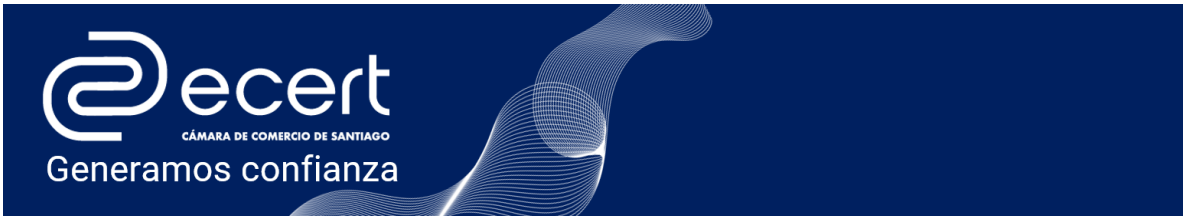

Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (CPS de ECERT)

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
G.A.M. FEA	4.18 Requisito PO02 – Declaración de prácticas de certificación	FEA: Firma Electrónica Avanzada PKI: Gestión procesos de productos PKI (FEA)	PC-FEA-0001
ISO 9001:2015	8.5 Producción y provisión del servicio		

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	27-01-2021	12-01-2026	12-01-2026	10	27-01-2021

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Jefe de Operaciones PKI	Gerente de Cumplimiento y Consultoría	Gerente General	Gerente de Cumplimiento y Consultoría	Público

CONTENIDO

1 INTRODUCCIÓN 9
1.1 Descripción General 10
1.2 Nombre e identificación del documento 11
1.2.1 Identificadores de certificados 11
1.3 Participantes de la PKI 11
1.3.1 Autoridad de Certificación 11
1.3.2 Autoridad de Registro 11
1.3.3 Titular 12
1.3.4 Partes que Confían 12
1.3.5 Otros Participantes 12
1.4 Usos del certificado 13
1.4.1 Usos apropiados del certificado 13
1.4.2 Usos prohibidos de los certificados 13
1.5 Administración de la Política 13
1.5.1 Organización que administra el documento 13
1.5.2 Contacto 14
1.5.3 Organización que determina la idoneidad de la CPS para la Política 14
1.5.4 Procedimiento de aprobación de la CPS 14
1.6 Definiciones y acrónimos 14
2 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO 15
2.1 Repositorios 15
2.2 Publicación de información de certificación 15
2.3 Tiempo o frecuencia de publicación 16
2.4 Controles de acceso a los repositorios 17
3 IDENTIFICACIÓN Y AUTENTICACIÓN 17
3.1 Denominación 17
3.1.1 Tipos de nombres 17
3.1.2 Necesidad de que los nombres tengan significado 18
3.1.3 Anonimato o seudónimo de los Titulares 18
3.1.4 Reglas para la interpretación de las distintas formas de nombres 18
3.1.5 Unicidad de los nombres 19
3.1.6 Reconocimiento, Autenticación y Función de las marcas 19
3.2 Comprobación de identidad inicial 19
3.2.1 Método para demostrar la posesión de la clave privada 19
3.2.2 Autenticación de la identidad de la organización 19
3.2.3 Autenticación de la identidad individual 19
3.2.4 Información de Titular no verificada 20
3.2.5 Validación de la autoridad 20
3.2.6 Criterio de interoperabilidad 20
3.3 Identificación y autenticación para solicitudes de renovación de claves 20
3.3.1 Identificación y autenticación para la renovación rutinaria de claves 20

3.3.2 Requisitos de identificación y autenticación para la renovación de claves después de la revocación del certificado 21
3.4 Identificación y autenticación para solicitudes de revocación 21
4 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 21
4.1 Solicitud de Certificados 21
4.1.1 Quién puede presentar una solicitud de certificado 21
4.1.2 Proceso de inscripción y responsabilidades 21
4.2 Tramitación de la solicitud de certificado 22
4.2.1 Comprobación Fehaciente de Identidad 22
4.2.2 Aprobación o rechazo de la solicitud de certificado 27
4.3 Emisión y entrega del Certificado 27
4.3.1 Emisión del Certificado 28
4.3.2 Notificación de la emisión al Titular 31
4.3.3 Periodo de Vigencia y Expiración del Certificado de Titular 31
4.4 Aceptación del Certificado 31
4.4.1 Conducta que constituye la aceptación del certificado 31
4.4.2 Publicación del certificado por la CA 32
4.4.3 Responsabilidades 32
4.5 Usos de pares de claves y certificados 36
4.5.1 Uso de la Llave Privada y del Certificado por el Titular 36
4.5.2 Uso de la Llave pública y certificado de la parte que confía 37
4.6 Renovación del certificado 37
4.6.1 Circunstancias para la renovación del certificado 38
4.6.2 Quién puede solicitar la renovación 38
4.6.3 Procesamiento de solicitudes de renovación de certificados 38
4.6.4 Notificación de la emisión del nuevo certificado al Titular 38
4.6.5 Conducta que constituye aceptación de un certificado de renovación 39
4.6.6 Publicación del certificado de renovación por la CA 39
4.7 Cambio de clave del certificado 39
4.7.1 Circunstancias para la renovación de la clave del certificado 39
4.7.2 Quién puede solicitar la certificación de una nueva clave pública 39
4.7.3 Procesamiento de solicitudes de renovación de claves de certificado 39
4.7.4 Notificación de la emisión de un nuevo certificado al Titular 39
4.7.5 Conducta que constituye aceptación de un certificado con nueva clave 40
4.7.6 Publicación del certificado renovado en la CA 40
4.8 Modificación del certificado 40
4.8.1 Circunstancias para la modificación del certificado 40
4.8.2 Quién puede solicitar la modificación del certificado 40
4.8.3 Procesamiento de solicitudes de modificación del certificado 40
4.8.4 Notificación de la emisión de un nuevo certificado al Titular 40
4.8.5 Conducta que constituye aceptación de un certificado modificado 41
4.8.6 Publicación del certificado modificado por la CA 41
4.9 Revocación y suspensión del certificado 41

4.9.1 Circunstancias revocación 41
4.9.2 Quién puede solicitar la revocación 42
4.9.3 Procedimiento para la solicitud de revocación 42
4.9.4 Plazo de gracia para la solicitud de revocación 45
4.9.5 Plazo en el que la CA debe tramitar la solicitud de revocación 45
4.9.6 Requisito de comprobación de revocación para las partes que confían 45
4.9.7 Frecuencia de emisión de CRL 45
4.9.8 Latencia máxima para la CRL 46
4.9.9 Disponibilidad de comprobación de estado/revocación en línea 46
4.9.10 Requisitos de comprobación de revocación en línea 46
4.9.11 Otras formas de anuncios de revocación disponibles 46
4.9.12 Requisitos especiales en materia de compromiso de claves 46
4.9.13 Circunstancias de suspensión 46
4.9.14 Quién puede solicitar la suspensión 47
4.9.15 Procedimiento para solicitud de suspensión 47
4.9.16 Límites del periodo de suspensión 48
4.10 Servicios de estado de certificados 49
4.10.1 Características operativas 49
4.10.2 Disponibilidad del servicio 49
4.10.3 Características opcionales 49
4.11 Terminación del Contrato 49
4.12 Custodia y recuperación de claves 49
4.12.1 Política y prácticas de depósito y recuperación de llaves 49
4.12.2 Política y prácticas de encapsulamiento y recuperación de llaves de sesión 49
5 CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIÓN 50
5.1 Controles físicos 50
5.1.1 Ubicación del sitio y construcción 50
5.1.2 Acceso físico 51
5.1.3 Energía y aire acondicionado 51
5.1.4 Exposición al agua 51
5.1.5 Prevención y protección contra incendios 52
5.1.6 Almacenamiento de medios 52
5.1.7 Eliminación de residuos 52
5.1.8 Copia de seguridad externa 52
5.2 Controles de procedimiento 52
5.2.1 Roles de confianza 52
5.2.2 Número de personas necesarias por tarea 53
5.2.3 Identificación y autenticación para cada rol 53
5.2.4 Funciones que requieren separación de funciones 54
5.3 Controles de personal 54
5.3.1 Requisitos de cualificación, experiencia y autorización 54
5.3.2 Procedimiento de verificación de antecedentes 55

5.3.3 Requisitos de formación 55
5.3.4 Frecuencia y requisitos de reentrenamiento 56
5.3.5 Frecuencia y secuencia de rotación de puestos 56
5.3.6 Sanciones por acciones no autorizadas 56
5.3.7 Requisitos del contratista independiente 56
5.3.8 Documentación suministrada al personal 57
5.4 Procedimientos de registro de auditoria 57
5.4.1 Tipos de eventos registrados 57
5.4.2 Frecuencia de procesamiento del registro 58
5.4.3 Periodo de conservación del registro de auditoria 58
5.4.4 Protección del registro de auditoria 58
5.4.5 Procedimientos de copias de seguridad del registro de auditoria 58
5.4.6 Notificación al sujeto causante del evento 59
5.4.7 Evaluaciones de vulnerabilidad 59
5.5 Registros archivados 59
5.5.1 Tipos de registros archivados 59
5.5.2 Periodo de conservación de los datos archivados 59
5.5.3 Protección del archivo 60
5.5.4 Procedimientos de copias de seguridad de archivo 60
5.5.5 Requisitos para el sellado de tiempo de los registros 60
5.5.6 Sistema de recopilación de archivos (interno o externo) 60
5.5.7 Procedimiento para obtener y verificar información de archivo 60
5.6 Cambio de clave 60
5.7 Compromiso y recuperación ante desastres 61
5.7.1 Procedimiento de manejo de incidentes y compromisos 61
5.7.2 Los recursos informáticos, el software y/o los datos están dañados 61
5.7.3 Procedimiento de compromiso de clave privada de la entidad 61
5.7.4 Capacidades de continuidad del negocio después de un desastre 61
5.8 Terminación de la CA o RA 62
6 CONTROLES TÉCNICOS DE SEGURIDAD 62
6.1 Generación e instalación de pares de claves 62
6.1.1 Generación de pares de claves 62
6.1.2 Entrega de claves privadas al Titular 63
6.1.3 Entrega de claves pública al emisor del certificado 63
6.1.4 Entrega de clave pública de CA a partes confiables 63
6.1.5 Tamaños de claves 63
6.1.6 Generación de parámetros de clave pública y control de calidad 63
6.1.7 Fines de uso de la clave (según el campo de uso de clave X.509 V3) 63
6.2 Protección de claves privadas e ingeniería de módulos criptográficos 64
6.2.1 Estándares y controles del módulo criptográfico 64
6.2.2 Control multi-persona de clave privada (n de m) 64
6.2.3 Depósito de clave privada 64
6.2.4 Copia de seguridad de la clave privada 64

6.2.5 Archivado de la clave privada 64
6.2.6 Transferencia de la clave privada hacia o desde un módulo criptográfico ... 65
6.2.7 Almacenamiento de clave privada en el módulo criptográfico 65
6.2.8 Método de activación de la clave privada 65
6.2.9 Método de desactivación de la clave privada 65
6.2.10 Método de destrucción de la clave privada 65
6.2.11 Clasificación del módulo criptográfico 65
6.3 Otros aspectos de la gestión de pares de claves 66
6.3.1 Archivado de claves públicas 66
6.3.2 Periodos operativos del certificado y periodos de uso del par de claves 66
6.4 Datos de activación 66
6.4.1 Generación e instalación de datos de activación 66
6.4.2 Protección de datos de activación 66
6.4.3 Otros aspectos de los datos de activación 66
6.5 Controles de seguridad informática 67
6.5.1 Requisitos técnicos específicos de seguridad informática 67
6.5.2 Clasificación de seguridad informática 67
6.6 Controles técnicos del ciclo de vida 67
6.6.1 Controles del desarrollo del sistema 67
6.6.2 Controles de gestión de seguridad 68
6.6.3 Controles de seguridad del ciclo de vida 68
6.7 Controles de seguridad de red 68
6.8 Sellado de tiempo 68
7 PERFILES DE CERTIFICADOS, CRL Y OCSP 69
7.1 Perfil del certificado 69
7.1.1 Números de versión 71
7.1.2 Extensiones de certificado 71
7.1.3 Identificadores de objetos de algoritmo 74
7.1.4 Forma de los nombres 74
7.1.5 Restricciones de nombre 74
7.1.6 Identificador de objeto de política de certificado 74
7.1.7 Uso de la extensión restricciones de política 74
7.1.8 Sintaxis y semántica de los certificadores de políticas 75
7.1.9 Semántica de procesamiento para las políticas de certificación critica 75
7.2 Perfil CRL 75
7.2.1 Números de versión 76
7.2.2 CRL y extensiones de entrada 76
7.3 Perfil OCSP 77
7.3.1 Números de versión 77
7.3.2 Extensiones OCSP 77
8 AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 78
8.1 Frecuencias o circunstancias de evaluación 78
8.2 Identidad/calificaciones del evaluador 78

8.3 Relación del evaluador con la entidad evaluada 78
8.4 Temas cubiertos por la evaluación 79
8.5 Acciones optadas como resultado de la deficiencia 79
8.6 Comunicación de resultados 79
9 OTROS ASUNTOS COMERCIALES Y LEGALES 79
9.1 Tarifas 79
9.1.1 Tarifas de emisión o renovación de certificados 80
9.1.2 Tarifas de acceso al certificado 80
9.1.3 Tarifas de acceso a la información de revocación o estado 80
9.1.4 Tarifas por otros servicios 80
9.1.5 Política de reembolso 81
9.2 Responsabilidad financiera 81
9.2.1 Cobertura de seguro 81
9.2.2 Otros activos 81
9.2.3 Cobertura de seguro o garantía para entidades finales 81
9.3 Confidencialidad de la información empresarial 82
9.3.1 Alcance de la información confidencial 82
9.3.2 Información que no está dentro del alcance de la información confidencial 82
9.3.3 Responsabilidad de proteger la información confidencial 83
9.4 Privacidad de la información personal 83
9.4.1 Política de privacidad 83
9.4.2 Información tratada como privada 83
9.4.3 Información no considerada como privada 83
9.4.4 Responsabilidad de proteger información privada 84
9.4.5 Aviso y consentimiento para el uso de la información privada 84
9.4.6 Divulgación en virtud de un proceso judicial o administrativo 84
9.4.7 Otras circunstancias de divulgación de información 84
9.5 Derechos de propiedad intelectual 84
9.6 Declaraciones y garantías 85
9.6.1 Declaraciones y garantías de CA 85
9.6.2 Declaraciones y garantías de RA 86
9.6.3 Declaraciones y garantías del Titular 87
9.6.4 Declaraciones y garantías de la parte que confía 87
9.6.5 Declaraciones y garantías de otros participantes 87
9.7 Renuncias de garantías 88
9.8 Limitaciones de responsabilidad 88
9.9 Indemnizaciones 88
9.10 Plazo y terminación 88
9.10.1 Plazo 88
9.10.2 Terminación 88
9.10.3 Efecto de la terminación y la supervivencia 89
9.11 Avisos y comunicaciones individuales con los participantes 89

9.12 Enmiendas 89
9.12.1 Procedimiento de modificación 89
9.12.2 Mecanismo y plazo de notificación 89
9.12.3 Circunstancias en las que debe cambiar el OID 90
9.13 Disposiciones de resolución de disputas 90
9.14 Ley Aplicable 91
9.15 Cumplimiento de la legislación aplicable 92
9.16 Disposiciones diversas 92
9.16.1 Acuerdo completo 92
9.16.2 Cesión 92
9.16.3 Divisibilidad 92
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos) 92
9.16.5 Fuerza Mayor 93
9.17 Otras disposiciones 93
10 CONTROL DE VERSIONES 94

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.

Esta Práctica de Certificación de Firma Electrónica Avanzada de ECERT describe detalladamente las políticas, procedimientos y mecanismos que seguimos en la prestación de nuestros servicios de certificación de firma electrónica avanzada.

Estas prácticas incluyen:

- Las obligaciones y responsabilidades de ECERT, sus Autoridades de Registro, los Solicitantes, Titulares y las Partes que confían en los certificados.
- La gestión del ciclo de vida del certificado.
- Los procedimientos de auditoría.
- La forma en que protegemos los datos personales.
- La forma en que gestionamos las contingencias y recuperación ante desastres.
- Las prácticas de seguridad física, del personal y el manejo de claves de ECERT.
- El contenido y la estructura de los certificados de firma electrónica avanzada.

Este documento está dirigido a:

a) Titulares de Certificados, quienes necesitan comprender cómo se valida su identidad al momento de la emisión del certificado de firma, 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.

Este documento ha sido elaborado, en cumplimiento con el Decreto Supremo 181 de 2002 y la Guía de Evaluación del Procedimiento de Acreditación de Prestadores de Servicios de Certificación de Firma Electrónica Avanzada versión 2.0 del Ministerio de Economía, Fomento y Turismo de Chile. De manera complementaria se han utilizado los siguientes documentos:

a) Guías de Evaluación "Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Firma Electrónica Avanzada", entregado por el Ministerio de Economía, Fomento y Turismo.
b) 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.

1.1 Descripción General

La presente Declaración de Prácticas de Certificación de Firma Electrónica Avanzada, en adelante "CPS de ECERT" describe la forma en que se cumplen estos requisitos relacionados con el ciclo de vida del certificado de firma electrónica avanzada, mientras que la Política de Certificados de Firma Electrónica Avanzada (MI-FEA-0029) en adelante "CP de ECERT", establece los requisitos que deben cumplirse, 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 la Certificación de la Firma Electrónica Avanzada.

La actividad de certificación de Firma Electrónica avanzada que realiza ECERT se encuentra acreditada por la Entidad Acreditadora desde el año 2003, mediante la Resolución Exenta Nº 317, de la Subsecretaría de Economía del Gobierno de Chile.

1.2 Nombre e identificación del documento

El presente documento establece la Declaración de Practicas de Certificación (PC-FEA-0001) dedicada a la emisión de certificados electrónicos de 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.

Tipo de certificados	Número de OID
Empresa ECERT	1.3.6.1.4.1.8658
Firma Electrónica Avanzada	1.3.6.1.4.1.8658.5

1.3 Participantes de la PKI

1.3.1 Autoridad de Certificación

Corresponde a las entidades que están autorizados para emitir certificados.

ECERT está constituido como Autoridad de Certificación también denominado Prestador de Servicios de Certificación de Firma Electrónica Avanzada (PSC) 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. 317, de 14 de Agosto de 2003, de la Subsecretaría de Economía, Fomento y Reconstrucción.

1.3.2 Autoridad de Registro

Corresponde a las entidades que establecen procedimientos de autenticación para solicitantes de certificados.

Son personas o instituciones autorizadas por ECERT, las que actuando en nombre y bajo la responsabilidad de ECERT para una comunidad de negocio específica, realizan las siguientes funciones:

a) Comprobar fehacientemente la identidad del solicitante en el otorgamiento de certificados de firma electrónica avanzada en concordancia con el artículo 12°, letra e) de la ley 19.799.
b) Registrar los antecedentes de los solicitantes que sirven de base para la emisión de los certificados.
c) Evaluar, aprobar o rechazar las solicitudes de certificados de acuerdo con las “CP de ECERT” y “CPS de ECERT”, definidas por ECERT.
d) Ejecutar la revocación, renovación y suspensión de certificados conforme a las “CP de ECERT” y “CPS de ECERT”.

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 "CPS 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 le ha emitido un certificado de firma electrónica avanzada.

1.3.4 Partes que Confían

Son todas aquellas personas naturales o jurídicas que voluntaria y libremente deciden aceptar y confiar en los certificados digitales emitidos por ECERT.

1.3.5 Otros Participantes

Solicitante: Persona natural mayor o igual a 18 años que requiere un certificado de firma electrónica avanzada.

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

1.4 Usos del certificado

1.4.1 Usos apropiados del certificado

Los certificados de firma electrónica avanzada emitidos por ECERT pueden ser utilizados legítimamente para la autenticación de documentos electrónicos, la realización de trámites administrativos y comerciales, y la formalización de contratos y acuerdos digitales. Además, pueden ser utilizados para la suscripción de instrumentos públicos.

La utilización de estos certificados debe respetar las normativas vigentes.

1.4.2 Usos prohibidos de los certificados

Tenga en consideración que la Ley 19.799 no permite que se suscriban actos o contratos mediante firma electrónica avanzada cuando la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, la ley requiere la concurrencia personal de alguna de las partes, y se trate de actos o contratos relativos al derecho de familia.

Los certificados de ECERT no están diseñados ni su uso autorizado para situaciones peligrosas o que requieran un rendimiento a prueba de fallos. Además, no deben usarse para certificar a otras personas, objetos o establecer cadenas de confianza.

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

1.5.3 Organización que determina la idoneidad de la CPS 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 CPS

Cualquier nueva versión de estas "CPS de ECERT" 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 "CPS de ECERT" al Comité de Sistema de Gestión de ECERT.
c) Después de obtener las aprobaciones mencionadas, se publicará la nueva versión de esta "CPS de ECERT", en la página web de ECERT, indicando la fecha de entrada en vigor.

Una vez que se publique la nueva "CPS 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 9.12.2 de estas "CPS 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)	CPS
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 Certificados)	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

Los Titulares y Partes que confían deben comprobar el estado de aquellos certificados en los cuales desean confiar, por lo anterior, ECERT tiene la responsabilidad de mantener un repositorio en línea de acceso público (OCSP) donde se publican los certificados aprobados, así como la lista de certificados revocados (CRL).

2.2 Publicación de información de certificación

ECERT realiza la publicación de la información relativa a los certificados de firma electrónica avanzada 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 Certificación Firma electrónica avanzada (PC-FEA-0001) “CPS de ECERT”.
b) Políticas de Certificado de Firma electrónica avanzada (MI-FEA-0029) “CP de ECERT”.
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 “CP de ECERT” y las “CPS de ECERT”, se realiza tan pronto como esté disponible.

Los cambios en esta “CPS de ECERT” y la “CP de ECERT” se rigen por lo dispuesto en el punto 1.5 de este documento de “CPS de ECERT”.

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 de los servicios

El registro diferencia entre certificados vigentes, suspendidos y revocados. El registro de acceso público de certificados se actualiza según las siguientes reglas:

a) La información de los certificados emitidos se publica en el momento de su emisión.
b) La información sobre la suspensión de certificados se publica dentro de un plazo máximo de 24 horas laborales (entre 9:00 y 18:00 horas) desde la solicitud de suspensión.
c) La información sobre la revocación de certificados se publica dentro de un plazo máximo de 24 horas laborales (entre 9:00 y 18:00 horas) desde la solicitud de revocación.

Cualquier situación ocasionada con relación a la vigencia de un certificado y de las obligaciones contraídas por ECERT se resolverán de acuerdo con esta "CPS 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, especialmente la relacionada con el estado de revocación.

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

De acuerdo con artículo 15°, letra c, de la ley 19.799, los certificados de firma electrónica avanzada deben contener los nombres del Titular.

Los tipos de nombres se refieren a las formas en que se puede identificar al sujeto al que pertenece el certificado. 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.

Tabla 1: Campos que contiene el DN (Distinguished Name)	
Nombre Común	CN=nombre apellido1 apellido2

Unidad Organizacional	OU= Toma el valor que se incluye en el formulario.
Organización	O=E-certchile
Localidad (ciudad)	L= Toma el valor que se incluye en el formulario.
Estado (región)	S= Toma el valor que se incluye en el formulario.
País	C=CL

Para la asignación del nombre a ser contenido en los certificados se incluirán:

a) 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.

b) Los mismos nombres que se encuentran informados en el Sistema ClaveÚnica o Terceros de confianza cuando la persona haya comparecido en forma personal y directa ante las plataformas virtuales de ECERT demostrando su identidad con dicho mecanismo de identificación digital.

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 “CPS 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

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 (comprobación fehaciente de identidad) de un solicitante se lleva a cabo mediante la validación de la cédula de identidad en forma presencial ante una Autoridad de Registro ECERT, o bien mediante el mecanismo de identificación digital ClaveÚnica, según lo dispuesto en el Decreto Supremo 24 de 2019 del Ministerio de Economía, Fomento y Turismo, siguiendo los procedimientos establecidos en el punto 4 de esta “CPS de ECERT”.

3.2.4 Información de Titular no verificada

ECERT no verifica el correo electrónico ni número de teléfono de los solicitantes de certificados, exceptuando para los Certificados de firma avanzada on-line (FAO) ya que se utilizará para el envío del segundo factor de seguridad especificado en punto 4.3.1.2 de estas "CPS de ECERT".

3.2.5 Validación 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 cumplen 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 "CPS de ECERT".

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

No aplica. Una vez revocado un certificado de firma electrónica avanzada, no se renuevan las claves, sino que se debe realizar el proceso de Comprobación fehaciente de identidad para la emisión de un nuevo certificado.

3.4 Identificación y autenticación para solicitudes de revocación

El Titular del certificado debe ser autenticado mediante procedimientos seguros antes de proceder con la revocación del certificado.

Una solicitud de revocación se debe efectuar de acuerdo con las modalidades indicadas en el punto 4.9.3 de esta "CPS de ECERT".

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 en ECERT.

4.1.2 Proceso de inscripción y responsabilidades

El Solicitante deberá completar formulario de Solicitud de firma electrónica avanzada donde se debe ingresar la siguiente información:

a) Nombre completo.
b) Rut.
c) Correo electrónico personal.
d) Nro. de teléfono móvil (Obligatorio solo si desea recibir el segundo factor de seguridad por mensajería celular para utilizar el certificado de firma).

4.2 Tramitación de la solicitud de certificado

Para la tramitación de la solicitud del certificado de firma electrónica avanzada el Solicitante deberá:

a) Realizar el pago de la tarifa correspondiente. El solicitante se obliga a pagar a ECERT y/o a las Autoridades de Registro las tarifas establecidas para los certificados de firma electrónica avanzada. Las tarifas se encuentran permanentemente publicadas y disponibles en www.ecertla.com. El pago indicado se realiza exclusivamente en virtud de la emisión del certificado. El Titular no tendrá derecho a solicitar ningún reembolso considerando que el certificado se emite con datos que el titular provee a la Entidad de Registro en el momento de la emisión del certificado de firma. De este modo, de conformidad con lo dispuesto en la letra b) del artículo 3 bis de la Ley 19.496, sobre derechos de los consumidores, no puede ejercerse el derecho a retracto por ser los certificados bienes o productos que ECERT los confecciona conforme a las especificaciones que el titular ha proporcionado (nombre, RUT y correo electrónico).
b) La tarifa asociada a la compra por volumen de certificados de firma electrónica avanzada ya sea por parte de una persona natural, de una empresa o institución para sus clientes o colaboradores se acordará de manera individual en cada caso y su pago se efectuará fuera de este proceso.
c) Aceptar el contrato de adhesión del titular el cual tiene como objetivo principal asegurar que el uso de la firma electrónica avanzada se realice de manera segura y conforme a la legislación vigente, protegiendo tanto al titular como a ECERT.

4.2.1 Comprobación Fehaciente de Identidad

ECERT en cumplimiento con la legislación vigente cuenta con dos modalidades de Comprobación Fehaciente de Identidad:

a) Modalidad Presencial.
b) Modalidad Presencial ClaveÚnica.

4.2.1.1 Modalidad Presencial:

Compareciendo en forma personal (físicamente) y directa a las oficinas de ECERT o ante una Autoridad de Registro, en estos casos la Autoridad de Registro ejecutará el proceso pidiendo la siguiente información al solicitante:

c) Paso 1: En las compras efectuadas a través de www.ecertla.com plataforma web pública de ECERT donde cualquier persona puede consultar información institucional, servicios y canales de contacto. Debe presentar la copia de la aprobación de la solicitud de certificado enviada al correo, ya sea en formato impreso o digital. En caso de no contar con ella, el registro podrá localizarse presentando su cédula de identidad y proceder a su validación.

d) Paso 2: Presentar Cédula de Identidad vigente (exigencia del artículo 15°, letra c, de la ley 19.799), con perfecto estado de los elementos que permiten la lectura biométrica.

e) Paso 3: Se comparan los datos personales ingresados por el solicitante en la página Web al momento de la compra con la cedula de identidad y se solicita el teléfono de contacto (no es obligatorio).

f) Paso 4: Colocar su huella dactilar los dispositivos habilitados especialmente para la comprobación fehaciente de identidad. ECERT valida la identidad a través de un pareo entre la información biométrica de la cédula de identidad y la huella dactilar del solicitante, proceso Match on card, para mayor detalle consultar la "DPSB de ECERT" (PC-BIO-0001). El resultado de esta comparación será una comprobación exitosa o rechazo de identidad. La biometría empleada por ECERT se encuentra acreditada ante la Subsecretaría de Economía y Empresas de Menor Tamaño mediante Resolución Administrativa Exenta Nº 3919 de 7 de diciembre de 2016.

g) Paso 5: 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, en los términos exigidos por el Auto Acordado sobre Uso de Documento y Firma Electrónica por Notarios, Conservadores y

Archiveros Judiciales de 2006. La Autoridad de Registro conservará una copia de esta certificación y en caso de ser exitosa la Comprobación fehaciente de identidad, esta información es incorporada en el detalle del certificado digital de firma electrónica avanzada generado.

Si el solicitante adquiere un dispositivo e-token y requiere que el proceso de comprobación fehaciente de identidad se realice de manera presencial en su domicilio por un Operador de Registro, ECERT ofrece este servicio con un costo adicional. El detalle de este costo está disponible en la página web de nuestra empresa.

Los procesos de comprobación fehaciente de identidad, emisión y descarga del certificado de firma se realizan en un entorno seguro, conforme a las políticas de seguridad de la información de ECERT. Por lo tanto, se aplican procedimientos de control de acceso lógico a través de una red segura, como VPN o la red Wi-Fi proporcionada por ECERT

En caso de fallo del sistema biométrico, el solicitante deberá comenzar un nuevo proceso de Comprobación de identidad y la Autoridad de Registro solicitará la siguiente información al solicitante:

a) Paso 1: Presentar la copia de la aprobación de la solicitud de certificado que le haya sido enviada.
b) Paso 2: Presentar Cédula de Identidad vigente (exigencia del artículo 15°, letra c, de la ley 19.799), con perfecto estado físico, no debe estar quebrada, rayada, doblada y debe ser visualmente legible.
c) Paso 3: Se comparan los datos personales ingresados por el solicitante en la página Web al momento de la compra con la cedula de identidad y se solicita el teléfono de contacto (no es obligatorio).
d) Paso 4: 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, en los términos exigidos por el Auto Acordado sobre Uso de Documento y Firma Electrónica por Notarios, Conservadores y

Archiveros Judiciales de 2006. La Autoridad de Registro conservará una copia de esta certificación y en caso de ser exitosa la Comprobación fehaciente de identidad, esta información es incorporada en el detalle del certificado digital de firma electrónica avanzada generado.

e) Paso 5: Si el solicitante cuenta con la información completa y vigente, entonces la autoridad de registro generara el "Formulario de Recepción de documentos" el cual contiene:
    i. Numero de Solicitud
    ii. Nombre completo del Solicitante
    iii. Rut
    iv. Numero de documento asociado al rut
    v. Correo electrónico
    vi. Imagen del CI por ambos lados
    vii. Fotografía del Solicitante
    viii. Huella dactilar Solicitante.
    ix. Nombre del Operador de Registro
    x. Rut del operador de Registro
    xi. Fecha de la Comprobación fehaciente identidad
    xii. Firma con puño y letra del Solicitante
    xiii. Firma con puño y letra del Operador de Registro de ECERT.

4.2.1.2 Modalidad Presencial ClaveÚnica:

h) Paso 1: Comparecencia presencial en plataforma Virtual de ECERT, las cuales pueden ser:

i) Página Web www.ecertla.com: Plataforma Web pública de ECERT donde cualquier persona puede consultar información institucional, servicios y canales de contacto.

j) GRUP www.migrup.cl: Plataforma Web privada orientada a personas naturales, que permite firmar documentos de manera ilimitada con firma electrónica avanzada y enviar documentos a terceros mediante firmas prepagadas, incluso si ellos no cuentan con firma electrónica.

k) Portal Empresa https://portalempresa.ecertchile.cl: Plataforma Web privada diseñada para soluciones corporativas, que permite gestionar documentos y procesos de firma electrónica avanzada y simple de forma directa, con o sin necesidad de integrar APIs.

A partir de los datos proporcionados en el formulario de Solicitud de Firma Electrónica Avanzada (datos del firmante), se habilita el acceso del solicitante a una de las plataformas virtuales de ECERT, dando así inicio al proceso de comprobación fehaciente de su identidad.

l) Paso 2: Ingresar la ClaveÚnica, provista por el registro civil y que de acuerdo con el artículo 1 del Decreto supremo 24 de 2019, del Ministerio de Economía, Fomento y Turismo reconoce este mecanismo de identificación digital, como medio de comprobación fehaciente de la identidad del solicitante de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la ley Nº19.799 además de la utilización de un mecanismo complementario digital, tal como se indica en el paso 4 siguiente.

m) Paso 3: Ingresar Número de documento asociado al Rut con el fin de comprobar que la persona tiene Cédula de identidad vigente, sin bloqueo, sin interdicción y se encuentra viva.

n) Paso 4: Responder el desafío de Preguntas personales. Se requiere responder correctamente al menos tres de cuatro preguntas para completar la Comprobación. Este paso corresponde a la utilización del mecanismo complementario digital de verificación fehaciente de identidad del solicitante, como lo exige el Decreto Supremo 24 de 2019, del Ministerio de Economía, Fomento y Turismo.

ECERT comprueba con terceros de confianza para la Comprobación fehaciente de identidad como el Registro Civil y Bureaus:

a) Registro civil: se obtiene el Servicio ClaveÚnica. Adicionalmente, utiliza el servicio que verifica la correspondencia entre el número de RUT y el número de documento,

así como la validez de la Cédula de Identidad, asegurando que esté vigente, no bloqueada y que la persona no figure como fallecido ni interdicto.

b) Bureaus: se utiliza en el servicio de desafío de preguntas, el cual cuenta con modelos de robustez documentados en los archivos 'Modelo de Fiabilidad – Desafío de Pregunta' SGI-F-104-0014 y SGI-F-104-0015, ambos tienen un 99,2% de fiabilidad. Adicionalmente, si ECERT lo requiere, se podrá utilizar el servicio que verifique la correspondencia entre el número de RUT y el número de documento, así como la validez de la Cédula de Identidad, asegurando que esté vigente, no bloqueada y que la persona no figure como fallecido o interdicto.

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

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

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 del punto 4.2.1 de estas "CPS de ECERT" con las modalidades:

a) Presencial
b) Presencial ClaveÚnica.

4.3 Emisión y entrega del Certificado

Si el proceso de Comprobación Fehaciente de identidad es exitoso la Autoridad de Registro confirmara a la Autoridad de Certificación proceder con la emisión del certificado de firma electrónica avanzada.

Los Certificados estarán 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.

ECERT informará oficialmente al Titular del certificado que su certificado digital ha sido emitido y está listo para ser utilizado. Esta notificación puede realizarse mediante un correo electrónico enviado al titular o envío de mensaje en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

4.3.1 Emisión del Certificado

ECERT dispone de dos modalidades para el almacenamiento de certificados de firma electrónica avanzada.

4.3.1.1 Emisión del certificado para almacenamiento en dispositivo e-token:

Si el solicitante del certificado elige almacenar su certificado de firma en un dispositivo e-token, el proceso de comprobación fehaciente de identidad debe realizarse conforme a lo descrito en el punto 4.2.1 de este documento, y debe completarse dentro del mismo ciclo temporal (misma instancia) en el que se emite y almacena el certificado en el e-token.

Los pasos a seguir para realizar el proceso de emisión y descarga del certificado de firma en el e-token son:

a) Validación técnica preliminar: Se deben validar las condiciones técnicas del computador y dispositivo e-token del solicitante. Para el caso del dispositivo e-token se pueden dar 2 casuísticas, el solicitante:
   i. Compra un nuevo e-token a ecert: Los e-token son dispositivos criptográficos USB portables para la generación y almacenamiento de los datos de creación de firma de un certificado. Los e-token que utiliza ECERT cumplen con la norma FIPs-140-2 Nivel 3 y corresponde a los modelos SafeNet eToken 5110 o SafeNet eToken 5110+.
   ii. Cuenta con un e-token: ECERT verifica que el e-token corresponda al modelo SafeNet eToken 5110 o SafeNet eToken 5110+, en caso de que no corresponda a estos modelos se le indicara al solicitante que debe adquirir un e-token que cumpla con las características indicadas. La autoridad de registro obtendrá como

evidencia la imagen del modelo de e-token y el FIPs-140-2 Nivel 3 para asegurar el cumplimiento de esta condición.

b) Descarga del Certificado: ECERT envía al correo electrónico entregado por el titular la siguiente información:
   i. Link de descarga: https://pki.ecertchile.cl/Certificacion/Descargar.aspx
   ii. Usuario y contraseña para la descarga del certificado.

c) Creación de claves del certificado: Concluida la descarga del certificado en el dispositivo e-token, el titular debe realizar la creación de la clave privada del certificado. Quedando así, en poder del Titular los datos de creación de firma. ECERT no mantiene copia de los datos de creación de firma, una vez que estos hayan sido modificados por el Titular, en cumplimiento con el Artículo 31 Decreto Supremo 181, Reglamento de Ley 19.799.

d) Entrega del certificado: una vez concluido el proceso de creación de claves privadas por parte del titular, se concreta la entrega del certificado de firma. Adicionalmente la autoridad de registro notifica al titular la emisión del certificado enviando al correo electrónico declarado por el titular para la generación del certificado, el acta de entrega y recepción conforme de certificado de firma electrónica avanzada.

Consideraciones adicionales:

Ya sea que el proceso de Comprobación fehaciente de identidad se realice de manera Presencial o Presencial ClaveÚnica, ECERT disponibiliza el servicio de Asistencia técnica para la emisión y descarga del certificado en el dispositivo e-token a través de un Operador de Registro. Esta asistencia técnica no constituye ni reemplaza la Comprobación Fehaciente de identidad, corresponde a un servicio que ECERT proporciona a las personas que adquieren un certificado de firma.

Esta asistencia se realiza en un entorno seguro, de acuerdo con las políticas de seguridad de la información de ECERT, por tanto, se aplican los procedimientos de control de acceso lógico, a través de red segura (VPN, red wifi provista por ECERT).

En caso de que el solicitante compre un dispositivo e-token y necesite que este sea enviado a su domicilio, ECERT provee el servicio de despacho a domicilio con un costo adicional, el cual es comunicado en la página web de nuestra empresa. En tal caso, el proceso de Comprobación fehaciente de identidad (Presencial o Presencial ClaveÚnica), emisión y descarga del certificado de firma solo se puede llevar a cabo cuando el solicitante cuenta con el dispositivo en su poder.

4.3.1.2 Emisión y Uso del certificado para almacenamiento en Modulo Criptográfico Masivo de ECERT:

Si el solicitante del certificado opta por almacenar y utilizar su certificado de firma electrónica avanzada a través de un dispositivo criptográfico masivo, deberá seguir los siguientes pasos:

a) Almacenaje del certificado de firma

A través de la plataforma utilizada para la Comprobación Fehaciente de Identidad, el Titular ingresa la clave privada de su certificado, generada con los datos que él mismo ha proporcionado. Desde ese momento, dichos datos quedan bajo el exclusivo control del Titular.

ECERT no conserva copia de esta información, en cumplimiento con lo establecido en el artículo 5° del Decreto Supremo N° 24 de 2019 del Ministerio de Economía, Fomento y Turismo.

b) Uso del certificado de Firma

Para hacer uso del certificado de firma, el Titular deberá utilizar su clave privada, la cual es personal e intransferible. Además, deberá autenticarse mediante un segundo factor de seguridad por lo que ECERT ha puesto las siguientes alternativas para su envío.

i. Clave dinámica (PIN) enviada al correo electrónico informado por el Titular.
ii. Clave dinámica (PIN) enviada al número de teléfono informado por el Titular.
iii. Usuario y contraseña de la plataforma mediante la cual se utiliza el certificado.

4.3.2 Notificación de la emisión al Titular.

ECERT informará oficialmente al titular del certificado que su certificado de firma ha sido emitido y está disponible para su uso. Esta notificación se puede realizar a través de correo electrónico al titular o envío de mensajes en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

4.3.3 Periodo de Vigencia y Expiración del Certificado de Titular

Los certificados emitidos por ECERT pueden tener las siguientes vigencias:

a) 30 días.
b) 1, 2 o 3 años.

La vigencia de los certificados comienza en el momento específico indicado como inicio de vigencia. De acuerdo con el artículo 16 de la Ley 19799, la vigencia del certificado concluye por:

a) Término del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión.
b) Revocación del certificado. Las circunstancias en las cuales se realiza la revocación de un certificado de firma electrónica avanzada se especifican en el punto 4.9.1 de estas “CPS de ECERT”.

Para los certificados con vigencia de 30 días, el Titular en la aceptación del “contrato adhesión titular”, solicita expresamente revocar el certificado utilizado.

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.

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 Responsabilidades

ECERT es responsable de todo el ciclo de vida de los certificados de firma electrónica avanzada que emite, con independencia de si el certificado de firma electrónica avanzada fue adquirido a través de la red de sucursales de ECERT, sus Autoridades de Registro, sus plataformas propias (Pagina web, GRUP y Portal Empresa), o a través de un partner con el que mantenga convenio de comercialización vigente.

Las responsabilidades de los participantes se declaran a continuación:

4.4.3.1 ECERT (AC)

Sin perjuicio de las demás obligaciones legales y de esta “CPS de ECERT” y de la “CP de ECERT”, ECERT es especialmente responsable de:

a) Emitir los certificados cumpliendo todas las exigencias establecidas en estas "CPS de ECERT” y "CP de ECERT”, de conformidad con la información proporcionada por el Titular.
b) Asegurarse de que el certificado no contenga errores de transcripción de los datos proporcionados por el Titular durante el proceso de solicitud del certificado.
c) Garantizar que la información incluida o incorporada por referencia en el certificado sea exacta.
d) Publicar el certificado en el registro de acceso público de certificados.
e) Aplicar correctamente todos los procedimientos empleados.
f) 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.

4.4.3.2 Autoridad de Registro (AR)

Se obliga a:

o) Comprobar fehacientemente la identidad del solicitante en el otorgamiento de certificados de firma electrónica avanzada en concordancia con el artículo 12°, letra e) de la ley 19.799. y de acuerdo con los procedimientos establecidos en esta “CPS de ECERT” y en las “CP de ECERT”.

p) Obtener la aceptación del contrato de adhesión del Titular.

q) Aprobar o rechazar las solicitudes de certificados, directamente o a través de sus Autoridades de Registro, conforme a estas "CPS de ECERT”.

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

s) 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. En cumplimiento con el artículo 11, Decreto Supremo 181, Reglamento de Ley 19.799)

t) Recibir las solicitudes de revocación y suspensión de certificados de firma electrónica avanzada e informarlas a ECERT.

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

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

4.4.3.3 Titular

El Titular es responsable de:

a) Proveer información necesaria e inequívoca para la generación del certificado digital (nombre, Rut, correo electrónico) cualquier error en la información proporcionado será responsabilidad exclusiva del Titular.

b) Aceptar el certificado de acuerdo con el punto 4.4 de esta “CPS de ECERT”.

c) Aceptar el Contrato adhesión del Titular.

d) 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.

e) 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.

f) 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.

g) Usar el certificado de firma para los fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, la "CP de ECERT" y en las "CPS de ECERT".

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

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

j) 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.

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

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

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

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

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

p) 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, de acuerdo con el artículo 2314 de Código Civil Chileno.

q) Almacenar los documentos firmados es responsabilidad del Titular, excluyendo de esta responsabilidad a ECERT.

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

4.4.3.4 Partes que Confían

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

a) Comprobar la validez del certificado consultando el registro de acceso público de certificados disponible permanentemente en https://www.ecertla.com/verifica-vigencia-de-certificado/ o utilizar las herramientas que ECERT ha especificado en las tablas 3 y 4 del punto 7.1.2 de estas “CPS de ECERT”.

b) Comprobar la autenticidad de la firma del Titular.

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

d) Verificar que el uso que se le está dando al certificado sea acorde con los propósitos autorizados por la ley 19.799, esta "CP de ECERT” y las "CPS 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, de acuerdo con el artículo 2314 de Código Civil Chileno.

f) 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.

4.5 Usos de pares de claves y certificados

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

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

El Titular debe dejar de utilizar la clave privada tras el termino de vigencia, suspensión o revocación del certificado.

El Titular se obliga a:

a) Emplear el certificado de acuerdo con lo establecido en este documento.
b) Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta “CPS de ECERT”.
c) Comunicar a ECERT sin retrasos injustificables:
    i. La pérdida, el robo o el compromiso potencial de su clave privada.
    ii. La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
    iii. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el Titular.
d) El Titular debe dejar de utilizar la clave privada tras el termino de vigencia, suspensión o revocación del certificado.
e) 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 la "CPS de ECERT" y "CP de ECERT". Además, ECERT informa al tercero que confía en certificados que este debe asumir las siguientes responsabilidades:

a) Disponer de suficiente información para tomar una decisión informada sobre si confiar o no en el certificado.
b) Ser el único responsable de decidir confiar o no en la información contenida en el certificado.
c) Asumir toda la responsabilidad en caso de incumplir con sus obligaciones como parte que confía en el certificado.

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

ECERT hará todos los esfuerzos razonables para notificar al Titular por correo electrónico cuando su certificado esté por terminar su vigencia. Esta notificación se enviará a la dirección de correo electrónico registrada en el certificado de firma electrónica avanzada que se requiere renovar.

En el caso de los certificados obtenidos para Titulares a través de clientes empresas, se harán los esfuerzos razonables para enviar una notificación a ella con el fin de alertar dicha situación.

En el caso de certificados obtenidos por Titulares a través de empresas clientes, se realizarán esfuerzos razonables para notificar a la empresa correspondiente en caso de renovación, con el fin de mantenerla debidamente informada.

Es importante recordar que esta notificación es un servicio adicional para facilitar el proceso, pero ECERT no asume responsabilidad por su envío. Por lo tanto, es fundamental que el

Titular esté atento a la fecha de termino de vigencia de su certificado para evitar cualquier interrupción en su uso.

4.6.1 Circunstancias para la renovación del certificado

Los certificados vigentes pueden renovarse mediante el procedimiento especificado en el punto 4.6.3 de estas "CPS de ECERT". Sin embargo, un certificado no puede renovarse después de su termino de vigencia. En tal caso, el Titular deberá solicitar un nuevo certificado y completar todos los procedimientos especificados en el punto 4 de esta "CPS de ECERT".

4.6.2 Quién puede solicitar la renovación

La solicitud de renovación solo puede ser realizada por el Titular del certificado de firma electrónica avanzada.

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. Existen dos formas de proceder frente al requerimiento dependiendo si el Titular:

a) Tiene un certificado de firma electrónica avanzada vigente: El Titular podrá solicitar otro certificado, firmando la solicitud de renovación con el Certificado que aún se encuentra vigente, sin necesidad de realizar todo el proceso descrito en el punto 4 de estas "CPS de ECERT".
b) No tiene certificado de firma electrónica avanzada vigente. Es necesario realizar todo el proceso descrito en el punto 4 de estas "CPS e ECERT" como si el solicitante nunca hubiere tenido un certificado de firma electrónica avanzada.

4.6.4 Notificación de la emisión del nuevo certificado al Titular

ECERT informará oficialmente al titular del certificado que su certificado de firma ha sido emitido y está disponible para su uso. Esta notificación se puede realizar a través del correo

electrónico al titular o envío de mensajes en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

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 “CPS de ECERT”.

4.6.6 Publicación del certificado de renovación 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.

4.7 Cambio de clave del certificado

4.7.1 Circunstancias para la renovación de la clave del certificado

No aplica dado que la "Clave" del certificado es de absoluto control del titular.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

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

4.7.3 Procesamiento de solicitudes de renovación de claves de certificado

No aplica dado que la "Clave" del certificado es de absoluto control del titular.

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 “CPS 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 “CPS de ECERT”.

4.7.6 Publicación del certificado renovado en la CA

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

4.8 Modificación del certificado

4.8.1 Circunstancias para la modificación del certificado

No aplica. La modificación de certificado se considerará como una nueva emisión de certificado con la correspondiente Comprobación fehaciente de identidad y de acuerdo con lo establecido en los puntos 4.1 al 4.5 de esta “CPS de ECERT”.

4.8.2 Quién puede solicitar la modificación del certificado

No aplica. La modificación de certificado se considerará como una nueva emisión de certificado con la correspondiente Comprobación fehaciente de identidad y de acuerdo con lo establecido en los puntos 4.1 al 4.5 de esta “CPS de ECERT”.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica. La modificación de certificado se considerará como una nueva emisión de certificado con la correspondiente Comprobación fehaciente de identidad y de acuerdo con lo establecido en los puntos 4.1 al 4.5 de esta “CPS de ECERT”.

4.8.4 Notificación de la emisión de un nuevo certificado al Titular

ECERT informará oficialmente al titular del certificado que su certificado de firma ha sido emitido y está disponible para su uso. Esta notificación se puede realizar a través de correo electrónico dirigido al titular o envío de mensajes en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

4.8.5 Conducta que constituye aceptación de un certificado modificado

No aplica. La modificación de certificado se considerará como una nueva emisión de certificado con la correspondiente Comprobación fehaciente de identidad y de acuerdo con lo establecido en los puntos 4.1 al 4.5 de esta "CPS de ECERT".

4.8.6 Publicación del certificado modificado por la CA

No aplica. La modificación de certificado se considerará como una nueva emisión de certificado con la correspondiente Comprobación fehaciente de identidad y de acuerdo con lo establecido en los puntos 4.1 al 4.5 de esta "CPS de ECERT".

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.

De acuerdo con el Artículo 34 del Decreto Supremo 181, Reglamento de Ley 19.799, la revocación tendrá lugar cuando ECERT constate alguna de las siguientes circunstancias:

a) Solicitud del titular del certificado.
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.
e) Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
f) Que el titular del certificado no ha actualizado sus datos al cambiar éstos.

g) Las demás causas que convengan el prestador de servicios de certificación con el titular del certificado.

Según lo estipulado en el artículo 24 de la ley 19.799, los puntos d, e y f corresponden a un incumplimiento de las obligaciones del Titular.

ECERT en cumplimiento con el artículo 16 de la ley 19.799, comunicara al Titular la causa del incumplimiento y la fecha en la que se efectuara la revocación. La comunicación se realizará mediante correo electrónico a la dirección declarada por el titular para la generación del certificado de firma electrónica avanzada.

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 detecta algunos de los casos mencionados en el punto 4.9.1 de esta "CPS de ECERT" o de acuerdo con la solicitud de los tribunales de justicia.

4.9.3 Procedimiento para la solicitud de revocación

El Titular que solicite una revocación de su certificado de firma electrónica avanzada debe comparecer personal y directamente ante una de las Autoridades de Registro de ECERT o comparecencia presencial en alguna de las plataformas virtuales de ECERT. En ambos casos, se llevará a cabo el proceso de identificación y autenticación del solicitante para verificar que efectivamente sea el titular del certificado. ECERT ofrece las siguientes modalidades para realizar este procedimiento:

4.9.3.1 Presencial:

a) Paso 1: Presentar Cédula de Identidad vigente con perfecto estado de los elementos que permiten la lectura biométrica.
b) Paso 2: Colocar su huella dactilar en los dispositivos habilitados especialmente para la comprobación de la identidad. ECERT valida la identidad a través de un pareo entre la información biométrica de la cédula de identidad y la huella dactilar del solicitante, proceso Match on card.

c) Paso 3: En caso de que el Titular sea un Notario, Conservador, Registrador de Comercio o Archivero Judicial, Titulares suplentes o interinos, adicionalmente deberán presentar una copia del Aviso de Extravío dado a la Corte de Apelaciones respectiva, en los términos exigidos por el Auto Acordado sobre Uso de Documento y Firma Electrónica por Notarios, Conservadores y Archiveros Judiciales de 2006. La Autoridad de Registro conservará una copia de este aviso de extravío.

ECERT conservará registro de las solicitudes de revocación que generen los titulares conservando la Solicitud Revocación firmada por el titular en sus sistemas de gestión internos.

En caso de fallo del sistema biométrico, el Titular deberá comenzar un nuevo proceso de Comprobación de identidad y la Autoridad de Registro solicitará la siguiente información al Titular:

w) Paso 1: Presentar Cédula de Identidad vigente con perfecto estado físico, no debe estar quebrada, rayada, doblada y debe ser visualmente legible.

x) Paso 2: La Autoridad de Registro genera “Formulario Solicitud Revocación” el cual contiene:

   i. Nombre completo del Solicitante
   ii. Rut
   iii. Numero de documento asociado al rut
   iv. Correo electrónico
   v. Imagen del CI por ambos lados
   vi. Fotografía del Titular
   vii. Huella dactilar del Titular.
   viii. Fecha solicitud Revocación
   ix. Firma con puño y letra del Titular.

y) Paso 3: En caso de que el Titular sea un Notario, Conservador, Registrador de Comercio o Archivero Judicial, Titulares suplentes o interinos, adicionalmente deberán presentar una copia del Aviso de Extravío dado a la Corte de Apelaciones

respectiva, en los términos exigidos por el Auto Acordado sobre Uso de Documento y Firma Electrónica por Notarios, Conservadores y Archiveros Judiciales de 2006. La Autoridad de Registro conservará una copia de este aviso de extravío.

ECERT conservará registro de las solicitudes de revocación que generen los titulares conservando el "Formulario Solicitud Revocación" en sus sistemas de gestión internos.

4.9.3.2 Presencial ClaveÚnica:

z) Paso 1: comparecer presencialmente en alguna de las plataformas virtuales de ECERT las cuales pueden ser:
   i. Página Web www.ecertla.com: Plataforma Web pública de ECERT donde cualquier persona puede consultar información institucional, servicios y canales de contacto.
   ii. GRUP www.migrup.cl: Plataforma Web privada orientada a personas naturales, que permite firmar documentos de manera ilimitada con firma electrónica avanzada y enviar documentos a terceros mediante firmas prepagadas, incluso si ellos no cuentan con firma electrónica.
   iii. Portal Empresa https://portalempresa.ecertchile.cl: Plataforma Web privada diseñada para soluciones corporativas, que permite gestionar documentos y procesos de firma electrónica avanzada y simple de forma directa, con o sin necesidad de integrar APIs.

aa) Paso 2: Ingresar Rut

bb) Paso 3: Ingresar la ClaveÚnica, provista por el registro civil, la cual es personal e intransferible, por lo que la solicitud de revocación por cualquiera de las plataformas virtuales mencionadas, la realiza directamente el Titular dueño del certificado.

Para los certificados con vigencia de 30 días, el Titular en la aceptación del "contrato adhesión titular", solicita expresamente revocar el certificado utilizado.

ECERT conservará el registro de las solicitudes de revocación que generen los titulares en sus sistemas de gestión internos.

Para los puntos 4.9.3.1 y 4.9.3.2 ECERT notificará oficialmente al titular del certificado que su certificado de firma ha sido revocado, esta notificación se puede realizar a través de correo electrónico al titular o envío de mensajes en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

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 máximo de 24 horas hábiles, de lunes a viernes de 9:00 a 18:00.

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

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

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 asegura una disponibilidad del sitio no menor al 99%.

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.

4.9.12 Requisitos especiales en materia de compromiso de claves

El compromiso de la clave privada de la CA será notificado a los participantes de los servicios de certificación de acuerdo con el Plan de continuidad de negocio (MI-FEA-0046).

4.9.13 Circunstancias 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 haya cumplido su periodo de vigencia.

4.9.14 Quién puede solicitar la suspensión

De acuerdo con el artículo 33 Decreto Supremo 181, Reglamento de Ley 19.799, procederá la suspensión de la vigencia del certificado de firma electrónica avanzada cuando se verifique alguna de las siguientes circunstancias:

a) Solicitud del Titular del certificado.
b) Decisión del prestador de servicios de certificación (ECERT) en virtud de razones técnicas.

4.9.15 Procedimiento para solicitud de suspensión

El procedimiento para la suspensión dependerá de quien solicita la Suspensión:

a) Decisión de ECERT en virtud de Razones Técnicas: ECERT, comunicará al Titular del certificado de firma electrónica avanzada mediante correo electrónico a la casilla informada por éste al momento de la generación del certificado, indicando la causa y el momento que se hará efectiva la suspensión de acuerdo con el artículo 16 de la Ley 19.799. El Titular y la Parte que Confía debe verificar el estado del certificado en el cual desea confiar, y podrán hacerlo a través del sitio web de ECERT y también mediante un servicio OCSP.
b) Solicitado por el Titular del certificado: Para procesar una solicitud de suspensión, ECERT confirma que la persona solicitante de la suspensión sea realmente el Titular del certificado y para ello se puede realizar mediante las siguientes opciones:
cc) Notificación enviada por el Titular a la Autoridad de Registro de ECERT mediante firma electrónica avanzada.
dd) Comparecencia presencial ante algunas de Autoridad de Registro de ECERT, donde se llevará a cabo la Comprobación de identidad del Solicitante de la suspensión mediante firma electrónica avanzada.

ee) Contacto de acuerdo con lo indicado en el punto 1.5.2 de estas “CP de ECERT” donde será derivado a la autoridad de registro, quien utilizará la Modalidad Presencial ClaveÚnica descrita en el punto 4.2.1 para realizar la Comprobación fehaciente de identidad.

ECERT conservará el registro de las solicitudes de suspensión que generen los titulares en sus sistemas de gestión internos.

ECERT notificará oficialmente al titular del certificado que su certificado de firma ha sido suspendido, esta notificación se puede realizar a través de correo electrónico al titular o envío de mensajes en el sistema de la Autoridad de Certificación hacia el titular del certificado de firma.

4.9.16 Límites del periodo de suspensión

De acuerdo con el artículo 33 Decreto Supremo 181, Reglamento de Ley 19.799, la suspensión del certificado terminará por cualquiera de las siguientes causas:

a) Por la decisión ECERT de revocar el certificado, en los casos previstos en la Ley.
b) Por la decisión ECERT de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.
c) Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

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

4.10.1 Características 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.

4.10.2 Disponibilidad del servicio

ECERT se compromete a mantener los Servicios de Estado de Certificados disponibles en todo momento. Salvo en interrupciones programadas donde ECERT asegura una disponibilidad del sitio no menor al 99%.

4.10.3 Características opcionales

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

4.11 Terminación del Contrato

El contrato del servicio finalizará cuando se cumpla el termino 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.

4.12.1 Política 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

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 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.

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

No aplica.

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 (PO-GER-0003) 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 fehaciente 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.

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.

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 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.

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, suspensión 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 privada de la Autoridad de Certificación.

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 2 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.

5.4.6 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. En caso de que el evento registrado corresponda a un incidente y este afecta las condiciones de acreditación de ECERT será informado a la entidad Acreditadora de acuerdo con el Plan de continuidad de negocio (MI-FEA-0046).

5.4.7 Evaluaciones de vulnerabilidad

ECERT cuenta con una política de gestión de vulnerabilidades técnicas (PO-GSI-0017), 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:

a) Información de Titular de Certificados.
b) Documentación de apoyo de solicitudes de Certificados.
c) 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 2 y 6 años, dependiendo del tipo de información registrada, en concordancia con lo establecido en el punto 5.4.3 de estas “CP de ECERT”

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 las Política General de Seguridad de la Información (PO-GER-0003) y 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.

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 Política y plan de Continuidad de Negocios (PO-GER-0007) y (MI-FEA-0046) 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 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.

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 OCSP y CRL) conforme al Plan de continuidad de negocio (MI-FEA-

0046) existente, asegurando la recuperación de las operaciones normales dentro de las 24 horas siguientes al desastre, salvo en interrupciones programadas donde ECERT asegura una disponibilidad del sitio no menor al 99%. 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 (MI-FEA-0046).

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

6.1 Generación e instalación de pares de claves

6.1.1 Generación de pares de claves

La generación de las llaves criptográficas de Root y CA de ECERT 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).

En el caso del Titular, para la generación del par de claves pública y privadas se utiliza un software criptográfico, la clave privada es generada por el mismo usuario.

6.1.2 Entrega de claves privadas al Titular

Los datos de creación de firma asociados a los certificados de firma siempre son generados por un mecanismo que se encuentra bajo el exclusivo control del Titular, sea porque se creen y almacenen en un dispositivo criptográfico que te permite guardar y transportar sus datos personales al Titular o en un dispositivo criptográfico masivo custodiado por ECERT.

6.1.3 Entrega de claves pública al emisor del certificado

El método de envío de la clave pública a la Autoridad de Certificación es PKCS#11, otra prueba criptográfica equivalente o cualquier otro método aprobado por ECERT.

6.1.4 Entrega de clave pública de CA a partes confiables

Los certificados de CA raíz y de CA intermedias se distribuyen a las partes que confían mediante la publicación en la página web de ECERT.

6.1.5 Tamaños de claves

- La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits
- La longitud de las claves de las Autoridad de Certificación subordinadas es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de, mínimo, 2048 bits
- El algoritmo de hash de firma digital es SHA-256.

6.1.6 Generación de parámetros de clave pública y control de calidad

La clave pública de la CA raíz, subordinadas y de los certificados de los Titulares está codificada de acuerdo con RFC 5280.

6.1.7 Fines de uso de la clave (según el campo de uso de clave X.509 V3)

Estos fines de uso se especifican en el campo “Uso de la clave” del certificado, lo que ayuda a determinar cómo se debe usar la clave asociada, por ejemplo: Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0).

6.2 Protección de claves privadas e ingeniería de módulos criptográficos

6.2.1 Estándares y controles del módulo criptográfico

En relación con los módulos que gestionan claves de ECERT y de los Titulares de certificados de firma electrónica avanzada, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2 Control multi-persona de clave privada (n de m)

Se requiere un control multi-persona para activar la clave privada de la AC. Se establece que un mínimo de tres partes separadas es necesario para respaldar o recuperar la clave privada de la CA.

6.2.3 Depósito de clave privada

El depósito de las claves privadas esta declarado en el “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050), el que es de uso confidencial de ECERT.

6.2.4 Copia de seguridad de la clave privada

ECERT realiza copias de respaldo de las claves privadas de las CAs para asegurar su recuperación en caso de desastre, pérdida o deterioro. El procedimiento de respaldo de las claves privadas se encuentra declarado en el “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050), el que es de uso confidencial de ECERT.

6.2.5 Archivado de la clave privada

El archivado de claves privadas de la CA se realiza en base al “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050).

ECERT no mantiene copias de las llaves privadas del Titular.

6.2.6 Transferencia de la clave privada hacia o desde un módulo criptográfico

La transferencia de la clave privada hacia o desde un módulo criptográfico se refiere al proceso de mover una clave privada entre un entorno seguro, como un módulo de seguridad hardware (HSM), y un entorno menos seguro, como un servidor o un sistema de almacenamiento. Las claves privadas se generan directamente en los módulos criptográficos de producción de ECERT.

6.2.7 Almacenamiento de clave privada en el módulo criptográfico

Las llaves privadas de CAs son almacenadas de forma encriptada en módulos de hardware criptográfico.

6.2.8 Método de activación de la clave privada

El Método de activación de las claves privadas de la CA se realiza en base al “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050).

6.2.9 Método de desactivación de la clave privada

El Método de desactivación de las claves privadas de la CA se realiza en base al “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050).

6.2.10 Método de destrucción de la clave privada

El Método de destrucción de las claves privadas de la CA se realiza en base al “Plan de Administración de Llaves Criptográficas” (MI-FEA-0050).

6.2.11 Clasificación del módulo criptográfico

Ver punto 6.2.1. de este documento.

6.3 Otros aspectos de la gestión de pares de claves

6.3.1 Archivado de claves públicas

Este punto se describe en el punto 5.5.1 y 5.4.1 de esta “CPS de ECERT”.

6.3.2 Periodos operativos del certificado y periodos de uso del par de claves

Para el caso de Titular revisar el punto 4.3.3 de este documento.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de ECERT son generados de acuerdo con lo establecido en el punto 6.2.2 de esta “CP de ECERT” y los Procedimiento Ceremonia de Generación de Llaves Root CA-CA Intermedia FEA (PS03_DigDoc.gen.llaves) (MI-FEA-0146) y Procedimiento Ceremonia de Generación de Llaves - CA Intermedia - Firma Electrónica Avanzada (FAO2) (MI-FEA-0316).

6.4.2 Protección de datos de activación

Diríjase a los puntos 6.2.3, 6.2.4, 6.2.5 de estas “CPS de ECERT”.

6.4.3 Otros aspectos de los datos de activación

6.4.3.1 Transmisión de Datos de Activación

Revise el punto 6.2.6 de estas “CPS de ECERT”.

6.4.3.2 Destrucción de los Datos de Activación

Revise el punto 6.2.10 de estas “CPS de ECERT”.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

ECERT cuenta con una Política General de seguridad de la información (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.

6.5.2 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.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles del desarrollo del sistema

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

6.6.2 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.

6.6.3 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.

6.7 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

6.8 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 PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1 Perfil del certificado

Todos los certificados emitidos bajo esta Declaración de Prácticas de Certificación cumplen con el estándar X.509 versión 3 y con el Decreto Supremo 181 de 2002, del Ministerio de Economía, Fomento y Turismo. El contenido mínimo de los certificados es el siguiente:

Tabla 1: Perfil de Certificado de la política de firma de Firma Electrónica Avanzada SHA2 E-CERTCHILE CA FEA 02		
Versión	V3	
Número de serie	Valor único por DN Emisor	
Algoritmo de firma	sha256RSA	
Emisor	Correo electrónico	E=sclientes@e-certchile.cl
	Nombre	CN=E-CERTCHILE CA FEA 02
	Unidad Organizacional	OU=Autoridad Certificadora
	Organización	O=E-CERTCHILE
	Localidad (ciudad)	L=Santiago
	Estado (región)	S=Región Metropolitana
	País	C=CL
Valid desde	Nombre Dia, día, mes, año hh:m:ss	
Valid hasta	Nombre Dia, día, mes, año hh:m:ss	
Asunto	Correo electrónico	E = nombrecorreo@dominio.cl
	Nombre	CN = Nombre Apellido1 Apellido2 (si aplica)

	Unidad Organizacional	OU = Dato libre (no obligatorio)
	Organización	O = Organización declarada (ej. Ecert)
	Localidad (ciudad)	L = Localidad declarada (ej. Santiago)
	Estado (región)	S = Región geográfica Declarada (ej. RM)
	Pais	C = CL
Clave Publica	RSA (2048 Bits)	

Tabla 2: Perfil de Certificado de la Política de Firma Electrónica On-line (FAO) SHA2
E-CERTCHILE CA SERVICIO FIRMA AVANZADA ONLINE

Versión	V3	
Número de serie	Valor único por DN Emisor	
Algoritmo de firma	SHA256RSA	
Algoritmo hash de firma	SHA256	
Emisor	Correo electrónico	E = sclientes@e-certchile.cl
	Nombre	CN = E-CERTCHILE CA SERVICIO FIRMA AVANZADA ONLINE
	Unidad Organizacional	OU= Autoridad Certificadora
	Organización	O = E-CERTCHILE
	Localidad (ciudad)	L = Santiago
	Estado (región)	S = Región Metropolitana
	País	C = CL
Valid desde	Nombre Dia, día, mes, año hh:m:ss	

Valid hasta	Nombre Dia, día, mes, año hh:m:ss	
Asunto	Correo electrónico	E=nombrecorreo@dominio.cl
	Nombre	CN = nombre apellido1 apellido2 (si aplica)
	Unidad Organizacional	OU = RUT XXXXXXXX-X
	Organización	O = E-CERTCHILE
	Localidad (ciudad)	L = STGO
	Estado (región)	ST= STGO
	País	C = CL
Clave Publica	RSA (2048 Bits)	

7.1.1 Números de versión

Los certificados de CA serán Certificados X.509 versión 3.

7.1.2 Extensiones de certificado

Las extensiones de certificado son atributos adicionales que proporcionan información específica sobre el uso y las características de un certificado digital. Estas extensiones permiten personalizar y definir el comportamiento del certificado en diferentes contextos de seguridad.

Tabla 3: Extensiones de Perfil de Certificado de la Política de Firma Electrónica Avanzada SHA2	
Nombre alternativo del titular	Rut del Titular, 1.3.6.1.4.1.8321.1=RUT del Titular
Nombre alternativo del emisor	Rut de EC emisora, 1.3.6.1.4.1.8321.2=16 0a 39 36 39 32 38 31 38 30 2d 35

Punto de distribución CRL	URL=http://crl.ecertchile.cl/E-CERTCHILE CA FEA 02(1).crl (http://crl.ecertchile.cl/E- CERTCHILE%20CA%20FEA%2002(1).crl)
Acceso a la información de entidad emisora	URL= http://ocsps2.ecertchile.cl/ocsp
Directivas del certificado	Id. de certificador de directiva=CPS Certificador: https://www.e-certchile.cl
Directivas del certificado	[1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado Firma Certificado emitido para Firma Electrónica Avanzada. PSC acreditado por Resolución Administrativa Exenta Nro. 317 del 14 de agosto del 2003 de la Subsecretaria de Economía.
Uso de la clave	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)

Tabla 4: Extensiones de Perfil de Certificado de la Política de Firma Electrónica On-line (FAO) SHA2		
Nombre del Titular	E = correo electrónico del Titular CN = nombres apellido1 apellido2 OU = RUT 12345678-9 O = Nombre de la empresa L = Localidad S = Región C = País CL	
KeyUsage	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)	
ExtendedKeyUsage	N/A.	
AuthorityKeyIdentifier	KeyID= 8b37df370e5691ac005ca964401e3a58a44ff3fc	
Subject Key Identifier	KeyID=	
CertificatePolicy	[1] Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.8658.5 1,1] Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://www.e-certchile.cl/ 1,2] Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso= Certificado emitido para Firma Electrónica Avanzada. PSC acreditado por Resolución Administrativa Exenta Nro. 317 del 14 de agosto del 2003 de la Subsecretaria de Economía.	
IssuerAltName	RUT de EC emisora, OID: 1.3.6.1.4.1.8321.2	
SubjectAltName	RUT del Titular, OID: 1.3.6.1.4.1.8321.1	

CrlDistributionPoint	Dirección URL=http://crlfao.ecertchile.cl/ECERTCHILECAFAO.crl	
Acceso a la información de la entidad emisora	Dirección URL=http://ocspfao.ecertchile.cl/ocsp	

7.1.3 Identificadores de objetos de algoritmo

El identificador de objeto del algoritmo de firma es: sha256 RSA

El identificador de objeto del algoritmo de la clave pública es: RSA (4096) bits.

7.1.4 Forma de los nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente Declaración de Prácticas en el punto 3.1.1 de este documento.

7.1.5 Restricciones de nombre

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

7.1.6 Identificador de objeto de política de certificado

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1 de este documento.

7.1.7 Uso de la extensión restricciones de política

ECERT no ha establecido restricciones de políticas en las extensiones de certificado.

7.1.8 Sintaxis y semántica de los certificadores de políticas

ECERT emite certificados con la extensión "Directivas del certificado" que apuntan a la página web de ECERT y adicionalmente contiene el texto que comunica la identificación de la resolución de acreditación entregada por la Entidad Acreditadora para Firma Electrónica Avanzada.

7.1.9 Semántica de procesamiento para las políticas de certificación critica

No aplica.

7.2 Perfil CRL

Un perfil de CRL (Certificate Revocation List) es un conjunto de directrices y formatos que define cómo se debe estructurar y gestionar una lista de certificados revocados. Esta lista es crucial para la seguridad de los sistemas que utilizan certificados digitales.

Las CRL contienen información clave como:

Tabla 5: CRL de Firma Electrónica Avanzada SHA2	
Versión	V2
Algoritmo de Firma	sha256RSA
Emisor	E = sclientes@e-certchile.cl CN = E-CERTCHILE CA FEA 02 OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana C = CL

Fecha Efectiva	Fecha de emisión de la CRL. Las CRLs son efectivas desde la emisión.
Próxima actualización	Fecha en la que la próxima CRL será publicada. Frecuencia de emisión de la CRL está de acuerdo con el punto 4.9.7 de este documento
Lista de revocaciones	Lista de Certificados revocados, incluyendo el Número de Serie del Certificado revocado y la Fecha de Revocación.
Tabla 6: CRL de Firma Electrónica On-line (FAO) SHA2	
Versión	V2
Algoritmo de Firma	sha256RSA
Emisor	E=sclientes@e-certchile.cl CN=E-CERTCHILE CA SERVICIO FIRMA AVANZADA ONLINE OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana DC = domecert C = CL
Fecha Efectiva	Fecha de emisión de la CRL. Las CRLs son efectivas desde la emisión.
Próxima actualización	Fecha en la que la próxima CRL será publicada. Frecuencia de emisión de la CRL está de acuerdo con el punto 4.9.7 de este documento
Lista de revocaciones	Lista de Certificados revocados, incluyendo el Número de Serie del Certificado revocado y la Fecha de Revocación.

7.2.1 Números de versión

ECERT soporta CRLs X.509 Versión 2.

7.2.2 CRL y extensiones de entrada

Las "extensiones de entrada de CRL" se refieren a los campos adicionales que pueden incluirse en una CRL para proporcionar información adicional o funcionalidades extendidas. Algunas de las extensiones comunes que pueden encontrarse en una CRL incluyen:

a) Código de razón de la lista de revocación: Permite identificar el motivo de revocación.
b) Número CRL: Identifica de manera única cada lista de revocación emitida por una autoridad de certificación.
c) Próxima Actualización: Indica la fecha y hora en la que se emitirá la próxima CRL actualizada la que contará con nuevo número de CRL e incluirá aquellos certificados de firma electrónica avanzada que han sido revocados y suspendidos. Las Listas de Certificados Revocados (CRL) son emitidas y actualizadas por lo menos 1 vez cada 24 horas, de acuerdo con lo establecido en el punto 4.9.7 de esta "CPS de ECERT".

Estas extensiones mejoran la funcionalidad y la eficacia de las CRL, facilitando la administración y el uso de certificados digitales dentro de un entorno de PKI.

7.3 Perfil OCSP

El RFC 2560 establece el Protocolo de Estado de Certificados en Línea (OCSP), el cual permite verificar el estado de revocación de un certificado digital en línea. Este protocolo proporciona una alternativa al método convencional de verificación mediante listas de revocación (CRL).

7.3.1 Números de versión

De acuerdo con el RFC 2560, ECERT utiliza la OCSP versión 1.

7.3.2 Extensiones OCSP

ECERT utiliza la extensión "responder ID" dado que identifica de manera única al servidor OCSP que responde a la solicitud de estado de revocación del certificado. Esto es crucial porque permite a los clientes verificar la autenticidad de la respuesta recibida y asegurarse de que proviene de una fuente confiable y autorizada.

En resumen, la aplicación del "responder ID" en OCSP asegura la autenticidad y la integridad de las respuestas de estado de revocación de certificados digitales, proporcionando así confianza en la validez de los certificados utilizados en conexiones seguras como SSL/TLS.

8 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.

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 Comunicación de resultados

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

9 OTROS ASUNTOS COMERCIALES Y LEGALES

9.1 Tarifas

El Solicitante deberá pagar las tarifas correspondientes a los certificados solicitados, las cuales cubren exclusivamente todas las actividades que ECERT realiza para gestionar el ciclo de vida del certificado de firma electrónica avanzada contratado.

Las tarifas para personas naturales se encuentran permanentemente publicadas y disponibles en www.ecertla.com/, en el menú “Productos”, opción “Ver todos los productos”.

La negativa posterior a aceptar un certificado por razones diferentes a errores o inexactitudes en el mismo, o su no utilización, no otorga al Titular el derecho a solicitar un reembolso. En consecuencia, según lo establecido en la letra b) del artículo 3 bis de la Ley 19.496 sobre derechos de los consumidores, el derecho de retracto no es aplicable, ya que los certificados son productos elaborados por Autoridad de Certificación de acuerdo con las especificaciones proporcionadas por el Titular (nombre, RUT y correo electrónico).

La tarifa asociada a la compra por volumen de certificados de firma electrónica avanzada por parte de una empresa o institución para sus clientes o colaboradores se acordará de manera individual en cada caso. Las condiciones específicas de dicha tarifa quedarán debidamente establecidas en el respectivo contrato, el cual reflejará los términos y acuerdos alcanzados entre las partes.

9.1.1 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.

9.1.2 Tarifas de acceso al certificado

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

9.1.3 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.

9.1.4 Tarifas por otros servicios

No aplica.

9.1.5 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.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

ECERT cumple con la normativa vigente y cuenta con un seguro de responsabilidad civil adecuado garantizando así una cobertura suficiente de su responsabilidad.

9.2.2 Otros activos

No aplica.

9.2.3 Cobertura de seguro o garantía para entidades finales

ECERT limita su responsabilidad al ejercicio de su actividad durante el ciclo de vida del certificado de firma electrónica avanzada 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 avanzada.

9.3 Confidencialidad de la información empresarial

9.3.1 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”.

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

La siguiente información se considera no confidencial:

a) La contenida en la presente “CPS de ECERT”.
b) La contenida en la Política de Certificación “CP 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”.

9.3.3 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.

9.4 Privacidad de la información personal

9.4.1 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”.

9.4.2 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.

9.4.3 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.

9.4.4 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.

9.4.5 Aviso y consentimiento para el uso de la información privada

A menos que se indique lo contrario en esta CPS, 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.

9.4.6 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.

9.4.7 Otras circunstancias de divulgación de información

No aplica.

9.5 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.

9.6 Declaraciones y garantías

9.6.1 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 estas "CPS de ECERT" y "CP de ECERT".
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 "CPS de ECERT" y la "CP de ECERT".
f) Emitir los certificados en conformidad al procedimiento establecido en esta "CPS 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 Autoridad 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.

9.6.2 Declaraciones y garantías de RA

La Autoridad de Registro se compromete a:

a) Comprobar la identidad del solicitante de un certificado de firma electrónica avanzada, según el procedimiento establecido en esta “CPS ECERT” y en la “CP de ECERT”.

b) Obtener la aceptación del contrato del Titular parte del solicitante.

c) Aprobar o rechazar las solicitudes de certificados, directamente o a través de sus Entidades de Registro, conforme a las "CPS de ECERT” y "CP 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 avanzada 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 avanzada.

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

9.6.3 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 "CPS de ECERT" y la"CP 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.

9.6.4 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 CPS.

9.6.5 Declaraciones y garantías de otros participantes

No Aplica.

9.7 Renuncias de garantías

ECERT rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en los puntos 9.6.1 y 9.6.2.

9.8 Limitaciones de responsabilidad

ECERT limita su responsabilidad de acuerdo con los establecido en este documento en los puntos 4.4.3 y 9.2.1 de este documento.

9.9 Indemnizaciones

Aplica de acuerdo con lo establecido en la legislación vigente, 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, de acuerdo con el artículo 2314 de Código Civil Chileno.

9.10 Plazo y terminación

9.10.1 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 CPS debe entrar en vigencia a partir de la fecha en que se publica en www.ecertla.com.

9.10.2 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.ecertl a.com.

9.10.3 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 estas Declaración de Prácticas de Certificación continúen vigentes tras el término del servicio.

9.11 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 CPS.

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.

9.12 Enmiendas

9.12.1 Procedimiento de modificación

Cualquier nueva versión de estas “CPS de ECERT”, estará sujeta al procedimiento de aprobación indicados en el punto 1.5.4 y 9.12.2 de esta “CPS de ECERT”.

Una vez que se publique la nueva “CPS 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.

9.12.2 Mecanismo y plazo de notificación

ECERT se reserva el derecho de modificar esta “CPS 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 "CPS 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.

9.12.3 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 CPS.

9.13 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.

9.14 Ley Aplicable

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

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) Decreto N° 24 del 09 abril 2019, del Ministerio de Economía, Fomento y Turismo que reglamenta la Ley 19.799.

d) Normas técnicas dictadas de conformidad con el Decreto Supremo 181 de 2002, del Ministerio de Economía, Fomento y Turismo que reglamenta la Ley 19.799.

e) Declaración de Prácticas de Certificación de Firma Electrónica Avanzada de ECERT (PC-FEA-0001).

f) Políticas de Certificado de Firma electrónica avanzada (MI-FEA-0029) “CP de ECERT”

g) Otros documentos relacionados con la prestación de servicios de certificación.

9.15 Cumplimiento de la legislación aplicable

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

9.16 Disposiciones diversas

9.16.1 Acuerdo completo

Esta “CP ECERT” junto con la “CPS de ECERT” y el Contrato Adhesión Titular de Certificado constituye el acuerdo completo entre las partes y reemplaza cualquier acuerdo previo.

9.16.2 Cesión

No aplica.

9.16.3 Divisibilidad

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

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

No Aplica.

9.16.5 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 avanzada 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 "CPS 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 laboral del personal de ECERT o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

9.17 Otras disposiciones

No aplica.

10 CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
1	27-01-2021	Migración del documento a ISOEasy.
2	12-01-2022	Se modifica redacción y se actualizan apartados 3.1.1. 3.1.3.a y 3.1.3.b..
3	30-03-2022	Se actualiza documento con base a solicitud de Entidad Acreditadora y observaciones de auditor ISO 27001
4	23-06-2022	Corresponde a la revisión anual de preparación IAO 2022
5	24-10-2022	Se incluyen punto: 2.1.1 letra d. y 2.1.5 Obligaciones generales, párrafo 2 y 3.
6	31-01-2023	• Se incluyen modificaciones indicadas por Raul Arrieta en los puntos: • Información sobre comercialización y emisión de certificados de firma electrónica. • Procedimiento de Atención de Reclamos. Exclusión del derecho a retracto. • Se reemplaza la palabra e-certchile por ECERT.
7	27-08-2024	Revisión IAO 2023 Se actualiza formato y contenido. • 4.2.1.2 Modalidad Digital ClaveÚnica. • Se agrega nuevo modelo de Renovación de FEA. • Se agrega Suspensión de FEA. • Se incluye uso del Contrato Adhesión Titular de Certificado. • Se incluyen aclaraciones de acuerdo a IAO 2023. • Se reemplaza la frase: “Validación fehaciente de Identidad” por “Comprobación fehaciente de Identidad”.
8	14-08-2025	Mejoras redacción y otros: • Se actualiza página Web de e-certchile.cl a ecertla.com donde corresponda. • Se especifica URL página Web para ver Política y Prácticas, Vigencia certificado y CRL. • Corrección de “Digital ClaveÚnica” a “Presencial ClaveÚnica” • Inclusión del detalle sobre la fuente del nombre del titular que figura en el certificado de firma. • Redacción optimizada de los procedimientos de identificación y uso del certificado con segundo factor. • Revisión Anual IAO 2025

9	25-09-2025	Mejora en redacción por Aclaratoria IAO 2025: • El comprobante de solicitud de FEA podrá presentarse en físico, digital o validarse con RUT. • Se incorporan descripciones de plataformas ECERT • Se corrige URL portal empresa. • Se incorporan plazos de actualización o revisión de este documento. Se referencian los documentos que demuestran la robustez del modelo de desafío de preguntas.
10	07-01-2026	Mejora en redacción por Feedback IAO 2025: • En 4.2.1.1 Modalidad Presencial - Paso 1, se incorpora que la compra y solicitud del certificado FEA se realiza a través del sitio web de ECERT (www.ecertla.com).En el mismo Paso 1, se explicita que el solicitante debe presentar copia de aprobación de solicitud (impresa o digital) o, en su defecto, su cédula de identidad para iniciar/continuar el proceso de emisión. • En el punto 4.9.3.2 Paso 1), se incorpora la descripción operacional sobre el funcionamiento de las plataformas: www.ecertla.com, www.migrup.cl y Portal Empresa. • Se actualiza la URL de Portal Empresa a https://portalempresa.ecertchile.cl. • En el punto 9.10.1. se incorpora la periodicidad de revisión y actualización de estas Prácticas. • En el punto 1.5.4 se define la gobernanza de aprobación de estas Prácticas frente al Comité de Sistema de Gestión de ECERT. • En el punto 4.2.1.2. letra b) se referencian los documentos del modelo de fiabilidad del Desafío de Preguntas de los Bureaus y se expresa el porcentaje de fiabilidad. • Se actualiza en carátula de las practicas el propietario del proceso por Gerente de Cumplimiento y Consultoría.

Fin del documento