Política de Biometría

(CPBIO de ECERT)

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
G.A.M. BIO	4.12 Requisito PO01 - Política de biometría	BIO: Servicio de Certificación de Biometría	MI-BIO-0039
		GPQ27: Gestión seguridad de la información ISO 27001	

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	15-09-2025	25-09-2025	25-09-2025	8	11-01-2021

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Jefe de Operaciones PKI	Chief Revenue 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.

Este documento está dirigido a:

a) Titulares de Certificados, quienes necesitan comprender cómo se comprueba su identidad al momento de la emisión del certificado de firma avanzada con Comprobación Biométrica, cuáles son sus responsabilidades y que medidas de protección ECERT le otorga a través de los certificados de firma electrónica avanzada.
b) Partes que confían en la validez y autenticidad de los certificados de firma emitidos por ECERT. Esta confianza es fundamental para garantizar la seguridad y la fiabilidad en transacciones electrónicas, comunicaciones seguras, y otras operaciones que requieren la autenticación digital.

Esta Política de Certificación de Biometría se ha preparado de conformidad con la RFC 3647 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework' y la ETSI TS 102 042 V1.1.1 (2002-04) 7.1 Certification Practice Statement, en cumplimiento con el Decreto Supremo 181 de 2002.

1.1 Descripción General

La presente Política de Certificación de Biometría de ECERT en adelante “CPB de ECERT”, establece los requisitos que deben cumplirse relacionados al ciclo de vida del certificado de firma electrónica avanzada, mientras que la Declaración de Prácticas de Certificación de Biometría (PC-BIO-0001) en adelante “DPSB de ECERT” describe la forma en que se cumplen estos requisitos relacionados con el ciclo de vida del certificado de firma electrónica en base a la Ley N° 19.799.

ECERT ha establecido una Política General de Seguridad de la Información (PO-GER-0003) y una Política de Tratamiento de datos personales (PO-GER-0008) acorde con el modelo de confianza requerido para brindar los servicios de Biometría.

La actividad de servicios de Biometría que realiza ECERT se encuentra acreditada por la Entidad Acreditadora desde el 07 de diciembre del año 2016, mediante la Resolución Exenta Nº 3919, de la Subsecretaría de Economía del Gobierno de Chile.

1.2 Nombre e identificación del documento

El presente documento establece la Políticas Biometría (MI-BIO-0039) dedicada a la prestación de servicios en biometría de la EMPRESA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA SpA, en adelante “ECERT".

1.2.1 Identificadores de certificados

ECERT ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por aplicaciones.

1.3 Participantes

1.3.1 Autoridad de Certificación

Corresponde a las entidades que están autorizados para hacer comprobación de la identidad del solicitante de un certificado de firma electrónica avanzada a través de sus datos biométricos.

ECERT está constituido como Autoridad de Certificación también denominado Proveedor de servicios de certificación en Biometría 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. 3919, del 7 de diciembre del 2016, de la Subsecretaría de Economía, Fomento y Reconstrucción.

1.3.2 Autoridad de Registro

Son personas o instituciones autorizadas por ECERT, las que actuando en nombre y bajo la responsabilidad de ECERT realizan la comprobación de la identidad de los solicitantes de los certificados de firma electrónica a través de la información biométrica del solicitante en los términos establecidos en las “CPB de ECERT” y su “DPSB de ECERT”.

a) Comprobar la identidad de los solicitantes utilizando la Comprobación de identidad biométrica.
b) Registrar los antecedentes de los solicitantes que sirven de base para la Comprobación Biométrica.
c) Evaluar, aprobar o rechazar las solicitudes de certificados de acuerdo con estas Prácticas.

Además, pueden desempeñar otras funciones que les encomiende el certificador. ECERT, en su rol de Autoridad de Registro, asume todas las obligaciones establecidas en la "DPSB de ECERT”. En caso de delegar esta función, ECERT también asume la responsabilidad por las acciones de sus mandatarios, ya que estos actúan en su nombre y bajo su riesgo.

1.3.3 Titular

Aquella persona natural mayor o igual a 18 años a quien ECERT realiza la comprobación de su identidad a partir de sus datos biométricos para la emisión de un certificado de firma electrónica.

1.3.4 Partes que Confían

Son todas aquellas personas naturales o jurídicas que voluntaria y libremente deciden aceptar y confiar en la comprobación de la identidad que realiza ECERT a partir de su sistema biométrico.

1.3.5 Otros Participantes

Solicitante: Persona natural mayor o igual a 18 años que requiere el servicio de Comprobación biométrica.

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

1.4 Usos de la Biometría

1.4.1 Usos apropiados de la Biometría.

La Ley Nº 19.799 de Chile regula el uso los datos biométricos gestionados por un Proveedor de Servicios de Biometría, donde el objetivo es verificar la identidad de una persona, confirmando que esta es efectivamente quien dice ser. Esta verificación puede integrarse en cualquier proceso en el que un mandante necesite asegurar la identidad de un titular para proteger los datos personales.

1.4.2 Usos prohibidos de la Biometría.

Los datos biométricos se utilizarán exclusivamente para los fines y funciones establecidos en la presente Política de Certificación y conforme a la normativa vigente. Cualquier uso distinto al especificado está estrictamente prohibido.

1.5 Administración de la Política

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: https://www.ecertla.com

Teléfono: 6003620400

Mail: mesasoporte@ecertchile.cl

1.5.3 Organización que determina la idoneidad de la DPSB para la Política

Razón social: EMPRESA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA SpA

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

1.5.4 Procedimiento de aprobación de la CPB

Cualquier nueva versión de esta Declaración de Prácticas de Biometría estará sujeta a un procedimiento de aprobación que incluye los siguientes pasos:

a) Elaboración y aprobación interna de la nueva versión.
b) Presentación de esta CPB al Comité de Sistema de Gestión de ECERT.
c) Después de obtener las aprobaciones mencionadas, se publicará la nueva versión de esta CPB, indicando la fecha de entrada en vigor.

Una vez que se publique la nueva "CPB 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.

Las especificaciones asociadas a los mecanismos y plazos de notificación se especifican en el punto 8.12.2 de estas "CPB de ECERT".

1.6 Definiciones y acrónimos

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

Definiciones	Acrónimos
Certificate Policy (Política de Certificación).	CP
Certification Practice Statement (Declaración de Prácticas de Certificación)	DPS
Prestador de Servicios de Certificación	PSC
Certification Authority (Autoridad de Certificación)	CA
Registration Authority (Autoridad de Registro)	RA
Certificate Revocation List (Lista de revocación de CertificadZOos)	CRL

Online Certificate Status Protocol (Protocolo de estado en línea de Certificado)	OCSP
Public Key Infrastructure (Infraestructura de clave pública)	PKI
Object Identifier (Identificador de objeto)	OID

2 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1 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.

2.2 Publicación de información de Biometría

ECERT realiza la publicación de la información relativa a los servicios de biometría 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 Biometría (PC-BIO-0001).
b) Política de Certificado de Biometría (MI-BIO-0039).
c) Política General de Seguridad de la Información (PO-GER-0003).
d) Política de Tratamiento de datos personales (PO-GER-0008).
e) Contratos Adhesión de Titular (MI-FEA-0326, MI-FEA-0327, MI-FEA-0346 y MI-FEA-0347)
f) Casilla de correo para validar partners.
g) Consulta del estado de certificado.
h) Las listas de certificados revocados (CRLs).

2.3 Tiempo o frecuencia de publicación

La publicación de la información de ECERT, que incluye la "CPB de ECERT" y la "DPSB de ECERT", se debe realizar tan pronto como esté disponible.

Los cambios en esta "CPB de ECERT" se rigen por lo dispuesto en el punto 1.5 de este documento.

ECERT mantiene permanentemente a disposición de los interesados a través de https://www.ecertla.com/verifica-vigencia-de-certificado/ un registro de acceso público de certificados.

El registro de acceso público de certificados se actualiza según las reglas descritas en las *"DPSB de ECERT"* asegurando la disponibilidad continua y la actualización periódica de la información.

Cualquier situación ocasionada con relación a la vigencia de un certificado y de las obligaciones contraídas por ECERT se resolverán de acuerdo con esta *"CPB de ECERT"* y las *"DPSB de ECERT"* vigente al momento de la emisión del certificado en cuestión.

2.4 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.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Denominación

3.1.1 Tipos de nombres

En el contexto de la firma y los certificados digitales, los tipos de nombres se refieren a las formas en que se puede identificar al sujeto al que pertenece el certificado generado con Comprobación de identidad Biométrica. Estos nombres se utilizan para indicar quién es el titular del certificado y pueden tomar diferentes formas según las normativas y estándares utilizados.

Todos los certificados de firma de ECERT contienen un nombre distintivo (Distinguished Name (DN), el cual corresponde a un nombre único y completo que identifica de manera inequívoca al sujeto dentro de un contexto específico.

Para la asignación del nombre a ser contenido en los certificados se incluirán los mismos nombres que figuran en el Registro Civil, Terceros de confianza o en su defecto los mismos nombres que figuran en la cédula de identidad del Solicitante cuando este haya comparecido en forma personal y directa a las oficinas de ECERT o de una Autoridad de Registro.

3.1.2 Necesidad de que los nombres tengan significado

Los nombres en los certificados deben tener un significado claro y comprensible para todos los usuarios y partes que confían en los certificados.

3.1.3 Anonimato o seudónimo de los Titulares

ECERT no emite en ninguna circunstancia certificados de firma anónimos. Por otro lado, los seudónimos tampoco están permitidos como identificadores de Titulares.

3.1.4 Reglas para la interpretación de las distintas formas de nombres

No se establecen reglas específicas adicionales a las indicadas en esta “DPSB de ECERT”.

3.1.5 Unicidad de los nombres

Es posible para un titular tener dos o más Certificados, con el mismo nombre distintivo (DN o distinguished name) según el estándar X.501 en el campo Subject, independientemente de que cada Certificado puede ser distinguido en forma unitaria.

3.1.6 Reconocimiento, Autenticación y Función de las marcas

No aplica considerando que la emisión de certificados que realiza ECERT es para personas naturales.

3.2 Comprobación de identidad inicial

La identificación de los solicitantes se realiza de conformidad con las normas y procedimientos establecidos en esta "DPSB de ECERT", sin perjuicio de los requisitos específicos establecidos por la Política de Biometría (MI-BIO-0039) "CPB de ECERT".

ECERT es responsable de todo el ciclo de vida de los certificados de firma electrónica que se emitan con Comprobación de Identidad Biométrica.

3.2.1 Método para demostrar la posesión de la clave privada

La posesión de la clave privada se establece mediante el procedimiento confiable de entrega y aceptación del certificado por parte del titular.

3.2.2 Autenticación de la identidad de la organización

No aplica considerando que la emisión de certificados que realiza ECERT es para personas naturales.

3.2.3 Autenticación de la identidad individual

La autenticación de la identidad de un individuo se realiza mediante documentos de identificación válidos y procesos de verificación presencial según los procedimientos establecidos en la Declaración de prácticas de Biometría (DPSB de ECERT).

Los métodos de Autenticación de identidad individual (Comprobación fehaciente de la identidad) de una persona natural identificada en un certificado de firma, podrá ser desarrollado por las Autoridades de Registro vinculadas a ECERT, dentro de los límites de la normativa aplicable.

La solicitud de un certificado de firma electrónica avanzada deberá realizarla el Solicitante compareciendo en forma personal (físicamente) y directa a las oficinas de ECERT o una Autoridad de Registro, en estos casos la Autoridad de Registro ejecutará el proceso siguiendo los requisitos del punto 4.1.2 de esta Política.

3.2.4 Información de solicitante no verificada

ECERT no verifica el correo electrónico de los solicitantes de certificados.

Para la asignación del correo electrónico en los certificados, se utilizará el correo electrónico declarado por el Solicitante al requerir el certificado de firma electrónica avanzada, sin que ECERT compruebe la existencia ni operatividad de este.

De este modo, cualquier error en la dirección de correo electrónico proporcionado será responsabilidad exclusiva del Solicitante.

3.2.5 Comprobación de la autoridad

No aplica considerando que la emisión de certificados que realiza ECERT es para personas naturales.

3.2.6 Criterio de interoperabilidad

Los certificados emitidos deben cumplir con los estándares de interoperabilidad establecidos en las normas internacionales aplicables.

3.3 Identificación y autenticación para solicitudes de renovación de claves

3.3.1 Identificación y autenticación para la renovación rutinaria de claves

Si el titular pierde el acceso a las claves, ni ECERT ni sus Autoridades de Registro pueden regenerarlos, siendo necesario que el titular proceda con la solicitud de revocación del certificado de firma.

En cuanto a los datos de creación de firma almacenados en un módulo criptográfico masivo de ECERT, se declara que ECERT no tiene ni mantiene métodos para acceder directa o indirectamente a estos datos, ni a la contraseña que los protege, la cual es de exclusivo control del titular.

Para mayor detalle del proceso de renovación vaya al punto 4.6.3 de esta Práctica.

3.3.2 Requisitos de identificación y autenticación para la renovación de claves después de la revocación del certificado

Después de una revocación, el proceso de identificación y autenticación debe ser completado de nuevo para asegurar la validez de la identidad del solicitante.

3.4 Identificación y autenticación para solicitudes de revocación

Una solicitud de revocación se debe efectuar por el titular de alguna de las siguientes formas:

a) Compareciendo en forma personal y directa ante ECERT o una de sus Autoridades de registro para hacer la solicitud y efectuar un procedimiento de identificación que permita formar la convicción respecto de su identidad.
b) Compareciendo en una Oficina Virtual de ECERT solicitando la revocación y acreditando la identidad con la ClaveUnica provista por el Registro Civil al titular.

4 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud de Certificados

4.1.1 Quién puede presentar una solicitud de certificado

Toda persona natural y mayor o igual a 18 años que desee obtener un certificado de firma electrónica avanzada en ECERT

4.1.2 Proceso de inscripción y responsabilidades

El proceso de solicitud de inscripción de un certificado de firma electrónica avanzada deberá realizarla el Solicitante compareciendo en forma personal (físicamente) y directa a las oficinas de ECERT o una Autoridad de Registro, en estos casos la Autoridad de Registro ejecutará el proceso pidiendo la siguiente información al solicitante:

a) Cédula de Identidad: para permitir realizar la comprobación automática del dato biométrico capturado en vivo contra ella.
b) Correo electrónico.
c) Teléfono de contacto (no es obligatorio).
d) Verificación de Identidad Biométrica: ECERT verifica la identidad de la persona a la cual se asociará el dato biométrico. Para esto el Solicitante debe posicionar su huella en el dispositivo Biométrico donde se realiza la comparación automática del dato biométrico capturado en vivo, respecto de aquel que se contiene en la cédula de identidad de la persona que requiere demostrar su identidad. El resultado de esta comparación será una aprobación o rechazo de identidad. A este proceso lo denominamos “Match on Card”.

El proceso Match on Card presenta las siguientes características:

a) Seguridad Mejorada: Al mantener los datos biométricos y las comparaciones dentro del dispositivo, se reduce el riesgo de exposición de datos sensibles durante la transmisión.

b) Protección de Privacidad: Los datos biométricos nunca salen del dispositivo, lo que mejora la privacidad del usuario.
c) Reducción de Riesgos de Compromiso: Dado que los datos biométricos no se envían a través de redes, el riesgo de interceptación o manipulación de datos se minimiza.

En caso de rechazo de identidad del sistema biométrico, revise las alternativas que se ofrecen en la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

a) Disponibilidad del solicitante para configurar computador y dispositivo e-Token con asistencia del Operador de Registro.

En caso de que el solicitante sea un Notario, Conservador, Registrador de Comercio o Archivero Judicial, titulares suplentes o interinos, adicionalmente deberán presentar la certificación de tal condición emitida por el Secretario de la Corte de Apelaciones respectiva.

ECERT utiliza diferentes interfaces (dispositivos y tecnología) para la captura de los datos relevantes para el proceso de comprobación de la identidad del solicitante de un certificado de firma electrónica avanzada. Estos son:

a) Sistema de Biometría SecuGen que cuenta con la tecnología biométrica de huellas dactilares de reflexión irregular mejorada en la superficie (SEIR) para obtener imágenes de huellas dactilares de muy alto contraste con muy baja distorsión. El alto contraste y la baja distorsión son las características de una excelente calidad de imagen.
b) Sistema de Biometría bajo los estándares ICAO 9303, Minutiae for a Match On Card ISO Compact Size ISO/IEC 19742-2 y Match On Card, Nist Minutiae Interoperability Exchange - MINEX II (para cédulas de identidad nueva).
c) Algoritmo de reconocimiento de impresión dactilar: Estándar ANSI 378 que establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas

La biometría empleada por ECERT se encuentra acreditada ante la Subsecretaría de Economía y Empresas de Menor Tamaño mediante Resolución Administrativa Exenta N° 3919 de 7 de diciembre de 2016.

En caso de cualquier inconveniente en el proceso de autenticación de identidad, el solicitante puede comunicarse con ECERT a través de los siguientes canales:

- Teléfono: 6003620400
- Página Web: Formulario de contacto (mesasoporte@ecertchile.cl)

Las responsabilidades de los participantes se declaran a continuación:

4.1.2.1 ECERT (AC)

Sin perjuicio de las demás obligaciones legales y de esta "DPSB de ECERT" y la "CPB de ECERT" Firma Electrónica Avanzada, ECERT es especialmente responsable de:

a) Implementar medidas de seguridad adecuadas para proteger los datos biométricos contra accesos no autorizados, pérdida, o compromisos.
b) Emitir los certificados cumpliendo todas las exigencias establecidas en esta "DPSB de ECERT" y en la "CPB de ECERT" de Certificado de firma Electrónica Avanzada, de conformidad con la información proporcionada por el titular.
c) Asegurarse de que el certificado no contenga errores de transcripción de los datos proporcionados por el titular durante el proceso de solicitud del certificado.
d) Garantizar que la información incluida o incorporada por referencia en el certificado sea exacta.
e) Publicar el certificado en el registro de acceso público de certificados.
f) Aplicar correctamente todos los procedimientos empleados.
g) Implementar adecuadamente la Ley 19.628 con la finalidad de proteger los datos personales de los Titulares.
h) ECERT no será responsable por ningún daño o perjuicio relacionado con el uso de certificados, incluyendo daños directos, indirectos, emergentes, lucro cesante o

pérdida de datos, ni por el uso indebido de los certificados, sus datos de firma o PIN de protección, aun cuando haya sido advertido de tales posibilidades.

4.1.2.2 Autoridad de Registro (AR)

Se obliga a:

a) Comprobar la identidad del solicitante de un certificado de firma electrónica, según el procedimiento establecido en esta "DPSB de ECERT" y en la "CPB de ECERT".
b) Obtener la aceptación del contrato del titular.
c) Aprobar o rechazar las solicitudes de certificados, directamente o a través de sus Autoridades de Registro, conforme a esta "DPSB de ECERT".
d) Permitir operar solo certificados de firma electrónica avanzada que hayan sido aceptados por el solicitante.
e) Conservar por 6 años la información utilizada como base para la emisión de los certificados de firma electrónica avanzada o remitirla a ECERT dentro de los plazos convenidos.
f) Recibir las solicitudes de revocación de certificados de firma electrónica e informarlas a ECERT.
g) Prestar cualquier otro servicio que ECERT le solicite y que guarde relación con la actividad de certificación de firma electrónica.
h) La Autoridad de Registro realiza todas las actuaciones indicadas anteriormente, gestionando el ciclo de vida del certificado de firma electrónica, por cuenta y riesgo de ECERT.

4.1.2.3 Titular

El titular es responsable de:

a) Aceptar el certificado de acuerdo con el punto 4.4 de esta "DPSB de ECERT".
b) Aceptar el Contrato Titular.
c) Comunicar a ECERT cualquier cambio en las declaraciones efectuadas al momento de solicitar el certificado y que impacte en alguna de las menciones del certificado

para que ECERT lo revoque. Si el Titular desea un nuevo certificado con las actualizaciones, debe presentar una nueva solicitud y asumir el costo de emisión.

d) No revelar el PIN del e-Token o del dispositivo criptográfico masivo que contiene los datos de creación de firma, ni el mecanismo de activación de la firma.

e) Si los datos de creación de firma se almacenan en un dispositivo criptográfico masivo, custodiar adecuadamente el segundo factor de seguridad para asegurar que el acceso y uso de los datos de creación de firma sean exclusivamente suyos.

f) Usar el certificado de firma para los fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, en estas "DPSB de ECERT" y en la "CPB de ECERT".

g) Ser una Parte que Confía final y no usar el certificado para actuar como certificador de firma electrónica.

h) Custodiar los datos de creación de firma, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.

i) Comunicar inmediatamente a ECERT y/o a una Autoridad de Registro cualquier compromiso, pérdida, hurto, robo, acceso no autorizado, extravío, falsificación de sus datos de creación de firma o certificado, o cualquier circunstancia que pueda ser causal de revocación de un certificado.

j) Comunicar la pérdida o destrucción del e-Token utilizado para el almacenamiento de los datos de creación de firma.

k) Responder de manera oportuna cualquier comunicación o requerimiento de información relacionado con el ciclo de vida del certificado que le haga ECERT.

l) Solicitar la revocación del certificado cuando se presente alguna de las causales indicadas para este efecto.

m) No usar los datos de creación de firma una vez que el certificado haya expirado, esté revocado o suspendido.

n) Destruir los datos de creación de firma si ECERT lo solicita.

o) Indemnizar a ECERT y/o a la Autoridad de registro de todo daño o perjuicio proveniente de cualquier acción u omisión negligente, culposa o dolosa de su parte. culposa o dolosa de su parte, de acuerdo con el artículo 2314 de Código Civil Chileno

p) Almacenar los documentos firmados es responsabilidad del titular, excluyendo de esta responsabilidad a ECERT.

q) Utilizar los canales formales de ECERT indicados en el punto 1.5.2 del presente documento para comunicarse en caso de Solicitudes o Quejas.

4.1.2.4 Partes que Confían

Las partes que confían en los certificados de firma electrónica emitidos por ECERT tienen las siguientes obligaciones:

a) Comprobar la validez del certificado consultando el registro de acceso público de certificados disponible permanentemente en www.ecertla.com o utilizar las herramientas que ECERT pone a disposición en esta misma página web.

b) Comprobar la autenticidad de la firma del Titular.

c) Comprobar cualquier limitación funcional que pueda tener incorporado el certificado de firma electrónica.

d) Verificar que el uso que se le está dando al certificado sea acorde con los propósitos autorizados por la ley, esta “DPSB de ECERT” y la “CPB de ECERT”.

e) Indemnizar a ECERT y/o a la Autoridad de registro de todo daño o perjuicio proveniente de cualquier acción u omisión negligente, culposa o dolosa de su parte.

Al utilizar un certificado de manera libre y espontánea las partes que confían asumen la responsabilidad y los riesgos que ello conlleva si no se han realizado previamente los pasos indicados anteriormente.

4.2 Tramitación de la solicitud de certificado

4.2.1 Realización de funciones de identificación y autenticación

Los procedimientos de identificación y autenticación de la información de los titulares, realizados por la Autoridad de Registro, están detallados en el punto 3.2 del documento actual.

4.2.2 Aprobación o rechazo de la solicitud de certificado

La Autoridad de Registro aprobará o rechazará la solicitud del certificado de firma en base al cumplimiento de los procedimientos de Identificación y Autenticación de la información están detallados en el punto 3.2 del documento actual.

4.2.3 Tiempo de tramitación de las solicitudes de certificados

Las Solicitudes de Certificado serán procesadas en un plazo razonable tras su recepción.

4.3 Emisión de Certificado

4.3.1 Acciones de la CA durante la emisión del certificado

El Certificado de firma se genera y entrega al titular después de que la Autoridad de Certificación recibe la confirmación de emisión de la Autoridad de Registro.

Los Certificados deben estar disponibles para los titulares ya sea a través de la descarga de los certificados de forma individual en un e-Token o en un dispositivo criptográfico masivo custodiado por ECERT.

4.3.2 Notificación de la emisión al titular

ECERT informará oficialmente al titular del certificado que su certificado digital ha sido emitido y está listo para ser utilizado. Esta notificación puede realizarse de diversas formas, como, por ejemplo: mediante un correo electrónico, un mensaje en el sistema de la Autoridad de Certificación, o cualquier otro método acordado previamente entre ECERT y el titular.

4.3.3 Periodo de Vigencia y Expiración del Certificado del Titular

Los certificados emitidos por ECERT pueden tener las siguientes vigencias.

a) Firma electrónica avanzada: 1, 2 o 3 años.
b) Firma electrónica avanzada Auxiliar Administración Justicia: 1, 2 o 3 años.

c) Firma electrónica avanzada on-line: 1, 2 o 3 años.

d) Firma electrónica avanzada on-line:

Opción 1: máximo 30 días, ya que de acuerdo con el contrato titular este autoriza la revocación del certificado una vez que se haya ejecutado un proceso de suscripción documental (firma) o bien transcurrido los 30 días desde su emisión.

Opción 2: 1, 2 o 3 años.

4.4 Aceptación del Certificado

4.4.1 Conducta que constituye la aceptación del certificado

La aceptación del certificado se considera efectiva cuando no se ha presentado un reclamo por error o inexactitud al momento de su recepción, el certificado ha sido utilizado por el titular o cuando se utiliza en cualquier transacción, comunicación o suscripción de un documento y según lo descrito en las “DPSB de ECERT”.

4.4.2 Publicación del certificado por la CA

ECERT publica los certificados emitidos en un repositorio de acceso público https://www.ecertla.com/verifica-vigencia-de-certificado/, el registro diferencia entre certificados vigentes, suspendidos y revocados.

4.4.3 Notificación de la emisión del Certificado por la CA a otras entidades

Las comunicaciones sobre la emisión de certificados por parte de la CA de ECERT a las Autoridades de Registro se llevarán a cabo según los métodos acordados de común acuerdo.

4.5 Usos de pares de claves y certificados

4.5.1 Uso de la Llave Privada y del Certificado por el Titular

El titular se obliga a:

El Titular debe usar la clave privada y el certificado solo para los fines autorizados en conformidad con esta “CPB de ECERT” y lo descrito en las "DPSB de ECERT”.

El titular debe dejar de utilizar la clave privada tras la expiración, suspensión o revocación del certificado.

En caso de que el titular entregue el acceso a sus datos de creación de firma a un tercero, los documentos electrónicos y/o las autenticaciones realizadas por estos terceros serán de su exclusiva responsabilidad, ya que el titular sigue siendo responsable del uso que se haga de dichos datos. Esto es sin perjuicio del derecho de ECERT de tomar acciones civiles, administrativas o penales contra los terceros que hayan hecho uso indebido de los datos de creación de firma.

4.5.2 Uso de la Llave pública y certificado de la parte que confía

Las Partes que Confían podrán revisar los términos de uso del Certificado, revisando las "DPSB de ECERT”.

Las partes que confían deben verificar la validez del certificado antes de confiar en la información firmada y asumir toda la responsabilidad en caso de incumplir con sus obligaciones como parte que confía en el certificado.

4.6 Renovación del certificado

Revisar las alternativas que se ofrecen en la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

4.6.1 Circunstancias para la renovación del certificado

Los certificados vigentes pueden renovarse mediante un procedimiento específico y simplificado de solicitud, asegurando la continuidad del servicio de certificación. Sin embargo, un certificado no puede renovarse después de su expiración. En tal caso, el titular deberá solicitar un nuevo certificado y completar todos los procedimientos necesarios.

4.6.2 Quién puede solicitar la renovación

La solicitud de renovación solo puede ser solicitada por el Titular del certificado de firma.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Frente a una solicitud de renovación de certificado por parte del titular, ECERT realizará la sustitución del certificado anterior por uno nuevo. El proceso de renovación sigue los procedimientos de comprobación fehaciente de la identidad descrito en la "DPSB de ECERT".

4.6.4 Notificación de la emisión del nuevo certificado al Titular

ECERT informará oficialmente al titular del certificado que su certificado digital ha sido emitido y está listo para ser utilizado de manera oportuna de acuerdo con los descrito en "DPSB de ECERT".

4.6.5 Conducta que constituye aceptación de un certificado de renovación

Un certificado se considera aceptado por el Titular de acuerdo con lo descrito en el punto 4.4.1 de esta "DPSB de ECERT".

4.6.6 Publicación del certificado de renovación por la CA

ECERT publica los certificados emitidos en un repositorio de acceso público.

4.6.7 Notificación de la emisión del Certificado por la CA a otras entidades

Las comunicaciones sobre la emisión de certificados se realizarán de acuerdo con lo descrito en el punto 4.4.3 de esta Política.

4.7 Cambio de clave del certificado

4.7.1 Circunstancias para la renovación de la clave del certificado

No aplica, el cambio de la clave del certificado se considerará como una nueva emisión de certificado.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

No aplica considerando el punto 4.7.1 de esta “DPSB de ECERT”.

4.7.3 Procesamiento de solicitudes de renovación de claves de certificado

No aplica, el cambio de la clave del certificado se considerará como una nueva emisión de certificado.

4.7.4 Notificación de la emisión de un nuevo certificado al Titular

ECERT informará oficialmente al Titular del certificado que su certificado digital ha sido emitido de acuerdo con lo indicado en el punto 4.3.2 de esta “CPB de ECERT”.

4.7.5 Conducta que constituye aceptación de un certificado con nueva clave

Un certificado se considera aceptado por el Titular de acuerdo con lo descrito en el punto 4.4.1 de esta “DPSB de ECERT”.

4.7.6 Publicación del certificado renovado en la CA

ECERT publica los certificados emitidos en un repositorio de acceso público.

4.7.7 Notificación de la emisión de certificados por parte de la CA a otras entidades

Las comunicaciones sobre la emisión de certificados se realizarán de acuerdo con lo descrito en el punto 4.4.3 de estas “CPB de ECERT” y según lo descrito en el mismo punto en las “DPSB de ECERT”.

4.8 Modificación del certificado

4.8.1 Circunstancias para la modificación del certificado

La modificación de certificado se considerará como una nueva emisión de certificado.

4.8.2 Quién puede solicitar la modificación del certificado

No aplica, la solicitud de modificación del certificado se considerará como una nueva emisión de certificado.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica, la solicitud de modificación del certificado se considerará como una nueva emisión de certificado.

4.8.4 Notificación de la emisión de un nuevo certificado al Titular

El titular es notificado sobre la emisión del nuevo certificado de acuerdo con lo indicado en el punto 4.3.2 de esta "DPSB de ECERT".

4.8.5 Conducta que constituye aceptación de un certificado modificado

No aplica, la solicitud de modificación del certificado se considerará como una nueva emisión de certificado.

4.8.6 Publicación del certificado modificado por la CA

No aplica, porque la solicitud de modificación del certificado se considerará como una nueva emisión de certificado.

4.8.7 Notificación de la emisión de certificado por la CA a otras entidades

Las comunicaciones sobre la emisión de certificados se realizarán de acuerdo con lo descrito en el punto 4.4.3 de estas prácticas.

4.9 Revocación y suspensión del certificado

4.9.1 Circunstancias revocación

La Revocación del certificado es el cese permanente de los efectos jurídicos de este conforme a los usos que le son propios e impide el uso legítimo del mismo.

La revocación tendrá lugar de acuerdo con lo indicador en este mismo punto en la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

4.9.2 Quién puede solicitar la revocación

La revocación de un certificado puede ser solicitada por el Titular o será realizada por ECERT o la Autoridad de Registro si detectan alguna de las circunstancias mencionadas en el punto 4.9.1.

4.9.3 Procedimiento para la solicitud de revocación

El solicitante de la revocación debe comparecer personal y directamente ante una oficina de ECERT, una de sus Autoridades de Registro o en su Oficina Virtual, siguiendo el procedimiento indicado en este mismo punto en la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

4.9.4 Plazo de gracia para la solicitud de revocación

Las solicitudes de revocación deben presentarse lo antes posible dentro de un plazo razonable el cual debe ser menor al plazo de vigencia del certificado.

4.9.5 Plazo en el que la CA debe tramitar la solicitud de revocación

Las solicitudes de revocación serán gestionadas por la Autoridad de Certificación dentro de un plazo razonable.

4.9.6 Requisito de comprobación de revocación para las partes que confían

Los Partes deben verificar el estado de los certificados en los que desean confiar. Una forma de verificar este estado es consultando la última Lista de Revocación de Certificados emitida por ECERT.

Las Listas de Revocación de Certificados se publican en el repositorio disponible en la web: https://www.ecertla.com/herramientas/crl/

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP o bien en la página web de ECERT: https://www.ecertla.com/verifica-vigencia-de-certificado/.

4.9.7 Frecuencia de emisión de CRL (si corresponde)

Las Listas de Certificados Revocados (CRL) son emitidas y actualizadas por lo menos 1 vez cada 24 horas.

4.9.8 Latencia máxima para la CRL (si corresponde)

Las Listas de Revocación de Certificados (CRL) se publican en el repositorio en un tiempo razonable después de su generación, generalmente en unos pocos minutos como máximo.

4.9.9 Disponibilidad de comprobación de estado/revocación en línea

Alternativamente, las partes que confíen en certificados pueden consultar el repositorio de certificados de ECERT, disponible los 7 días de la semana en la web. Salvo en interrupciones programadas donde ECERT hará los mejores esfuerzos por asegurar que esta interrupción sea el menor tiempo posible.

4.9.10 Requisitos de comprobación de revocación en línea

Una Parte que Confía debe verificar el estado del certificado en el cual desea confiar. Si dicha Parte que Confía no verifica el estado del certificado mediante la consulta de la Lista de Revocación de Certificados (CRL) más reciente, deberá hacerlo consultando el Estado del Certificado utilizando el servicio OCSP.

4.9.11 Otras formas de anuncios de revocación disponibles

No aplica.

4.9.12Requisitos especiales en materia de compromiso de claves

En caso de que se detecte o se sospeche un compromiso en las llaves privadas de la CA, los participantes de ECERT serán notificados de manera oportuna mediante métodos que sean comercialmente razonables.

4.9.13Circunstancias de suspensión

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del Titular y es reversible.

La suspensión aplica a aquellos certificados que están en estado Vigente, y que por lo tanto no se encuentran revocados y no se ha cumplido su periodo de vigencia.

La reactivación de un certificado supone su paso de estado suspendido a estado vigente, siempre y cuando no se ha cumplido su periodo de vigencia.

4.9.14Quién puede solicitar la suspensión

La suspensión del certificado tendrá lugar cuando:

a) Lo decida ECERT por razones técnicas.
b) Sea solicitado por el Titular del certificado.

4.9.15Procedimiento para solicitud de suspensión

El procedimiento para la suspensión depender a de quien solicita la Suspensión y se especifica en este mismo punto de las Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

4.9.16Límites del periodo de suspensión

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta el cumplimiento del periodo de vigencia del certificado.

La suspensión de un certificado en ningún caso implica un cambio en la fecha de termino de vigencia del certificado.

4.10 Servicios de estado de certificados

4.10.1Características operativas

El estado de los certificados públicos está disponible en la Lista de Revocación de Certificados (CRL) a través de un sitio web de ECERT y también mediante un servicio OCSP.

4.10.2Disponibilidad del servicio

ECERT se compromete a mantener los Servicios de Estado de Certificados disponibles en todo momento, salvo durante interrupciones programadas donde ECERT hará los mejores esfuerzos por asegurar que esta interrupción sea el menor tiempo posible.

4.10.3Características opcionales

El servicio OCSP es una opción sistémica para verificar el estado de los certificados, que complementa la funcionalidad de la CRL.

4.11 Fin de la suscripción

La suscripción al servicio finalizará cuando expire el periodo de vigencia del certificado o si este es revocado antes de dicha fecha.

4.12 Custodia y recuperación de claves

ECERT no custodia ni recupera llaves del Titular.

4.12.1Política y prácticas de depósito y recuperación de llaves

No aplica.

4.12.2 Política y prácticas de encapsulamiento y recuperación de llaves de sesión

No aplica.

5 CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN

Los controles que se tratan en este punto ayudan a proteger tanto el hardware como el entorno en el que se recopilan y procesan los datos biométricos.

5.1 Controles físicos

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 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.

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 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.

5.1.5 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.

5.1.6 Almacenamiento de medios

El almacenamiento de medios de biometría dactilar se refiere a cómo se guardan los datos relacionados con las huellas dactilares en un sistema de seguridad biométrica. Estos medios de almacenamiento deben asegurar la integridad, seguridad y privacidad de la información biométrica conforme a la Ley 19.799.

5.1.7 Eliminación de residuos

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

5.1.8 Copia de seguridad externa

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

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 de ECERT.

5.2.1 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) Operador de Registro: Persona responsable de aprobar las peticiones de certificación realizadas por el solicitante y emitir certificados digitales.
d) 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. 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.

5.2.2 Número de personas necesarias por tarea

Al prestar el servicio, se garantiza la presencia de al menos dos personas encargadas de realizar las tareas relacionadas con la generación, recuperación y copia de seguridad de la clave privada de las Autoridades de Certificación.

Este mismo criterio se aplica a la ejecución de tareas como la emisión y activación de certificados y claves privadas de las Autoridades de Certificación, así como a cualquier manipulación del dispositivo que custodia las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3 Identificación y autenticación para cada rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4 Funciones que requieren 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) Emisión, suspensión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
c) La administración de los sistemas, así como la activación de una CA en un ambiente de producción es incompatible con las funciones del Operador de registro y Auditor.

5.3 Controles de personal

5.3.1 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 Comprobación 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 según lo permita la legislación aplicable, que abarca:

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

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.

5.3.2 Procedimiento de verificación de antecedentes

ECERT antes de contratar a una persona o permitir que acceda al puesto de trabajo, se llevan a cabo las siguientes verificaciones:

a) Referencias de empleos anteriores.
b) Nivel de estudios.

c) De antecedentes judiciales.

Todas las verificaciones se realizan dentro de los límites establecidos por la legislación vigente aplicable.

5.3.3 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.

5.3.4 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.

5.3.5 Frecuencia y secuencia de rotación de puestos

No aplica.

5.3.6 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.

5.3.7 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 esta “DPSB de ECERT”. 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.

5.3.8 Documentación suministrada al personal

ECERT debe asegurarse de que todo su personal, incluidas las personas de confianza, reciban la formación adecuada y tengan acceso a la documentación necesaria para desempeñar sus responsabilidades laborales de manera competente y satisfactoria.

5.4 Procedimientos de registro de auditoria

5.4.1 Tipos de eventos registrados

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

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.

ECERT no almacena huellas ni almacena minucias.

5.4.2 Frecuencia de procesamiento del registro

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.

5.4.3 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.

Es importante destacar que los registros de auditoría relacionados con la gestión del ciclo de vida de los certificados digitales se conservarán por un período de 6 años desde la emisión del certificado.

5.4.4 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.

5.4.5 Procedimientos 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.

5.4.6 Sistema de recopilación de auditoria (internas vs. externas)

El sistema de auditoria interno está centralizado en un sistema de gestión de eventos e información de seguridad.

5.4.7 Notificación al sujeto causante del evento

Cuando el sistema de registro de auditoría registre un evento, no es necesario enviar una notificación al individuo, organización, dispositivo o aplicación responsable del evento.

5.4.8 Evaluaciones de vulnerabilidad

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

5.5 Registros archivados

5.5.1 Tipos de registros archivados

Archivos de CAs

- Todos los datos de auditoría recopilados según lo establecido en el punto 5.4.

Autoridad de Registro incluyen:

- Información de Titular de Certificados.
- Documentación de apoyo de solicitudes de Certificados.
- Información del Ciclo de Vida de Certificados.

5.5.2 Periodo de conservación de los datos archivados

ECERT almacena la información de los registros durante un periodo que varía entre 1 y 6 años, dependiendo del tipo de información registrada, en concordancia con lo establecido en el punto 5.4.3.

5.5.3 Protección del archivo

ECERT protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo.

El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable. ECERT asegura la correcta protección de los archivos mediante la asignación de personal calificado para su tratamiento y el almacenamiento en instalaciones seguras.

5.5.4 Procedimientos de copias de seguridad de archivo

La copia de seguridad se encuentra externa al centro de datos donde se genera el respaldo.

5.5.5 Requisitos para el sellado de tiempo de los registros

Los Certificados, CRLs y otras entradas en la base de datos de revocación deben incluir información de fecha y hora. Esta información temporal no requiere estar respaldada criptográficamente.

5.5.6 Sistema de recopilación de archivos (interno o externo)

El sistema de auditoria interno está centralizado en un sistema de gestión de eventos e información de seguridad.

5.5.7 Procedimiento para obtener y verificar información de archivo

Sólo personal de confianza autorizado de ECERT puede obtener acceso al archivo. La integridad de la información es verificada cuando el archivo se recupera desde los registros archivados.

5.6 Cambio de clave

El proceso de cambio de claves de una Autoridad Certificación (CA) es un procedimiento crítico y delicado que debe llevarse a cabo con cuidado para garantizar la seguridad y la continuidad del servicio, por lo cual ECERT ha desarrollado un “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050), el que es de uso confidencial.

5.7 Compromiso y recuperación ante desastres

5.7.1 Procedimiento de manejo de incidentes y compromisos

ECERT ha desarrollado Políticas de Seguridad y Continuidad del Negocio 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.

5.7.2 Los recursos informáticos, el software y/o los datos están dañados

Cuando ocurra un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión correspondientes de acuerdo con la Políticas de Continuidad de Negocios de ECERT. Estas políticas incluyen el escalamiento, investigación y respuesta al incidente de continuidad de negocio.

5.7.3 Procedimiento de compromiso de clave privada de la entidad

En caso de que ECERT sospeche o confirme el compromiso de las claves privadas de la CA, se pondrán en marcha los procedimientos establecidos en las políticas de seguridad, gestión de incidentes y continuidad del negocio, 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.

5.7.4 Capacidades de continuidad del negocio después de un desastre

Se restablecerán los servicios críticos (suspensión, revocación y publicación de información de estado de certificados) 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.

5.8 Terminación de la CA o RA

En caso de que ECERT cese voluntariamente en la prestación los servicios de certificación de firma electrónica avanzada comunicarán tal situación a los Titulares con una antelación de a lo menos dos meses. Asimismo, indicará que, de no existir objeción a la transferencia de los certificados a otro certificador, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el Tercero que Confía ha consentido en la transferencia de estos. En caso de que el Titular se oponga a la transferencia del certificado a otro prestador de servicios de certificación, éste será revocado y ECERT restituirá la parte

del precio que corresponda por tiempo en que el servicio no será prestado, no teniendo el Titular derecho a algún tipo de compensación o indemnización de naturaleza diferente.

6 CONTROLES TÉCNICOS DE SEGURIDAD

La seguridad en un sistema biométrico implica una combinación de medidas técnicas, físicas y procedimentales para proteger los datos biométricos contra accesos no autorizados, manipulaciones y pérdidas. Implementar controles robustos, mantener el software actualizado, y asegurar el cumplimiento de las normativas de protección de datos son fundamentales para garantizar la integridad y la privacidad en el manejo de datos biométricos.

6.1 Controles de seguridad informática

6.1.1 Requisitos técnicos específicos de seguridad informática

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 informática.

6.1.2 Clasificación de seguridad informática

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.

6.2 Controles técnicos del ciclo de vida

6.2.1 Controles del desarrollo del sistema

ECERT cuenta con una Política (PO-GSI-0002) y Procedimiento de Desarrollo seguro de software (PR-SGI-0003).

6.2.2 Controles de gestión de seguridad

ECERT ha certificado los procesos de "Provisión de servicios de firma electrónica avanzada" conforme al estándar ISO 27001, asegurando el cumplimiento de los requisitos del Sistema de Gestión de la Seguridad de la Información.

Adicionalmente, se llevan a cabo actividades de formación y concienciación para los colaboradores en seguridad de la información, según el plan de formación anual de ECERT.

6.2.3 Controles de seguridad del ciclo de vida

ECERT para asegurar el cumplimiento de los controles establecidos en la norma ISO 27001, anualmente se somete a un proceso de Auditoría interna y externa al Sistema de Gestión de la Seguridad de la Información.

6.3 Controles de seguridad de red

ECERT como organización certificada ISO 27001 ha establecido controles de seguridad en las redes con la finalidad de proteger los activos de la información relacionados a los procesos de Certificación de firma electrónica avanzada, por ejemplo:

a) Control de Acceso
b) Protección de la Red
c) Seguridad de las Comunicaciones
d) Monitoreo y Registro

e) Gestión de Incidentes

6.4 6.4 Sellado de tiempo

El sellado de tiempo es un proceso mediante el cual se certifica y registra electrónicamente la fecha y hora en que un documento digital o un conjunto de datos fueron firmados digitalmente. ECERT sincroniza los con el servicio NTP del SHOA.

7 AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

ECERT, en su calidad de certificador acreditado, es inspeccionado anualmente por la Entidad Acreditadora para mantener vigente la acreditación obtenida en el año 2003.

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.

7.1 Frecuencias o circunstancias de evaluación

ECERT lleva a cabo una auditoría de Cumplimiento (Terceras partes) de manera anual. Sin embargo, eso no excluye que se puedan realizar auditorías internas bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

7.2 Identidad/calificaciones del evaluador

Las auditorías de Terceras partes deberán ser realizadas por una empresa auditora externa e independiente, con experiencia demostrada en seguridad de la información o por profesionales de informática acreditados en seguridad TI.

7.3 Relación del evaluador con la entidad evaluada

Las auditorías de Terceras partes se llevarán a cabo por empresas independientes a ECERT. Estas empresas no deben tener conflicto de intereses que obstaculicen su capacidad para realizar servicios de auditoría.

En el caso de las auditorías a las Autoridades de Registro estas pueden realizarse por el Auditor interno de ECERT.

7.4 Temas cubiertos por la evaluación

La auditoría verifica el cumplimiento en base al servicio contratado, por tanto, el alcance de esta se define en el "Plan de Auditoría" acordado entre las partes.

7.5 Acciones optadas como resultado de la deficiencia

Una vez que la dirección de ECERT recibe el informe de la auditoría, se analizan las deficiencias encontradas con la empresa auditora. Posteriormente, ECERT elaborará un plan de acciones correctivas.

Si ECERT es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Sistema de Gestión de ECERT que podrá ejecutar las siguientes acciones:

a) Cesar las operaciones transitoriamente.
b) Revocar la clave de la Autoridad de Certificación y regenerar la infraestructura.
c) Terminar el servicio de la Autoridad de Certificación.
d) Otras acciones complementarias que resulten necesarias.

7.6 Comunicación de resultados

Los informes de resultados de auditoría se entregan al Comité de ECERT en un plazo máximo de 15 días hábiles tras la ejecución de la auditoría.

8 OTROS ASUNTOS COMERCIALES Y LEGALES

8.1 Tarifas

El Solicitante deberá pagar las tarifas correspondientes a los certificados solicitados, las cuales de detallan en este mismo punto de las Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

8.1.1 Tarifas de emisión o renovación de certificados

ECERT puede establecer una tarifa por la emisión o por la renovación de los certificados, la que se informará oportunamente a los Titulares.

8.1.2 Tarifas de acceso al certificado

ECERT no ha establecido ninguna tarifa por el acceso a los certificados.

8.1.3 Tarifas de acceso a la información de revocación o estado

ECERT no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

8.1.4 Tarifas por otros servicios

No aplica.

8.1.5 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 que los certificados son productos elaborados por AUTORIDAD DE CERTIFICACIÓN conforme a las especificaciones proporcionadas por el Titular (nombre, RUT y correo electrónico). La negativa posterior a aceptar un certificado por motivos distintos a errores o inexactitudes en el mismo, o la no utilización del certificado, no confiere al Titular el derecho a solicitar un reembolso.

8.2 Responsabilidad financiera

8.2.1 Cobertura de seguro

ECERT limita su responsabilidad al ejercicio de su actividad durante el ciclo de vida del certificado y hasta por un monto máximo de UF 5.000. 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 de un certificado de firma electrónica.

8.2.2 Otros activos

No aplica.

8.2.3 Cobertura de seguro o garantía para entidades finales

ECERT limita su responsabilidad al ejercicio de su actividad durante el ciclo de vida del certificado y hasta por un monto máximo de UF 5.000. 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 de un certificado de firma electrónica.

8.3 8.3 Confidencialidad de la información empresarial

8.3.1 Alcance de la información confidencial

Las siguientes informaciones son mantenidas confidenciales por ECERT:

a) Solicitudes de certificados, aprobadas o rechazados.

b) Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
c) Registros de auditoría interna y externa, creados y/o mantenidos por la Autoridad de Certificación y sus auditores.
d) Planes de continuidad de negocio y recuperación de desastres.
e) Planes de seguridad.
f) Documentación de operaciones, archivo, monitorización y otros análogos.
g) Toda otra información identificada como “Confidencial”.

8.3.2 Información que no está dentro del alcance de la información confidencial

La siguiente información se considera no confidencial:

a) La contenida en la presente “DPSB de ECERT”.
b) La contenida en la Política de Certificación “CPB de ECERT”.”.
c) La información contenida en los certificados, puesto que para su emisión el Titular otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
d) Las listas de revocación de certificados (CRL’s), así como las restantes informaciones de estado de revocación.
e) La información contenida en el registro público de certificados (OCSP).
f) Cualquier información cuya publicidad sea impuesta normativamente.

Toda otra información que no esté identificada como “Uso Interno” o “Confidencial”.

8.3.3 Responsabilidad de proteger la información confidencial

ECERT divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del Titular del certificado.

8.4 Privacidad de la información personal

8.4.1 Política de privacidad

Para ECERT, la privacidad de la información es fundamental y con el objetivo de protegerla adecuadamente, hemos desarrollado una Política de Tratamiento de Datos (PO-GER-0008) que detalla cómo gestionamos los datos personales de los Titulares de certificados de firmas, cumpliendo con el marco legal establecido por la Ley 19.799 y en los términos definidos por la Ley 19.628. Puede consultar nuestra política vigente en https://www.ecertla.com sección “Políticas y Prácticas de ecert”.

8.4.2 Información tratada como privada

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.

Cualquier información sobre los Titulares que no está disponible públicamente a través del contenido del Certificado emitido, el directorio de Certificados y la CRL en línea se trata como información privada.

8.4.3 Información no considerada como privada

Toda clase de información que es tratada en la prestación de los servicios y que no es considerada dato personal o dato sensible en los términos establecidos en la Ley 19.628.

8.4.4 Responsabilidad de proteger información privada

Los participantes ECERT que reciban información privada deben asegurarla contra compromisos y divulgación a terceros y deberán cumplir con todas las leyes de privacidad locales de su jurisdicción.

8.4.5 Aviso y consentimiento para el uso de la información privada

A menos que se indique lo contrario en esta "DPSB de ECERT", en la Política de Tratamiento de Datos (PO-GER-0008) o por aceptación del contrato del Titular, la información privada no será utilizada sin el consentimiento de la parte a la que corresponde dicha información. Esta sección se rige por las leyes de privacidad pertinentes.

8.4.6 Divulgación en virtud de un proceso judicial o administrativo

En caso de orden judicial o administrativa competente, ECERT entregará los datos personales que haya recolectado en el marco de la prestación de sus servicios.

8.4.7 Otras circunstancias de divulgación de información

No aplica.

8.5 Derechos de propiedad intelectual

En ECERT, reconocemos y protegemos la importancia crucial de los derechos de propiedad intelectual e industrial en el ámbito de la tecnología. Estos derechos son fundamentales para fomentar la innovación, asegurar nuestra competitividad y mantener nuestra posición de liderazgo en el sector.

ECERT será 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, Titulares 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.

8.6 Declaraciones y garantías

8.6.1 Declaraciones y garantías de CA

ECERT se compromete a:

a) Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados 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 esta "DPSB de ECERT" y la Política de Certificado de Firma Electrónica Avanzada (MI-FEA-0029).

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) Cumplir con lo dispuesto en la Ley 19.496 sobre protección de los derechos de los consumidores y en la Ley 19.628 sobre protección de la vida privada.

e) Aprobar o rechazar las solicitudes de certificados, directamente o a través de las Entidades de Registro, de conformidad con esta "DPSB de ECERT" y la Política de Certificado de Firma Electrónica Avanzada (MI-FEA-0029).

f) Emitir los certificados en conformidad al procedimiento establecido en esta "DPSB de ECERT".

g) Proveer al titular el e-Token o de un dispositivo criptográfico masivo (HSM) para que custodie los datos de creación de firma.

h) Cuando los datos de creación de firma se almacenen en un dispositivo masivo criptográfico poner a disposición del titular un segundo factor de seguridad (con alta fiabilidad) para permitir que los datos de creación de firma se mantengan bajo su exclusivo control.

i) Comunicar al titular de la emisión de su certificado.

j) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que han quedado sin efecto.

k) Suspender o revocar los certificados emitidos, según corresponda, notificando de ello al titular.

l) Realizar razonables esfuerzos para comunicar a los titulares cualquier hecho conocido por ECERT que pudiera afectar la validez del certificado.

m) Delegar la función de Entidad de Registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.

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

8.6.2 Declaraciones y garantías de RA

La Autoridad de Registro se compromete a:

a) Comprobar la identidad del solicitante de un certificado de firma electrónica, según el procedimiento establecido en esta Declaración y en la política de certificado aplicable.

b) Obtener la aceptación del contrato del titular por parte del solicitante.

c) Aprobar o rechazar las solicitudes de certificados, directamente o a través de sus Entidades de Registro, conforme a esta “DPSB de ECERT”.

d) Permitir operar solo certificados de firma electrónica avanzada que hayan sido aceptados por el solicitante.

e) Conservar por 6 años la información utilizada como base para la emisión de los certificados de firma electrónica avanzada o remitirla a ECERT dentro de los plazos convenidos.

f) Recibir las solicitudes de revocación de certificados de firma electrónica e informarlas a ECERT.

g) Prestar cualquier otro servicio que ECERT le solicite y que guarde relación con la actividad de certificación de firma electrónica.

h) La Entidad de Registro realiza todas las actuaciones indicadas anteriormente, gestionando el ciclo de vida del certificado de firma electrónica, por cuenta y riesgo de ECERT.

8.6.3 Declaraciones y garantías del Titular

El Titular es responsable de:

a) Ser persona natural mayor o igual a 18 años.
b) Entregar información veraz a ECERT y/o la Entidad de Registro al momento de solicitar el certificado de firma.
c) Validar que los datos contenidos en el certificado de firma son verdaderos.
d) Pagar la tarifa asociada al certificado solicitado.
e) Aceptar los términos y condiciones descritos en esta "DPSB de ECERT" y la "CPB de ECERT".
f) Aceptar contrato Titular.
g) No usar los datos de creación de firma una vez que el certificado haya expirado, esté revocado o suspendido.

8.6.4 Declaraciones y garantías de la parte que confía

Las partes que confían deben garantizar que cuentan con información suficiente para confiar en la información de un certificado emitido por ECERT y que son responsables de decidir confiar en estos certificados y que por lo tanto asumirán las consecuencias legales si no cumplen con estas garantías descritas en esta Política.

8.6.5 Declaraciones y garantías de otros participantes

No Aplica.

8.7 Renuncias de garantías

ECERT rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en los puntos 8.6.1 y 8.6.2.

8.8 Limitaciones de responsabilidad

ECERT limita su responsabilidad de acuerdo con los establecido en este documento en los puntos 4.1.2 y 8.2.1 de este documento.

8.9 Indemnizaciones

Aplica de acuerdo con lo establecido en la legislación vigente y en concordancia con los puntos 4.1.2.3, letra o) y 4.1.2.4, letra e) los Titulares y partes que confían deberán Indemnizar a ECERT y/o a la Autoridad de registro de todo daño o perjuicio proveniente de cualquier acción u omisión negligente, culposa o dolosa de su parte.

8.10 Plazo y terminación

8.10.1 Plazo

Esta Declaración de Prácticas de Certificación 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 Política debe entrar en vigor partir de la fecha en que se publica en www.ecertla.com.

8.10.2 Terminación

Esta Declaración de Prácticas de Certificación permanecerá vigente hasta que se genere una nueva versión y sea reemplaza en la página web de ECERT www.ecertla.com.

8.10.3 Efecto de la terminación y la supervivencia

La Autoridad de Certificación vela porque al menos ciertas reglas continúen vigentes tras el término de la relación jurídica reguladora del servicio entre las partes y al menos las

obligaciones contenidas en el punto 4.1.2 de esta Política de Certificación continúen vigentes tras el término del servicio.

8.11 Avisos y comunicaciones individuales con los participantes

Cada una de las partes utilizaran formas comercialmente razonables para comunicarse entre sí, las que se pueden llevar a cabo por medios electrónicos como son el correo electrónico proporcionado por Titular y el correo informado por ECERT en el punto 1.5.2 de esta Política.

Sin embargo, el Titular tiene la obligación de responder de manera oportuna cualquier comunicación o requerimiento de información relacionado con el ciclo de vida del certificado que le haga ECERT.

8.12 Enmiendas

8.12.1 Procedimiento de modificación

Cualquier nueva versión de esta "DPSB de ECERT" estará sujeta al procedimiento de aprobación indicados en el punto 1.5.4 de este documento.

8.12.2 Mecanismo y plazo de notificación

ECERT se reserva el derecho de modificar esta "DPSB de ECERT", considerando que se aplicaran los siguientes mecanismos de notificación hacia las partes interesadas:

Modificaciones Materiales: corresponden a enmiendas que modifiquen significativamente el ciclo de vida del certificado.

Modificaciones no Materiales: corresponden a los cambios se limiten a errores tipográficos, cambios en información de contacto, URL, Nombre de roles ECERT, etc.

Ambos tipos de modificaciones implicaran nuevas publicaciones en la página web de ECERT El plazo para recibir comentarios a estas políticas es de 10 días corridos, a partir de la publicación en el sitio web de ECERT.

Transcurrido dicho plazo sin que medie comunicación se entenderá que Titulares y Partes que confían acepta los cambios introducidos.

Una vez que se publique la nueva ““DPSB 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.

8.12.3 Circunstancias en las que debe cambiar el OID

Si ECERT determina que es necesario realizar un cambio en el identificador de objeto (OID) correspondiente a la Declaración de Prácticas de Certificación, la enmienda deberá incluir los nuevos identificadores de objeto (OID) de dicha Política.

8.13 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.

8.14 Ley Aplicable

Esta “DPSB de ECERT” se rige por la ley chilena y se someterán al Tribunal Arbitral expresado en el punto 9.13.

8.15 Cumplimiento de la legislación aplicable

ECERT cumple con toda la legislación aplicable en la prestación de sus servicios de certificación.

8.16 Disposiciones diversas

8.16.1 Acuerdo completo

Esta Política de Certificación junto con la Declaración de Prácticas y el Contrato Titular de Certificado constituye el acuerdo completo entre las partes y reemplaza cualquier acuerdo previo.

8.16.2 Cesión

No aplica.

8.16.3 Divisibilidad

Si alguna disposición de esta política se considera inválida o inaplicable, las disposiciones restantes seguirán siendo válidas y aplicables.

8.16.4 Ejecución (honorarios de abogados y renuncia de derechos).

No Aplica.

8.16.5 Fuerza Mayor

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

Las obligaciones de 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 “DPSB 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.

8.17 Otras disposiciones

No aplica.

9 CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
3	11-01-2021	Creación del documento en ISOEasy.
4	01-08-2022	Revisión Anual IAO 2022
5	03-08-2023	Revisión anual IAO 2023
6	28-08-2024	Cambio de formato Revisión anual IAO 2024
7	14-08-2025	Mejoras 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 Certificación. • Actualización del enlace a la CRL (Lista de Certificados Revocados) y Vigencia de certificado conforme al nuevo sitio web. • Ampliación de la información publicada en la web relacionada con la verificación de certificados. • Incorporación de un mecanismo de notificación para comunicar la entrada en vigencia de nuevos documentos. • Inclusión de cuatro nuevos documentos que complementan esta Política. • Precisión en la frecuencia y forma de publicación de la información sobre certificados. • Inclusión del detalle sobre la fuente del nombre del titular que figura en el certificado de firma. • Se actualiza Repositorio de Documentación. Revisión Anual IAO 2025
8	25-09-2025	Mejora en redacción por Aclaratoria IAO 2025: • Se incorporan plazos de actualización o revisión de este documento.

Fin del documento