Política de Certificados (CP) Firma Electrónica Avanzada

VERSION 2.0.04

PSC
CERTINET
2022

Audiencia

Titulares/Usuarios, Profesionales de áreas de operaciones y tecnologías de Empresas que estén involucrados con la puesta en marcha u operación de la Aplicaciones que reciben objetos electrónicos firmados electrónicamente y público general participante del comercio electrónico, interesados en obtener confianza en la seguridad e interoperabilidad de estos Certificados.

Versión	Descripción	Fecha	Autor
2.0.01	Primer borrador de la Segunda versión del documento: Esta nueva CP se genera a partir de la versión 1.8 publicada vigente. Considera todos sus elementos, sin embargo modifica su estructura acorde a ETSI 102 042	10/01/2022	A. Carreño
2.0.02	Versión borrador final, para ser presentado a Autorización y Firma de la Gerencia General.	07/02/2022	A. Carreño
2.0.03	Revisión General por parte del nuevo Oficial de Seguridad	02/08/2022	I. Infante
2.0.04	Se incorpora Enrolamiento a Domicilio	30/06/2022	R. Riveros

1 Introducción

La Política de Certificados de Firma Electrónica Avanzada de CertiNet “CP-FEA CertiNet”, establece "lo que se debe cumplir" y la Declaración de Prácticas de Certificación, establece "el cómo se cumple", es decir, los procesos que utilizará para crear y mantener el certificado. Por tanto esta Política establece las directrices y reglas generales que se deben observar en el ciclo de vida de los certificados que se emitan bajo esta.

Esta Política se desarrolla conforme al Modelo de Certificación de CertiNet, que tiene como objetivo proveer servicios de certificación para Firma Electrónica Avanzada que permitan apoyar el desarrollo de negocios electrónicos de nuestros clientes considerado los aspectos legales, tecnológicos, comerciales y operacionales de un Modelo de Confianza incorporando los requisitos de la ley N° 19.799, su reglamento y los requisitos para Firma Electrónica Avanzada establecidos en la Guía de Acreditación de la Subsecretaría de Economía y Empresas de Menor Tamaño, mediante la aplicación de procedimientos y normas de nivel mundial, que CertiNet adopta como Autoridad Certificadora en la provisión de Servicios de Certificación.

CertiNet opera en base a una visión de evolución del Modelo de Confianza que incluye la operatividad de sus Certificados de Firma Electrónica Avanzada según lo expresado en la ley 19.799 y su reglamento decreto 181 de 2002, en la implementación de su plataforma de PKI bajo la CA Raíz CertiNet, para lo cual dispone una Política de Seguridad y Protección de datos acorde a este modelo.

1.1 Generalidades

1.1.1 Sobre la Política de Certificados

Esta Política de Certificados está definida, como un conjunto de reglas y directrices que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes según el estándar internacional “ISO/IEC 9594-8/ITU-T Recomendación RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

Esta CP-FEA CertiNet en conjunto con la CPS-FEA CertiNet, son los instrumentos que establecen las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, suspensión, traspaso y revocación de los certificados conforme a la ley 19.799, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados”, conforme a la ETSI TS 102 042 V1.1.1 (2002-04) según lo dispuesto en el Reglamento de Ley de Firma Electrónica, decreto 181 de 2002 y decreto 24 de 2019.

La explicación detallada de las prácticas que CertiNet emplea para emitir y gestionar los certificados se encuentra en la CPS-FEA CertiNet.

1.1.2 Alcance

Esta Política debe ser aplicada por la organización en todos sus Certificados de Firma Electrónica Avanzada y se encuentra disponible para los titulares/usuarios y terceras partes que decidan operar con dichos certificados.

1.2 Identificación

Nombre: CP-FEA CertiNet
O.I.D.: 1.3.6.1.4.1.52428.100
Descripción: Política de certificados (CP) de Firma Electrónica Avanzada de CertiNet S.A.
Versión: 2.0
Fecha de Emisión: 01 de Agosto del 2022
Ubicación: https://www.certinet.cl/acreditacion

CPS relacionada: Declaración de Prácticas de Certificación (CPS-FEA CertiNet)
Ubicación: https://www.certinet.cl/acreditacion

Detalle de Contacto:
Razón Social: CertiNet S.A.
Rut: 99.532.830-5
Representante Legal: Roberto Riveros Durán
Dirección Social: Huérfanos #1052 Piso 12, Santiago.

Esta política es administrada por el PSC CertiNet S.A., que puede ser contactado al e-mail: soporte@certinet.cl o bien www.certinet.cl, el servicio de atención a clientes, usuarios y Terceros, atiende mediante el mail indicado, bajo un esquema de "Ticket Jerarquizado de Servicio", por lo que el flujo de atención depende del motivo y urgencia de la consulta.

1.3 Comunidad y Aplicabilidad

Esta Política se aplica a todos los Certificados de Firma Electrónica Avanzada emitidos por CertiNet S.A. y establece las directrices generales y protocolos que se deben observar y cumplir de acuerdo a la normativa vigente a lo largo de todo el ciclo de vida de los certificados desde su emisión hasta su revocación, y se aplica a todos los Certificados de Firma Electrónica Avanzada emitidos por CertiNet.

Los Certificados de Firma Electrónica Avanzada emitidos bajo esta Política están dirigidos a satisfacer las necesidades de identificación y autenticación establecidas en la ley 19.799,

sobre firmas y documentos electrónicos y los servicios de certificación de estos. Tanto para titulares/usuarios como para las terceras partes que decidan libremente confiar en su cadena de confianza y tecnologías.

1.4 Entidades

1.4.1 Prestador de Servicios de Certificación (PSC)

Entendemos bajo la presente política al PSC como aquella entidad que presta servicios concretos relativos al ciclo de vida de los certificados.

CertiNet está constituido como Prestador de Servicios de Certificación de Firma Electrónica Avanzada de conformidad con la ley de la República de Chile Nº 19.799, sobre Documentos Electrónicos, Firma Electrónica Avanzada y Servicios de Certificación de dicha firma y su Reglamento, DS 181, del Ministerio de Economía, Fomento y Turismo, según da cuenta la R.A. Exenta No. 380, de 21 de Julio de 2006, de la Subsecretaría de Economía y Empresas de Menor Tamaño.

1.4.2 Autoridad de Certificación PSC CertiNet

Para efectos de esta política la Autoridad de Certificación es la entidad de confianza acreditada para prestar servicios de certificación electrónica avanzada responsable de emitir y revocar certificados de dicha naturaleza, de acuerdo con los requisitos legales establecidos en la ley 19.799, su reglamento, guías, normas y estándares técnicos contenidos en ellos.

1.4.3 Autoridad de Registro PSC CertiNet

CertiNet, para efectos de esta política define una Autoridad de Registro, como la entidad de apoyo que realiza el proceso de identificar fehacientemente la identidad del Titular/usuario de un Certificado de Firma Electrónica Avanzada, conforme a la ley 19.799, su reglamento y guías de procedimientos asociadas. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados y validados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado.

1.4.4 Solicitante

CertiNet, reconoce como Solicitante a toda “Persona”, natural o jurídica debidamente representada, que solicita para sí o para un tercero la emisión de un Certificado en conformidad a lo establecido en la CPS-FEA CertiNet y los procedimientos que la empresa tiene definidos para el registro de estas solicitudes.

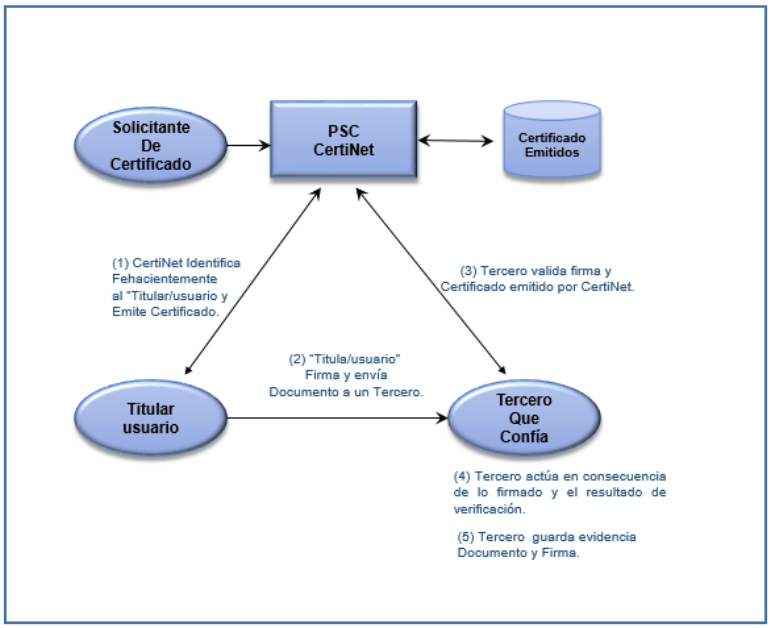
1.4.5 Titular/Usuario

Bajo esta Política el titular/usuario de un certificado es una persona natural o jurídica, con cédula de identidad o Rol Único Tributario, según sea el caso, chileno y vigente, que ha sido debidamente autenticada y que cumple con los requisitos legales para solicitar un certificado de firma electrónica avanzada que utiliza bajo su exclusivo control.

1.4.6 Tercero que Confía

Esta política reconoce como Tercero que Confía, a toda persona, natural o jurídica, que recibe información firmada a través de una Firma Electrónica Avanzada asociada a un certificado válidamente emitido por CertiNet, que busca confiar en la integridad y autenticidad de la información contenida con certeza de la identidad del firmante.
El "Tercero que Confía", Es responsable de validar el contenido del documento, la firma y el certificado asociado a dicha firma previo a confiar en él.

Esquemáticamente la interacción entre las entidades es:



1.5 Tipos y Usos del Certificado de Firma Electrónica Avanzada:

Certinet, declara que emite Certificados de Firma Electrónica Avanzada que cumplen con las directrices, normas y estándares, establecidos en la Ley 19.799, su reglamento y los requisitos contenidos en la Guía de Evaluación Procedimiento de Acreditación Prestador de Servicios de Certificación Firma Electrónica Avanzada versión 2.0. Ubicada en:

https://www.entidadacreditadora.gob.cl/marco-legal/

https://www.entidadacreditadora.gob.cl/normas-tecnicas/

https://www.entidadacreditadora.gob.cl/guias/

1.5.1 Tipos de Certificados:

Certinet emite Certificados de Firma Electrónica Avanzada a personas naturales solo después de haber verificado fehacientemente la identidad de un solicitante conforme a la Ley 19.799 y su reglamento, y con ello garantiza que el Titular/usuario de un Certificado de Firma Electrónica Avanzada no pueda "repudiar", la firma de un documento cualquiera.

1.5.2 Usos del Certificado:

El uso de los certificados de Firma Electrónica Avanzada y su información asociada está restringido a las condiciones de uso específicas descritas en este instrumento y en la Ley 19.799, y en particular, no pueden ser usados para certificar a otros individuos, empresas de ningún tipo u objetos.

En la CPS-FEA CertiNet; número 1.5.2, se encuentra descrito en detalle el:

- ✓ Uso Permitido de un Certificado
- ✓ Uso no Autorizado de un Certificado

2 Requerimientos Generales

2.1 Obligaciones

CertiNet, declara que en general toda entidad o personas que hagan uso directa o indirectamente de los servicios de nuestra empresa debe observar y cumplir con las obligaciones contenidas en la Ley 19.799, sobre firmas y documentos electrónicos, que se resumen, pero no se limitan a:

2.1.1 Autoridad Certificadora CertiNet

CertiNet como Autoridad Certificadora acreditada opera de acuerdo con las mejores prácticas internacionales siguiendo los estándares vigentes de modo que los certificados emitidos cumplen con las condiciones establecidas en la Ley 19.799, garantizando que su uso en las diferentes aplicaciones del mercado y leyes o reglamentos internacionales que operen bajo los estándares reconocidos por la industria, siendo compatible con normativas como eIDas, CSC y otras. Del mismo modo se obliga según lo dispuesto en la legislación normativa vigente, en lo detallado en la Declaración de Prácticas de Certificación de CertiNet para Firma Electrónica Avanzada (CPS-FEA CertiNet) numeral 2.1. Y lo descrito en esta política.

2.1.2 Autoridad de Registro

La Autoridad de Registro defina en los términos descritos en el punto 1.4.3 de esta política, es delegada por la Autoridad Certificadora del PSC CertiNet, para comprobar fehacientemente la identidad del solicitante de un Certificado de Firma Electrónica Avanzada antes de la emisión de dicho certificado y debe observa en todo momento los estándares, procedimientos y otras instrucciones que se emitan, siguiendo siempre las mejores prácticas de modo de garantizar el no repudio de una firma una vez emitido un certificado. Por lo tanto también se obliga en los términos definidos en detalle en la CPS-FEA CertiNet para la emisión de certificados de firma electrónica avanzada (numeral 2.1.2.).

2.1.3 Obligaciones del Solicitante

Un Solicitante, según lo define el numeral 1.4.4, se obliga a cumplir con todos los procedimientos y requisitos establecidos por CertiNet para poder comprobar fehacientemente la identidad de un titular de un Certificado de Firma Electrónica Avanzada conforme a la Ley 19.799 y su reglamento, estos se encuentran detallados en la CPS-FEA CertiNet, los que se resumen pero no se limitan a:

- ✓ Establecer una solicitud formal de emisión de certificado, en la que acepta los términos y condiciones descritos en esta Política y en la "CPS-FEA CertiNet"
- ✓ Comprobar y comunicar a CertiNet al momento de recibir su certificado cualquier error o inexactitud contenida en el Certificado.

2.1.4 Titular/Usuario

Esta política establece que todo titular/usuario de un Certificado de Firma Electrónica Avanzada; Según lo definido en el numeral 1.4.5 de esta. Y lo dispuesto en el artículo 24 de la Ley 19.799:

> *"Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando."*

Se obliga a entregar información fidedigna y legitima a la autoridad de registro delegada y cumplir con todos los requerimientos solicitados por la Autoridad de Certificadora CertiNet, consecuentemente también se obliga a:

- ✓ No revelar ni compartir por ningún medio la contraseña creada bajo su exclusivo control y que da acceso tanto a los dispositivos de almacenamiento (HSM o Token) y al certificado de firma electrónica avanzada.
- ✓ Custodiar la contraseña tomando todas las precauciones a su alcance para evitar su pérdida o uso no autorizado
- ✓ Hacer uso de su certificado solo para los fines autorizados por CertiNet.

Una descripción detallada respecto a cómo se realiza esto, se encuentra en el numeral 2.1.4 de la Declaración de Prácticas de Certificación (CPS-FEA CertiNet)

2.1.5 Obligaciones del "Tercero que Confía"

Los terceros definidos en el numeral 1.4.6, que deciden confiar en la cadena de confianza de los Certificados de Firma Electrónica Avanzada emitidos por CertiNet, se obligan en forma previa a:

- ✓ Verificar la validez del certificado mediante consulta al registro de certificados
- ✓ Verificar la firma del titular del certificado.
- ✓ Comprobar las restricciones de uso que figuren en el certificado y la CPS-FEA CertiNet

Lo anterior se puede realizar en https://www.certinet.cl/acreditacion

2.1.6 Obligación General

Titulares/Usuarios, Terceros que Confían y en general toda entidad o personas que hagan uso directa o indirectamente de los servicios de CertiNet. Declaran conocer, aceptar y cumplir con los términos, condiciones y límites. Que en su conjunto regulen la prestación de los servicios de certificación materia de esta política, de forma previa a la contratación de los mismos.

En particular, pero no limitados a los contenidos en:

- ✓ La Ley 19.799 y su reglamento
- ✓ Esta Política CP-FEA CertiNet
- ✓ La CPS-FEA CertiNet
- ✓ Demás normas y procedimientos que se dispongan respecto de estos servicios.

Del mismo modo que lo descrito en este numeral. Se obligan también a mantenerse debidamente informados de las actualizaciones o modificaciones que CertiNet publique en su sitio Web www.certinet.cl

2.2 Responsabilidades

En este punto se incluye en forma unificada las responsabilidades establecidas en la ley 19.799 SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA.

2.2.1 CertiNet

Esta política define que CertiNet, en su actividad como Prestador de Servicios de Certificación acreditado, responderá de acuerdo con el régimen de responsabilidad que establece la Ley chilena 19.799 y la legislación normativa aplicable. Por lo anterior, los Titulares/Usuarios, Terceros que Confían y en general toda entidad o persona que utilice del servicio de certificación declaran conocer y aceptar los términos, condiciones y límites contenidos en esta Política y la "CPS-FEA CertiNet" bajo las cuales se emiten los Certificados de Firma Electrónica Avanzada que se suscriban.

CertiNet no es ni será responsable del uso indebido o incorrecto de los Certificados de Firma Electrónica Avanzada, sus contraseña, sus dispositivos de almacenamiento de llaves o activación, emitidos conforme a la ley 19.799, su reglamento, esta Política y la CPS-FEA CertiNet.

2.2.2 Limitaciones de Responsabilidad

CertiNet limita su responsabilidad a lo indicado en el artículo 14 de la ley 19.799, conforme a lo declarado y regulado en esta Política y la CPS-FEA CertiNet numeral 2.2.2:

"Artículo 14.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.
Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados en virtud de lo dispuesto en el inciso final del artículo 15.
El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.

En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado."

2.2.3 Responsabilidad de la RA y CA

Está Política provee las directrices generales que limitan, restringen y condicionan las responsabilidades en el actuar tanto de la Autoridad de Registro delegada (RA) y de la Autoridad Certificadora (CA), las que se subordinan a lo establecido en la Ley 19.799 y su reglamento, las que incluyen:

- ✓ Realizar la aplicación correcta de los procedimientos autorizados por CertiNet.
- ✓ La RA deberá, Comprobar fehacientemente la identidad del solicitante de un Certificado de Firma Electrónica Avanzada, mediante comparecencia personal ante Certinet, o ante Notario público, o en el domicilio comercial o a través del sistema ClaveÚnica del Registro Civil de Chile u otras que se establezcan por la Entidad Acreditadora o el Legislador.

  Las modalidades específicas son:

  Modalidad 1: Por comparecencia personal ante CertiNet o Notario Público.

  En caso de sea ante Certinet el solicitante debe concurrir a las oficinas de Certinet.

  En caso que se haga la validación de acto presencial ante notario como parte del proceso de solicitud de Certificado de Firma Electrónica Avanzada de la PSC CertiNet S.A., CertiNet entrega formulario que debe ser completado y firmado ante el notario, una vez recepcionado dicho formulario, CertiNet lo valida, y continua el proceso de enrolamiento. Este proceso esta acogido a lo estipulado en el Artículo 12 letra (e) de la ley 19.799,

  Modalidad 2: Por comparecencia personal en el domicilio comercial

  El solicitante debe entregar los elementos de identificación previamente a que agende la visita del Oficial de Enrolamiento, una vez autorizada la visita, el Oficial concurre a efectuar el acto presencial de corroboración de la identidad como indica la ley. El Oficial se coordina con el Supervisor de Enrolamiento

revisan las piezas de identificación del solicitante enviadas en el proceso, autoriza la generación del certificado en forma segura.

Modalidad 3 - Enrolamiento FAR CertiNet: Firma Electrónica Avanzada con Autorización Remota FAR es un servicio de custodia centralizada segura en CertiNet basado en un HSM "Hardware Security Module", en la nube autorizado por la Entidad acrteditadora, el cual *cumple con lo requerido en el Decreto N°24 de la Ley 19.799 y está apto para que pueda ser implementado y de esta forma los ciudadanos puedan adquirir certificados mediante esta metodología a partir del lunes 6 de Diciembre de 2021.*

- ✓ La CA deberá emitir el Certificado de Firma Electrónica Avanzada cumpliendo todas las exigencias técnicas y legales, requeridas en esta política y la "CPS-FEA CertiNet" de conformidad con los datos entregados por el Titular/usuario y publicar el Certificado de Firma Electrónica Avanzada en el directorio correspondiente.

El detalle de cómo deben ser aplicadas se pueden revisar en la CPS-FEA CertiNet, numerales 2.2.1, 2.2.3., la que está disponible en https://www.certinet.cl/acreditacion

2.2.4 Responsabilidad del Titular/Usuario

El Titular/Usuario según lo definido en los numerales 1.4.5 y 2.1.4 de esta Política, es responsable de:

- ✓ La veracidad de la información entregada a CertiNet y/o la Autoridad de Registro al momento de solicitar un certificado
- ✓ Mantener bajo su custodia y exclusivo control su contraseña que da acceso a la llave privada y/o el acceso al mecanismo complementario digital y el o los factores secundarios de seguridad dispuestos para la activación de firma, desde el momento de su generación hasta su extinción
- ✓ Informar de cualquier anomalía detectada en el uso, seguridad, u otras que pudieren afectar al normal funcionamiento del certificado dentro del modelo con el que fue otorgado.
- ✓ Las demás contenidas en la Ley aplicable y sus normas, esta política y la CPS-FEA CertiNet.

2.2.5 Terceros que Confían

De conformidad a lo dispuesto en esta Política, CertiNet declara que todo receptor de un documento firmado con un certificado válidamente emitido que decide confiar libre y espontáneamente en un Certificado de Firma Electrónica Avanzada asume la total responsabilidad y riesgos derivados de la aceptación de dicho Certificado, cuando no haya

realizado en forma previa los pasos necesarios para la verificación de su validez de acuerdo con esta Política y la "CPS-FEA CertiNet".

2.3 Interpretación y Resguardos Legales

Esta Política y la CPS-FEA CertiNet se regirán por la ley chilena y se someterán al Tribunal Arbitral que más adelante se expresa. Un adecuado desglose de este punto lo encontrará en el numeral 2.3 Interpretación y Cumplimiento de la referida "CPS-FEA CertiNet".

El Prestador de Servicios de Certificación, en cumplimiento con las obligaciones impuestas por el legislador en la ley 21.398, dispondrá de un servicio de atención al cliente, por medio del cual se podrán dirigir, por medios remotos (correo soporte@certinet.cl) y/o físicos, cualquier reclamo de los consumidores finales de los servicios prestados en virtud del presente contrato.

2.4 Tarifas

CertiNet declara que tiene una Política de Tarifas no discriminatoria, pública e informada, con apego a las prácticas legales, normativas y de uso general en el comercio. Sin perjuicio de los contratos o tratos comerciales que pueda concertar como parte de su gestión comercial.

Que se resumen en:

- ✓ Los precios de los servicios de certificación o cualquier otro servicio relacionado están disponibles para los usuarios en el sitio https://www.certinet.cl/acreditacion
- ✓ CertiNet cobra una tarifa diferente por cada uno de los servicios que otorgue
- ✓ Como regla general establece que en el evento que un Titular/Usuario determine devolver un certificado ya sea aceptado o no, este será revocado y la tarifa pagada no será devuelta.

Las clases y detalle de tarifas están referidas en el numeral 2.4 de la CPS-FEA CertiNet.

2.5 Publicación y Repositorios

Esta política y la CPS-FEA CertiNet, están disponibles para los Titulaes/Usuarios, Usuarios y público en general a título de información vía electrónica en una página Web contenida en el repositorio de documentos de CertiNet en el sitio Web https://www.certinet.cl/acreditacion

Cualquier cambio o modificación en esta CP-FEA CertiNet generará una nueva versión, debiendo publicarse dicho cambio, además de guardar y custodiar la versión anterior, toda vez que al amparo de esta última pudiesen haberse originado derechos y obligaciones para los Titulares/usuarios de las mismas

Todas aquellas situaciones de vigencia de Certificados y de obligaciones contraídas, se resolverán de acuerdo con la "CPS-FEA CertiNet" vigente al momento de la emisión del Certificado en cuestión.

2.6 Auditorías

CertiNet, realiza a lo menos una auditoría al año a sus procedimientos y procesos, además se somete a un proceso de inspección anual independiente que realiza la Subsecretaría de Economía y Empresas de Menor Tamaño para mantener nuestra acreditación como Prestador de Servicios de Certificación calificado.

Está cláusula se encuentra también en nuestra CPS-FEA CertiNet en la sección 2.6.

2.7 Privacidad y Protección de los Datos

CertiNet declara que está sujeto a la obligación de reserva, de conformidad con la Ley N° 19.628 sobre Protección de la Vida Privada, lo dispuesto en la Ley 19.799, considerando los principios internacionales de protección de datos, los relativos a Secreto Bancario y los emanados de contratos suscritos para la prestación de servicios con condiciones particulares.

Por lo anterior se compromete a realizar dentro de su alcance, todo esfuerzo para garantizar la privacidad y protección de los datos que pueda requerir para el cumplimiento de la prestación de sus servicios conforme a las leyes vigentes, tanto chilenas como internacionales de conocimiento general. Lo anterior se complementa con su política de privacidad publicada en https://www.certinet.cl/politicadeprivacidad

Lo dispuesto en esta Política se encuentra debidamente descrito en detalle en la Declaración de Prácticas de Certificación (CPS-FEA CertiNet) numeral 2.7.

2.8 Derechos de Propiedad Intelectual

CertiNet es titular de los derechos de Propiedad Intelectual de todas las "CP y CPS CertiNet" que se emitan bajo su Modelo de Confianza, y de todos los derechos que la Ley N° 17.336 sobre Propiedad Intelectual contempla respecto de los mismos, lo mismo respecto de los derechos contemplados en virtud de la Ley N° 19.039 de Propiedad Industrial.

En consecuencia, queda prohibida su reproducción total o parcial, por cualquier medio y de cualquier forma sin expresa autorización previa de CertiNet.

Adicionalmente, CertiNet es dueño de la propiedad intelectual y de los derechos de la información de certificados que se mantienen en forma pública, por lo que esta información no puede ser extraída ni copiada sin previo acuerdo con CertiNet.

3 Identificación y Autenticación

CertiNet actúa como Autoridad de Registro o Autoridad de Registro delegada, conforme a la legislación vigente y normativas regulatorias de la actividad, establecidas en la letra e) del artículo 12 de la ley 19.799, el cual señala:

> *"En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;"*

Para mayor detalle sobre el proceso identificación y autentificación del solicitante, está puede ser encontrada en las Declaraciones de Prácticas de Certificación (CPS-FEA CertiNet) Sección 3 y lo estipulado en dentro de los puntos de esta política.

4 Requerimientos Operacionales

CertiNet declara, tener y mantener procedimientos formales para la operación de sus sistemas de acuerdo las mejores prácticas nacionales e internacionales del comercio durante todo el ciclo de vida de los Certificados de Firma Electrónica Avanzada emitidos bajo esta política, los que son inspeccionados integralmente una vez cada año, por la Subsecretaría de Economía y Empresas de Menor Tamaño con el objeto de validar el pleno uso, seguridad y funcionamiento requeridos por la Ley 19.799 el reglamento y las normas técnicas internacionales.

Estos requerimientos cumplen como mínimo con:

4.1 Solicitud de Certificados

Toda persona que desee obtener un certificado de Firma Electrónica Avanzada emitido por CertiNet, debe completar el formulario de solicitud de Certificado.

4.2 Emisión de Certificados:

CertiNet identifica en forma fehaciente la identidad del titular/usuario conforme a lo establecido en la ley 19.799, su reglamento, el Decreto N° 24 de MINECON de 2019, las normas técnicas internacionales reconocidas por la industria y los mecanismos

complementarios y factores secundarios de seguridad que disponga. Lo anterior se encuentra en detalla en la CPS-FEA CertiNet punto 4.2 de dicho documento.

Para la Emisión de los Certificados, el usuario que desee obtener un Certificado emitido por CertiNet, debe presentar a la Autoridad de Registro correspondiente los antecedentes necesarios para que su identidad sea verificada fehacientemente. Los factores de identificación a utilizar son:

Modalidad 1: Por comparecencia personal ante CertiNet o Notario Público.

Tipo de Certificado	Antecedentes Requeridos: Comparecencia ante CertiNet o Notario Público
Firma Electrónica Avanzada	• Comparecer de forma presencial ante CertiNet o Notario Público. • Cédula o Carnet de Identidad vigente • Correo electrónico • Teléfono de contacto • Fotografía el caso de comparecencia personal ante un oficial de registro autorizado por CertiNet • Disponibilidad para Configurar Computador y Dispositivo Token con asistencia de ejecutivos CertiNet.

En caso que se haga la validación de acto presencial ante notario CertiNet entrega formulario que debe ser completado y firmado ante el notario, una vez recepcionado dicho formulario, CertiNet lo valida, envía el token previo a transferencia del cliente y coordina la atención para otra validación de identidad al momento del enrolamiento final con los datos provistos en la notaría.

Modalidad 2: Por comparecencia personal en el domicilio comercial

Tipo de Certificado	Antecedentes Requeridos: Domicilio Comercial
Firma Electrónica Avanzada	• Enviar previamente copia de Cédula o Carnet de Identidad vigente • Indicar el Correo electrónico que se usará para el Certificado • Teléfono de contacto • Pagar la tarifa de Certificado, enrolamiento y token. • Agendar con CertiNet la visita del Oficial de Enrolamiento de CertiNet al domicilio comercial. • Recibir y Comparecer de forma presencial ante el oficial de CertiNet • Fotografía de la comparecencia personal ante un oficial de registro autorizado por CertiNet • Disponibilidad para Configurar Computador y Dispositivo Token con asistencia de ejecutivos CertiNet.

El acto presencial se hace con la corroboración de la identidad por medio de Oficial de Enrolamiento, en el Domicilio Comercial agendado, usando elementos de seguridad de comunicaciones y computador. En conjunto con el Supervisor de Enrolamiento quien dispone de los elementos previos, que son revisados con las piezas de identificación del solicitante enviadas previamente, si correponden a las recogidas en la visita, autoriza la generación del certificado en forma segura.

Modalidad 3 - Enrolamiento FAR CertiNet: Firma Electrónica Avanzada con Autorización Remota FAR es un servicio de custodia centralizada segura en CertiNet basado en un HSM "Hardware Security Module", en la nube.

Tipo de Certificado	Antecedentes Requeridos
Firma Electrónica Avanzada	• Capacidad de acceso a sitio WEB vía internet. • Identificarse a través del sistema “Clave Única”, proporcionada por el Registro Civil de Chile. • Identificarse con un mecanismo complementario como es • pago del servicio con transferencia electrónica o con pago en línea desde una cuenta asociada al RUT del solicitante, transferencia • Correo electrónico, para activación segundo factor de seguridad. • Teléfono Móvil para activación de segundo factor de seguridad.

Basado en el *“flujo entregado para el proceso de emisión de Firmas Electrónicas Avanzadas llamado -Flujo Certinet FAR EEUD”* aprobado por la Entidad Acretidatora.

4.3 Aceptación de Certificados

Se considera que un Titular/usuario acepta su certificado cuando ha cumplido con todos los requisitos y formalidades descritas y descarga su certificado en el dispositivo autorizado por CertiNet.

4.4 Vigencia de Certificados

Los Certificados tienen una vigencia de 1 año calendario, sin perjuicio de otras que pudiere acordar un cliente empresa solicitante o un Titular/usuario con CertiNet. Sin perjuicio de lo anterior la fecha de vigencia de un certificado está incluida en el mismo.

4.5 Usos de Certificados

Solamente se podrán utilizar certificados durante su período de vigencia, de acuerdo con el modelo comercial que el cliente elija y solo para los efectos y términos previstos en esta política y la CPS-FEA Certinet.

4.6 Suspensión y Revocación de Certificados

La suspensión tiene como principal efecto el cese temporal del período de vigencia del certificado hasta el término de esta. CertiNet podrá suspender la vigencia de un certificado cuando se constate o verifique alguna de las circunstancias descritas en esta sección en la CPS-FEA CertiNet.

La revocación es la cancelación anticipada del período operativo de un Certificado válidamente emitido y tiene como principal efecto la terminación inmediata del período de vigencia del Certificado y como consecuencia de lo anterior impide su uso para los fines con que fue solicitado, ya sea por petición expresa del Titular, o por fallecimiento del titular; por resolución judicial ejecutoriada; por incumplimiento de las obligaciones del usuario establecidas en el artículo 24 de la Ley; o por cancelación de la acreditación y de la inscripción como PSC, cuando no se pueda traspasar a otra PCS autorizada.

4.7 Renovación de Certificados

La renovación se produce cuando el certificado va a expirar y el titular/usuario manifiesta voluntariamente su deseo de continuar usándolo. Para esto el titular/usuario deberá presentar una solicitud de renovación en los términos que CertiNet haya definido en su CPS-FEA CertiNet punto 4.7. Consultar detalle en https://www.certinet.cl/acreditacion

4.8 Procedimientos de Auditoría de Seguridad

CertiNet podrá ser Inspeccionado y/o Auditado en los términos y condiciones establecidas en la Ley de Firma Electrónica y el Decreto Supremo N°181 de 2002 del MINECON.

Por su parte CertiNet efectuará de forma periódica auditorias de seguridad a los procedimientos de registro delegados a las Autoridades de Registro y procedimientos internos de la PKI.

4.9 Archivo de Registro

CertiNet dispondrá de registros históricos acorde a sus prácticas, en los cuales mantendrá la información del proceso de registro y estado del certificado conforme a la Ley y lo establecido en esta política y CPS-FEA CertiNet.

4.10 Cese de Actividad de CertiNet

CertiNet procederá según lo establecido en el artículo 12 letra c), de la Ley chilena N° 19.799 sobre firma electrónica y las normas regulatorias vigentes.

"En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;"

Fuente: Art 12 letra c), de la citada ley.

Los requerimientos antes definidos, se desglosan de forma suficiente y completa respecto del cómo se ejecutan materialmente en la Declaración de Prácticas de Certificación (CPS-FEA CertiNet) Sección 4.

5 Control Físico, Procedimientos y Personal

CertiNet declara que utiliza y se apega a las mejores prácticas internacionales y siempre acorde a la regulación nacional vigente para el control físico, con procedimientos operacionales, de seguridad y control formales e informados a la organización y por tanto además contrata personal idóneo, competente que es evaluado respecto de su rol y perfil.

Los procedimientos y prácticas específicas están descritas con alto grado de detalle en la CPS-FEA CertiNet. Punto 5. Consultar detalle en https://www.certinet.cl/acreditacion

6 Controles de Seguridad Técnica:

CertiNet declara que cumple con las mejores prácticas nacionales e internacionales en seguridad de la información, estas prácticas comprenden soluciones tecnológicas de seguridad en las áreas de control, redes, aplicaciones y sistemas.

Dentro del área de aplicaciones, CertiNet evalúa y selecciona proveedores nacionales e internacionales certificados y de reconocida trayectoria. Dado que considera esencial para la integridad de un Prestador de Servicios de Certificación la fiabilidad de su Llave raíz (Llave privada), que es la base de la Cadena de Confianza de CertiNet como Autoridad Certificadora. Lo anterior se realiza conforme a la Ley, Reglamento y normativas vigentes y de acuerdo con lo estipulado en la norma ETSI TS 102 042 V2.4.1 (2013-02), sección 7.

La descripción detallada de estos controles se encuentra en la sección 6 de la CPS-FEA CertiNet.

7 Perfiles de Certificado y CRL.

CertiNet dispone de acuerdo a la ley y normas vigentes, de listas de certificados revocados (CRL), estas listas son archivos públicos que permiten validar la vigencia de los Certificados de Firma Electrónica Avanzada a través de internet, las características principales de estas listas son:

7.1 Perfil del Certificado (Contenido del Certificado):

Los Certificados de Firma Electrónica Avanzada emitidos bajo esta Política están en conformidad con el estándar X.509 versión 3 y contienen a lo menos:

- ✓ Un código de identificación único del certificado;
- ✓ Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único nacional, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia Firma Electrónica Avanzada;
- ✓ Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y
- ✓ Su plazo de vigencia.

Fuente: Articulo 15 de la Ley 19.799.

La composición y estructura de un Certificado de Firma Electrónica Avanzada de Certinet emitido bajo esta política y conforme a la descripción detallada de los procesos asociados contenidos en la CPS-FEA CertiNet, se encuentran de acuerdo con la ley y el Reglamento.

7.2 Perfil de la CRL (Lista de Certificados Revocados)

CertiNet mantiene un Registro Público de Certificados donde publica el estado de los Certificados que se encuentren Vigentes, Suspendidos, Revocados y Traspasados.

En forma adicional y sin perjuicio del acceso en línea (OCSP) descrito, CertiNet emite listas de certificados revocados.

Estructura de la CRL:

7.2.1 Número de Versión

Cada CRL emitida cuenta con un número de versión que permite identificarla.

7.2.2 Periodo de emisión y validez:

Las CRL, son archivos públicos que tienen una vigencia de 24 horas. Estas se reemiten cada 4 horas o cada vez que un certificado es revocado.

7.2.3 Publicación:

Las CRLs se Publican y difunden a través de nuestra página web en:
https://www.certinet.cl/acreditacion

7.2.4 CRLs y Extensiones:

Las CRLs V3, contienen entre otras cosas la siguiente información:

- ✓ Numero de Versión
- ✓ Emisor
- ✓ Fecha Efectiva
- ✓ Fecha de Actualización
- ✓ Algoritmo de firma
- ✓ Algoritmo de Hash de Firma
- ✓ Identificador llave pública de Entidad Emisora
- ✓ Número de la CRL

8 Administración de la Política

8.1 Procedimiento para Modificar esta Política:

Esta Política podrá ser modificada por CertiNet según lo requiera para mantener los estándares de calidad de sus servicios, las imposiciones normativas y en general cualquiera otra que CertiNet estime pertinente.

8.2 Procedimiento de Aprobación

CertiNet dispone de un procedimiento de aprobación de sus políticas que cumple con las siguientes etapas:

- ✓ Desarrollo y presentación a los organismos técnicos y fiscalizadores competentes para recepción de observaciones y sugerencias.
- ✓ Presentación y probación intermedia ante el Comité de Seguridad de la Información.
- ✓ Presentación y aprobación de la Gerencia General de CertiNet

8.3 Procedimiento de Publicación y Notificación

El procedimiento operativo de publicación y notificación debe considerar los siguientes pasos:

- ✓ Será publicada en su sitio Web https://www.certinet.cl/acreditacion al menos 30 días antes de su entrada en vigencia.
- ✓ Se entenderá notificada en concordancia con los numerales 2.1.6 y 2.5 de esta Política.
- ✓ Los Titulares/usuarios que no estén de acuerdo con actualizaciones o modificaciones efectuadas, tendrán derecho a solicitar voluntariamente la revocación o término del servicio con devolución económica proporcional de la parte no consumida del mismo. Sin perjuicio de las garantías legales respecto a las eventuales validaciones posteriores que se requieran a petición de parte competente para efectos de garantizar el no repudio de las firmas efectuadas y/o los derechos que pudiere haber adquirido respecto de la versión de esta política vigente al momento de la contratación de los mismos.

  Sin perjuicio de lo anterior, esta Política se entenderá vigente y valida, solo cuando esté firmada por la Gerencia General de CertiNet o quien le subrogue.

9 Control Documental

Cuando sea necesario se actualizara la Política, asociado a los servicios de certificación, para garantizar la excelencia del servicio y mejora continua, a fin de adecuarlo a las características de uso del momento.