o eliminación de accesos. Este proceso está documentado en la Política de control de acceso (PO-GSI-0007).
- Restricciones de acceso: Se aplican restricciones al acceso a la información y a los sistemas de aplicación, conforme a la Política de control de acceso (PO-GSI-0007), así como la desagregación de funciones en los roles de confianza definidos.
- Control del personal autorizado: Se implementa un control riguroso de la identificación y autenticación del personal autorizado antes de que acceda a las aplicaciones relacionadas con los sellos de tiempo. ECERT también mantiene un inventario de activos que incluye los roles y las personas asignadas a cada uno.
- Registros de operaciones: Se generan registros de las operaciones realizadas por el personal para facilitar auditorías posteriores.

3.4.7 Mantenimiento en implementación de sistemas de confianza

ECERT cuenta con una Política (PO-GSI-0002) y Procedimiento de Desarrollo seguro de software (PR-SGI-0003), los cuales establecen los mecanismos para asegurar que no se realicen modificaciones no autorizadas.

Además, ECERT cuenta con una Política Gestión de Cambio (PO-GER-0010) y un Procedimiento de Gestión y Control de Cambios (PR-GER-0002), cuyo objetivo es minimizar el impacto y las incidencias que se puedan producir debido a las modificaciones y/o actualizaciones en los sistemas.

Para el caso de la TSA ECERT, la administración de las llaves criptográficas se realiza bajo restricciones estrictas de seguridad, en la que participa personal capacitado e involucra más de una persona. Las normas que rigen esta generación de llaves están contenidas en el “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050).

3.4.8 Compromiso de los servicios de TSA

En caso de que ECERT sospeche o confirme el compromiso de las claves privadas de la CA, se pondrán en marcha procedimientos establecidos en las políticas General de Seguridad de la Información (PO-GER-0003), gestión de incidentes (PO-GER-0006) y continuidad del negocio (PO-GER-0007), permitiendo la recuperación de los sistemas críticos, si fuera necesario, en un centro de datos alternativo. En el caso de un compromiso de la clave privada de la CA, tal CA será revocada.

Con todo, ECERT comunicará a los titulares y partes que confían, por los medios que estime pertinentes, los incidentes que consideren el compromiso de la llave de firma de la TSU o la pérdida de precisión declarada del reloj.

3.4.9 Cese de la TSA

En caso de que ECERT cese sus operaciones como Autoridad de Sello de Tiempo comunicará tal situación a quienes consumen el servicio prestado, con una antelación de a lo menos dos meses considerando a:

- Solicitantes
- Partes que confían
- Autoridades acreditadas para emitir sello de tiempo.

Por ello, ECERT procederá a transferir los datos de sus sellos de tiempo a otro proveedor de servicios en la fecha en que se produzca el cese. Esta información incluirá, como mínimo, los datos de los solicitantes, los certificados de la TSU revocados, así como la transferencia de las obligaciones relacionadas con el mantenimiento de logs, archivos de auditoría, y el acceso a las llaves públicas o certificados utilizados por los terceros que confían, por un período de tiempo razonable.

En cuanto a las claves y copias de respaldo de la TSA de ECERT, estas serán borradas y destruidas. Además, los componentes de la red local se mantendrán en el Data Center bajo un ambiente seguro y con auditorías periódicas para garantizar que no puedan ser

recuperados, de acuerdo con lo especificado en las Prácticas de Certificación de Sellado de Tiempo DPST ECERT (PC-TSA-0001).

3.4.10 Cumplimiento de los requerimientos legales

Esta "DPST de ECERT" se rige por la ley chilena y se someterán al Tribunal Arbitral expresado en el punto 2.2.4.

3.4.11 Registro de información concierne a las operaciones del servicio de sellado de tiempo

ECERT produce y mantiene registros los siguientes eventos relacionados con el servicio de sellado de tiempo:

a) Requerimiento de sello de tiempo Sello de tiempo creado.
b) Eventos relacionados con la administración de la certificadora, incluyendo:
    - Registros de eventos correspondientes al ciclo de vida de las llaves de la unidad de sello de tiempo.
    - Registros de eventos correspondientes a los certificados de la unidad de sellos de tiempo.
    - Registros relacionados con la sincronización del reloj de usado por la unidad de sello de tiempo contenida en sus sellos de tiempo.
    - Registros asociados a eventos de detección de pérdida de sincronización.

La información personal de los titulares, que ha recolectado la PSC ECERT como parte de su operación, está protegida de acuerdo con la Política de Tratamiento de Datos Personales (PO-GER-0008) publicadas en el sitio web. Todos los registros relacionados con la operación del servicio de sello de tiempo están disponibles únicamente para el titular o en caso de que sean solicitados por un tribunal a través de un requerimiento legal, con el fin de proteger la confidencialidad de dichos datos.

La integridad de esta información es mantenida por ECERT 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.

Los registros antes mencionados, son almacenados por ECERT. A estos registros, sólo tiene acceso el personal autorizado por la PSC de ECERT.

3.5 Organización

La actividad de Certificación de Sellado de Tiempo que realiza ECERT se encuentra acreditada por la Entidad Acreditadora desde el año 2016, mediante la Resolución Exenta Nº 3779, de la Subsecretaría de Economía del Gobierno de Chile.

Las políticas y procedimientos bajo los cuales opera ECERT no incluyen cláusulas discriminatorias que contravengan la Ley 19.496 sobre los derechos de los consumidores en Chile. ECERT ofrece su servicio de sello de tiempo a cualquier titular que cumpla con las obligaciones establecidas en la Política de sellado de tiempo (MI-TSA-0037) y la Declaración de Prácticas de TSA (PC-TSA-0001).

Para la provisión de sus servicios, ECERT cumple con la normativa legal vigente en Chile relacionada con la formación y operación de empresas y personas jurídicas. Además, en cumplimiento de la Ley 19.799, artículo 14, ECERT cuenta con un seguro de responsabilidad civil para cubrir daños o perjuicios derivados de su operación.

ECERT es auditada anualmente en cuanto a sus estados financieros y al cumplimiento de la normativa vigente. ECERT dispone de personal calificado para la prestación de sus servicios y realiza capacitación continua a través de sus planes anuales de formación.

En caso de un conflicto con un titular que no pueda resolverse de manera favorable entre las partes, ECERT recurrirá al procedimiento de resolución de disputas declarado en este documento en el punto 2.2.4

ECERT mantiene en su repositorio documental todos los contratos, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

4 CONSIDERACIONES DE SEGURIDAD

ECERT declara que la llave usada por la TSU es generada 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 ECERT utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, al cual solo puede acceder personal definido que cumple roles de confianza, aplicando el Plan de Administración de Llaves Criptográficas (MI-FEA-0050).

La TSA de ECERT tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por las siguientes circunstancias:

- Un evento de seguridad que vulnere a la llave de la TSU
- Por un cese de actividades.
- Por requerimiento del titular (en este caso ECERT como dueño del certificado de firma de su TSU), por lo que se ajusta a las atribuciones que establece la ley 19.799 en el artículo 16.

Una vez revocado, todos los sellos de tiempo emitidos con ese certificado de firma de sello de tiempo también se consideran inválidos.

5 CONTROL DE VERISONES

Control de versiones		
Versión	**Fecha**	**Descripción**
1	22-03-2021	Migración del documento a ISOEasy.
2	18-08-2022	Revisión anual IAO 2022.
3	28-08-2023	Revisión anual IAO 2023.
4	07-08-2024	Se actualiza formato y contenido. 3.2 Se modifica redacción del ciclo de vida del sellado de tiempo. 3.2.8 Se incluye la expiración de los certificados emitidos. 3.3.3 Procedimiento de registro
5	14-08-2025	Mejoras en Redacción • Actualización del dominio institucional de e-certchile.cl a ecertla.com en todas las referencias del documento. • Inclusión de la URL del sitio web para acceder a la Política y Prácticas de TSA. • Se incorpora como se informa a la EA en caso de ser cambios materiales. • Se actualiza Repositorio de Documentación. • Se elimina el numeral duplicado y se ajusta la numeración, continuando la secuencia con 3.4.3. Revisión Anual IAO 2025
6	25-09-2025	Mejora en redacción por Aclaratoria IAO 2025: Se incorporan plazos de actualización o revisión de este documento.

Fin del documento

Una copia impresa de este documento es válida sólo por el día en que se imprimió.

Cualquier modificación y/o copia total o parcial, por cualquier medio, queda totalmente PROHIBIDA.