# PRÁCTICAS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA

e-certchile

CAMARA DE COMERCIO DE SANTIAGO

# ÍNDICE

## 1. Introducción.

### 1.1. Presentación.

Las prácticas de certificación de e-certchile son una descripción detallada de las políticas, procedimientos y mecanismos que nos obligamos a cumplir en la prestación de nuestros servicios de certificación de firma electrónica. En ellas se explican, entre otras cosas:

- Las obligaciones y responsabilidades que tiene e-certchile, sus autoridades de registro, los solicitantes, suscriptores y los usuarios de los certificados.
- La forma en que se gestiona el ciclo de vida del certificado.
- Los procedimientos para las auditorías, la forma en que protegemos los datos personales que tratamos y la forma en que hacemos frente a la contingencia y recuperación de desastres.
- Las prácticas de seguridad física, del personal y del manejo de claves de e-certchile.
- El contenido y estructura de los certificados emitidos, vigentes, suspendidos y revocados.
- La forma en que se administra nuestra Práctica de Certificación, incluyendo la forma en que puede ser modificada.

### 1.2. Identificación.

El presente documento se individualiza como “Prácticas de Certificación e-certchile” o “CPS e-certchile”.

La “CPS e-certchile” se ha preparado de conformidad con la RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, emitido por el Internet Engineering Task Force “IETF”, según lo exigido por el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

A esta “CPS e-certchile” podrá acceder permanentemente a través de https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0

1.3. Comunidad y aplicabilidad.

La “CPS e-certchile” se aplica a todos los certificados de firma electrónica emitidos por e-certchile, los que sólo podrán otorgarse a personas naturales mayores de 18 años que cumplan con los requisitos establecidos en la Ley 19.799, su reglamentación y en esta ˝CPS e-certchile”.

El uso de los certificados y la información asociada está restringida a las condiciones de uso específicamente descritas en esta “CPS e-certchile”. Con todo, se previene que los certificados no pueden usarse para certificar a otras personas u objetos.

Los certificados permiten ser usados para demostrar:

- Autoría. Dado el proceso de comprobación de la identidad del solicitante que realiza e-certchile damos confianza respecto a que el suscriptor es quien dice ser.
- Integridad. La información firmada con un certificado emitido por e-certchile permite verificar si el documento electrónico firmado ha sufrido modificaciones con posterioridad a su suscripción.
- No repudio. Dado que se encuentra resguardada la autoría e integridad de los documentos electrónicos, los certificados emitidos por e-certchile permiten demostrar la integridad y autoría.

Adicionalmente, permite cifrar elementos para que sólo pueden ser visualizados por el suscriptor.

1.4. Tipos y usos de certificados.

e-certchile emite diferentes tipos de certificados:

- Firma electrónica simple.

Certificado emitido a personas naturales mayores de 18 años a través de un proceso de comprobación de la identidad del solicitante a través del uso de técnicas y medios electrónicos, sin exigirse la comparecencia personal del solicitante.

Los usos más corrientes de este certificado son la firma de correos electrónicos, el cifrado de correos electrónicos, la autenticación del suscriptor en plataformas electrónicas, facturación electrónica y cualquier otro en que las partes elijan confiar en éstos.

- Firma electrónica avanzada.

Certificado emitido a personas naturales mayores de 18 años a través de un proceso de comprobación fehaciente de la identidad del solicitante a través de la comparecencia personal y directa ante e-certchile o una de sus autoridades de registro.

Los usos más corrientes de esta clase de certificados son los mismos señalados para la firma electrónica simple más la firma de instrumentos públicos y de instrumentos privados en que se desea que tengan el mismo valor probatorio que un instrumento público.

- Firma electrónica avanzada Auxiliar Administración de Justicia.

Certificado emitido a Notarios, Archiveros Judiciales, Conservadores de Bienes Raíces y Registradores de Comercio a través de un proceso de comprobación fehaciente de la identidad del solicitante a través de la comparecencia personal y directa ante e-certchile o una Entidad de Registro. Adicionalmente, se verifica la condición de Notario, Conservador de Bienes Raíces, Registrador de Comercio o Archivero Judicial a través de la certificación correspondiente expedida por la Corte de Apelaciones respectiva.

El uso de este certificado es para la suscripción de documentos electrónicos en que el Notario, Conservador de Bienes Raíces, Registrador de Comercio o Archivero Judicial actúa en dicha calidad.

- Firma electrónica avanzada on-line y firma electrónica avanzada un solo uso.

Certificado emitido a personas naturales mayores de 18 años a través de un proceso de comprobación fehaciente de la identidad del solicitante a través de la comparecencia personal y directa ante www.e-certchile.cl con la clave única que el Registro Civil e Identificación le otorgó al solicitante más la utilización de un segundo factor electrónico de autenticación puesto a disposición del solicitante por e-certchile.

Los usos más corrientes de esta clase de certificados son los mismos señalados para la firma electrónica simple más la firma de instrumentos públicos y de instrumentos privados en que se desea que tengan el mismo valor probatorio que un instrumento público.

1.5. Entidades.

1.5.1. Solicitante.

Persona natural que solicita un certificado de firma electrónica.

1.5.2. Autoridad de Registro.

Son aquellas personas o instituciones que autorizadas por e-certchile y actuando por cuenta y riesgo de e-certchile para una determinada comunidad de negocio, realizan: a) la comprobación de la identidad de los solicitantes, b) registran los antecedentes de los solicitantes que sirven de base para la emisión de los certificados, c) evalúan, aprueban o rechazar las solicitudes de certificados de acuerdo a las políticas definidas por e-certchile d) realizar las funciones de solicitar la suspensión, la revocación, la renovación de certificados de acuerdo a las políticas de e-certchile, además de otras funciones que se le encomienden. e-certchile es por esencia una autoridad de registro y cuando actúa como tal, asume todas y cada una de las obligaciones establecidas en estas “CPS e-certchile”; en el evento de delegar dicha función asume también la responsabilidad por el cometido de sus mandatarios dado que éstos actúan por su cuenta y riesgo.

1.5.3. Certificador.

Son las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorgan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. En caso de que deseen acreditarse deberán encontrarse domiciliadas en Chile y seguir el procedimiento de acreditación que señala el Título V de la ley y desarrolla el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

e-certchile se encuentra acreditado por la Entidad Acreditadora desde el año 2003, mediante la Resolución Exenta Nº 317, de la Subsecretaría de Economía.

1.5.4. Suscriptor.

Aquella persona natural a quien e-certchile le ha emitido un certificado de firma electrónica.

1.5.5. Usuarios.

Aquella persona que voluntaria y libremente decide hacer uso y/o confiar en un certificado emitido por e-certchile.

1.5.6. Entidad Acreditadora

La Subsecretaría de Economía y Empresas de Menor Tamaño en virtud de lo dispuesto en la Ley 19.799.

1.6. Detalles de contacto.

- Dirección postal: Monjitas 392 Piso 17, comuna y ciudad de Santiago de Chile.
- Correo electrónico: sclientes@e-certchile.cl
- Teléfono: (+56 2) 2360 7175
- Mesa ayuda certificación: (+56 2) 2818 5760
- Sucursales
  - Enrique Mac-Iver 410, Local 1, comuna y ciudad de Santiago de Chile:

    Lunes a Jueves: 09:00 – 17:30 hrs.

    Viernes 09:00 – 14:30 hrs.
  - Av. Nueva Providencia 2260, Local 81, comuna de Providencia y ciudad de Santiago de Chile

    Lunes a Jueves: 09:00 – 17:30 hrs.

    Viernes 09:00 – 14:30 hrs.

## 2. Obligaciones y responsabilidades.

### 2.1. Obligaciones.

#### 2.1.1. e-certchile.

Se obliga a:

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

b. Cumplir y respetar los procedimientos establecidos en esta "CPS e-certchile" y en las Prácticas Específicas de Certificados (CP) que se otorguen para la emisión de certificados.

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. Aprobar o rechazar las solicitudes de certificados, directamente o a través de las autoridades de registro, de conformidad con la "CPS e-certchile".

e. Emitir los certificados en conformidad al procedimiento establecido en las "CPS e-certchile".

f. Proveer al suscriptor los dispositivos de custodia de los datos de creación de firma.

g. Comunicar al suscriptor de la emisión de su certificado.

h. Configurar y mantener un Registro de Acceso Público de Certificados, con expresa indicación del estado de éstos (vigente, suspendido o revocado).

i. Revocar o suspender los certificados, notificando de ello al suscriptor.

j. Realizar razonables esfuerzos para comunicar a los suscriptores cualquier hecho conocido por e-certchile que pudiera afectar la validez del certificado.

k. Delegar la función de autoridad de registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.

l. Mantener www.e-certchile.cl con información para el público sobre los servicios de e-certchile.

2.1.2. Autoridad de registro.

Se obliga a:

a. Comprobar la identidad de los solicitantes de un certificado de conformidad al procedimiento establecido en esta "CPS e-certchile", y en las Prácticas Específicas de Certificado (CP).

b. Registrar y custodiar por 6 años los antecedentes, requeridos a los solicitantes, que sirvieron de base para la emisión de los certificados, de conformidad con los requisitos establecidos en las Prácticas Específicas de Certificado (CP).

c. Aprobar o rechazar las solicitudes de emisión de certificados.

d. Entregar al suscriptor su certificado o dar las instrucciones para su retiro y/o de uso, según el mecanismo de custodia que el cliente haya elegido libremente.

e. Recibir las solicitudes de revocación o suspensión de certificados e informarlas a e-certchile.

f. Obtener la aceptación en forma inequívoca de los términos y condiciones del servicio por parte del solicitante.

g. Permitir operar solamente certificados que hayan sido aceptados por el solicitante.

h. Prestar cualquier otro servicio que e-certchile le solicite.

Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro por cuenta y riesgo de e-certchile.

2.1.3. Obligaciones del suscriptor.

*Antes de la emisión del certificado se obliga a:*

a. Ser persona natural mayor de 18 años.

b. Solicitar la emisión del certificado aceptando los términos y condiciones descritos en esta "CPS e-certchile".

c. Proveer a e-certchile y/o la autoridad de registro toda la información que de acuerdo con esta "CPS e-certchile" es requerida para comprobar su identidad.

d. Elegir si los datos de creación de firma serán almacenados en un e-Token o en un dispositivo masivo criptográfico custodiado por e-certchile, estableciendo el pin de protección de éstos. En el caso de elegir el almacenamiento en un dispositivo masivo criptográfico custodiado por e-certchile deberá mantener accesible un segundo factor de seguridad que le permita controlar que el acceso y utilización de los datos de creación de firma pueden ser únicamente utilizados por él.

e. No revelar el PIN del dispositivo que contiene los datos de creación de firma asociados al certificado y/o no relevar el mecanismo de activación de la firma, según lo señalado en la letra d).

f. Pagar las tarifas convenidas por concepto de los servicios de certificación, aun cuando no se acepten o no se ocupen los certificados emitidos.

*Una vez emitido el certificado se obliga a:*

a. Aceptar el certificado. Se entiende que un certificado es aceptado por el suscriptor cuando:

i) Haya sido emitido por e-certchile, aun cuando el certificado no haya entrado en vigor por contener una fecha de inicio de operación posterior a su fecha de emisión.

ii) No se haya formulado un reclamo por error o inexactitud en la emisión al momento de su recepción.

iii) Se haya utilizado la clave de confirmación comunicada por e-certchile para retirar el certificado, se haya instalado éste en el dispositivo de

generación y almacenamiento de firma o haya sido utilizado por el suscriptor.

b. Comunicar a e-certchile cualquier error o inexactitud en el certificado que reciba. Si no lo hace al momento de su recepción todas las declaraciones se tendrán por verdaderas.

c. Usar los datos de creación de firma asociados al certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, las "CPS e-certchile" y en las Prácticas Específicas de Certificado (CP).

d. Utilizar correctamente el certificado.

e. Ser un usuario final, y no usar el certificado para actuar como certificador de firma electrónica.

f. Comunicar inmediatamente a e-certchile y/o a una autoridad de registro el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de sus datos de creación de firma o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.

g. Comunicar la pérdida o destrucción del eToken utilizado para el almacenamiento de los datos de creación de firma.

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

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

j. No usar los datos de creación de firma una vez que el certificado haya expirado o haya sido solicitada la suspensión o revocación.

k. Destruir los datos de creación de firma en caso de que e-certchile así se lo solicite y haya sido revocado previamente el certificado.

2.1.4. Obligaciones de los usuarios.

Los usuarios que decidan en forma libre y espontánea confiar y usar los certificados emitidos por e-certchile, se obligan en forma previa a:

a. Verificar la validez del certificado mediante una consulta al registro de acceso público de certificados.
b. Verificar la firma del suscriptor,
c. Comprobar cualquier limitación funcional que incorpore el certificado.
d. Validar el uso de certificado para propósitos autorizados de conformidad con la legislación vigente.

2.1.5. Obligación general.

Los usuarios de los servicios de certificación de e-certchile se obligan a conocer y aceptar los términos, condiciones y límites contenidos en estas “CPS e-certchile” y en las Políticas de Específicas de Certificados (CP), los que en conjunto regulan la prestación de los servicios de certificación de firma electrónica.

2.2. Responsabilidades.

2.2.1. e-certchile.

a. Emitir los certificados cumpliendo todas las exigencias establecidas en estas “CPS e-certchile” y de conformidad con la información proporcionada por el suscriptor.
b. Que el certificado no contenga errores de trascripción de los datos proporcionados por el suscriptor durante el proceso de comprobación de la identidad.
c. 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. La aplicación correcta del procedimiento empleado.

e-certchile no será responsable por ningún daño o perjuicio actual o futuro, directo o indirecto, previsto o imprevisto, emergente o lucro cesante, pérdida de datos u otros, debidos, ocasionados o conectados con el uso indebido, no uso, uso tardío de certificados, aun cuando e-certchile hubiera sido advertido de la posibilidad de producción de tales daños.

e-certchile no será responsable del uso indebido o incorrecto de los certificados, sus datos de creación de firma o los PIN con que los dispositivos de almacenamiento de éstos son protegidos.

2.2.2. Limitación de responsabilidad de e-certchile.

Las responsabilidades que afectan la operación de e-certchile se encuentran limitadas a lo establecido en el artículo 14 de la Ley 19.799.

En todo caso, la responsabilidad de e-certchile cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a e-certchile, quedará limitada como máximo al monto correspondiente a UF 5.000 (cinco mil unidades de fomento), monto asegurado de conformidad con lo dispuesto en el artículo 14 de la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

La actividad de certificación de e-certchile se encuentra limitada al ciclo de vida del certificado, esto es los procesos asociados a la solicitud del certificado, el registro del solicitante, la firma y emisión del certificado, la publicación y archivo de éste y la revocación y suspensión del certificado.

2.2.3. Fuerza mayor.

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

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

2.2.4. Autoridad de registro.

Es responsable de:

a. Comprobar la identidad del solicitante de acuerdo con esta "CPS e-certchile" y la Práctica Específica de Certificado (CP).
b. Registrar y custodiar los antecedentes requeridos a los solicitantes que sirvieron de base para la emisión de los certificados, de conformidad con los requisitos establecidos en las Práctica Específica de Certificado (CP).
c. Realizar con la diligencia y el cuidado debido las funciones que conforme a esta "CPS e-certchile" le correspondan como Autoridad de Registro o que e-certchile le solicite.

2.2.5. Suscriptor.

El Suscriptor es responsable de:

a. La veracidad de la información entregada a e-certchile y/o la autoridad de registro al momento de solicitar un certificado.
b. Que todas las declaraciones que realizó al momento de solicitar el certificado son verdaderas.
c. Pagar la tarifa asociada al certificado solicitado.
d. Que todas las menciones contenidas en el certificado son verdaderas.
e. Mantener bajo su custodia y exclusivo control los datos de creación de firma.
f. Que cada firma electrónica creada utilizando los datos de creación de firma asociadas a la clave pública contenida en el certificado, corresponde a su firma electrónica y que el certificado ha sido aceptado y se encontraba vigente al momento de la creación de dicha firma.

g. Indemnizar e-certchile 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.

2.2.6. Usuario.

El Usuario que confía y usa libre y espontáneamente un certificado asume la 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 las "CPS e-certchile".

2.3. Ley aplicable y resolución de controversias.

2.3.1. Ley aplicable.

Esta "CPS e-certchile" y las Prácticas Específicas de Certificado (CP) se rigen por la ley Chilena y se someterán al Tribunal Arbitral que más adelante se expresa.

2.3.2. Procedimiento de resolución de conflictos.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de esta "CPS e-certchile, las Prácticas Específicas de Certificados (CP) y en general la actividad de certificación que realiza e-certchile será resuelto definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que, en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El arbitraje se llevará a cabo en la ciudad de Santiago. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse en conformidad a las reglas

establecidas para dichas resoluciones en el Título Sexto, del Libro Primero, del Código de Procedimiento Civil. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualesquiera de las Partes presentaren ante el sustituto. La evidencia de haberse ausentado del país el árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro deberá tener el carácter de mixto y su designación será efectuada, a solicitud escrita de cualquiera de las Partes, por la Cámara de Comercio de Santiago A.G. de entre los integrantes de la lista arbitral de su Centro de Arbitraje y Mediación, para lo cual las Partes le otorgan, mediante este instrumento, un mandato especial e irrevocable.

2.3.3. Separación y divisibilidad de cláusulas.

En el evento que alguna disposición contenida en las “CPS e-certchile” o en las Prácticas Específicas de Certificados (CP) sea declarada nula, inoponible o cualquier otra causa de ineficacia jurídica, se deja constancia que dicha declaración sólo afecta la norma en particular, dejando vigente en su integridad el resto del documento.

2.3.4. 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.

d) “CPS e-certhile” vigente.

e) Prácticas Específicas de Certificado (CP).

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

2.3.5. Limitación de uso de certificados.

Se deja constancia de que los certificados no son medios de pago, sino que su finalidad es identificar a una persona en un sistema de redes abiertas o cerradas. No obstante, los certificados regidos por esta "CPS e-certchile" pueden ser utilizados en operaciones que importen órdenes de pago o transferencias de dinero.

No se permite un uso del Certificado contrario a:

a. La normativa chilena y a los convenios internacionales ratificados por el Estado chileno.
b. Lo establecido en esta "CPS e-certchile", en la Política Específica de Certificados (CP) y en los contratos que se firmen entre e-certchile o sus autoridades de registro y el suscriptor.

Los certificados e-certchile no podrán ser alterados y deberán utilizarse tal y como son suministrados por e-certchile.

2.4. Tarifas.

El solicitante se obliga a pagar a e-certchile y/o a las Autoridades de Registro las tarifas establecidas para los certificados cuya emisión se solicite.

Las tarifas se encuentran permanentemente publicadas y disponibles en www.e-certchile.cl/tarifas.

El pago señalado tiene como causa y fundamento exclusivamente la Emisión del certificado. Tratándose de certificados de firma electrónica avanzada adicionalmente considera la entrega de los mecanismos de custodia de los datos de creación de firma, sea que el suscriptor opte por almacenarlos en un e-Token o porque e-certchile los mantenga custodiados en un dispositivo masivo criptográfico.

La no aceptación posterior de un certificado por una causal distinta a errores o inexactitudes en éste o su no uso no autoriza al suscriptor para pedir reembolso alguno.

2.5. Publicaciones y repositorio.

e-certchile mantiene permanentemente a disposición de cualquier interesado esta "CPS e-certchile" en https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0Cualquier modificación a esta "CPS e-certchile" generará una nueva versión, debiendo publicarse dicho cambio y custodiarse la versión anterior.

Cualquier situación ocasionada con relación a la vigencia de un certificado y de las obligaciones contraídas por e-certchile se resolverán de acuerdo con la "CPS e-certchile" vigente al momento de la emisión del certificado en cuestión.

La información respecto al estado de vigencia de los certificados emitidos por e-certchile se encuentra disponible en el registro de acceso público de certificados, al que también se puede acceder desde www.e-certchile.cl.

El registro de acceso público de certificados se actualiza de acuerdo con las siguientes reglas:

a. La información relativa a los certificados es publicada en el mismo momento en que éstos son emitidos.
b. La información relativa a la revocación de los certificados es publicada dentro de un plazo que no puede exceder de 24 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación.
c. La información relativa a la suspensión de los certificados es publicada en el mismo momento en que ésta es solicitada.

2.6. Auditorías.

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

e-certchile realiza auditorías a su instalaciones y sistemas como parte de sus certificaciones ISO 9.001 y ISO/IEC 27.001, comprometiéndose a corregir dentro de un plazo razonable, las eventuales deficiencias que se puedan encontrar.

Adicionalmente, e-certchile auditará, directamente o a través de empresas especialmente contratadas, a sus autoridades de registro cuando lo estime conveniente, incluyéndose al menos, una auditoria al iniciar la operación como autoridad de registro.

2.7. Protección de datos personales.

Su privacidad es importante para nosotros y para protegerla de mejor manera hemos diseñado una política de tratamiento de datos.

Esta política explica la forma en que tratamos sus datos personales y las opciones que Ud. tiene respecto a lo que hacemos. En todo caso, tenga presente que todos los tratamientos los hacemos en el marco de la habilitación legal que nos otorga la Ley 19.799 y en los términos establecidos en la Ley 19.628. Nuestra política vigente siempre la encontrará disponible en https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0.

2.8. Derechos de propiedad intelectual e industrial.

Pertenecerá a e-certchile, en forma total y exclusiva, la propiedad intelectual e industrial de las obras creadas, desarrolladas o modificadas para la prestación de los servicios de certificación. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por e-certchile se entenderá conferido a cualquiera de las personas individualizadas en el punto 1.5 Entidades.

Los solicitantes, suscriptores y usuarios no podrán hacer uso del nombre, marca o logo de e-certchile para efectos de publicidad o cualquiera otro, sin perjuicio de poder pactar especialmente, de acuerdo al tipo y alcances de difusión, condiciones diversas con e-certchile, mediante un acuerdo escrito.

## 3. Identificación y autenticación.

3.1. Registro inicial.

La identificación de los solicitantes se realiza de conformidad con las normas y procedimientos establecidos en esta “CPS e-certchile”, sin perjuicio de los requisitos específicos que las Prácticas Específicas de Certificados (CP) establezcan para un tipo de certificado.

Con todo, la solicitud de un certificado de firma electrónica avanzada deberá realizarla el Solicitante:

a. Compareciendo en forma personal y directa a las oficinas de e-certchile o de la autoridad de registro.
b. Compareciendo en forma personal y directa en www.e-certchile.cl utilizando la clave única que le hubiere sido otorgada por el Registro Civil.

Todas las autoridades de registro de e-certchile realizarán de idéntica forma el proceso de comprobación de la identidad de los solicitantes, sea para el otorgamiento de firma electrónica simple o avanzada.

3.1.2. Presentación de antecedentes.

Cuando el solicitante comparezca en forma personal y directa a las oficinas de e-certchile o de la autoridad de registro deberá presenta su cédula de identidad, una fotocopia de la misma y la aprobación de la solicitud de certificado que le haya enviada debidamente impresa.

Para el caso de los Notarios, Conservadores, Registradores de Comercio y Archiveros Judiciales, titulares, suplentes e interinos, adicionalmente deberán presentar la certificación de tal condición emitida por el Secretario de la Corte de Apelaciones respectiva.

Cuando el solicitante comparezca en forma personal y directa en www.e-certchile.cl utilizando la clave única que le hubiere sido otorgada por el Registro Civil no requerirá presentar antecedentes complementarios.

3.1.3. Existencia de antecedentes.

No serán requeridos aquellos antecedentes necesarios para la emisión de certificados cuando la información a confirmar ya se encuentre en poder de e-certchile, de una autoridad de registro o la comprobación de identidad se realice a través de la clave única del solicitante.

Tampoco será necesario acompañar dichos antecedentes si la solicitud es suscrita electrónicamente por el solicitante a través de una firma electrónica avanzada emitida por e-certchile y que se encuentre vigente.

3.1.4. Comprobaciones con terceros de confianza.

e-certchile comprueba con terceros de confianza como el Registro Civil y bureaus de información que la cédula de identidad se encuentre vigente y no bloqueada y que el solicitante se encuentre vivo.

Adicionalmente, para el otorgamiento de firma electrónica avanzada:

a. Cuando el solicitante comparezca en forma personal y directa a las oficinas de e-certchile o de la autoridad de registro se valida la identidad a través de un pareo entre la información biométrica de la cédula de identidad y la huella digital del solicitante.
b. Cuando el solicitante comparezca en forma personal y directa en www.e-certchile.cl utilizando la clave única que le hubiere sido otorgada por el Registro Civil se utiliza complementariamente un servicio de *challenge de preguntas* provisto por un bureau de información para los efectos de utilizarlo como segundo factor digital de comprobación de identidad del solicitante.

3.1.5. Asignación de nombres.

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

a. Los mismos nombres que figuran en la cédula de identidad cuando el solicitante haya comparecido en forma personal y directa a las oficinas de e-certchile o de la Autoridad de Registro
b. Los mismos nombres que consten en el Sistema ClaveÚnica cuando la persona haya comparecido en forma personal y directa ante www.e-certchile.cl a través de dicho mecanismo.

3.1.6. Asignación de RUT.

Para la asignación del RUT a ser contenido en los certificados se incluirá:

a. El RUT que figura en la cédula de identidad cuando el solicitante haya comparecido en forma personal y directa a las oficinas de e-certchile o de la Autoridad de Registro
b. El RUT que conste en el Sistema ClaveÚnica cuando la persona haya comparecido en forma personal y directa ante www.e-certchile.cl a través de dicho mecanismo.

3.1.7. Asignación de correo electrónico.

Para la asignación del correo electrónico a ser contenido en los certificados se incluirá:

a. El correo electrónico declarado por el solicitante al comparecer en forma personal y directa a las oficinas de e-certchile o de la Autoridad de Registro
b. El que conste en el Sistema ClaveÚnica cuando la persona haya comparecido en forma personal y directa ante www.e-certchile.cl a través de dicho mecanismo.

3.1.8. Generación de claves.

El Suscriptor del certificado debe poder generar sus datos de creación de firma y su correspondiente clave pública, en forma segura y bajo su exclusivo control.

Cuando el Suscriptor vaya a generar los datos de creación de firma y su correspondiente clave publica para un certificado de firma electrónica avanzada deberá utilizar los dispositivos de almacenamiento que le hayan sido provistos por e-certchile (etoken o dispositivo masivo criptográfico con custodia e-certchile). Este es un requisito esencial para obtener un certificado de este tipo.

3.1.9. Protección de claves.

El suscriptor es el único responsable de la protección de sus datos de creación de firma, por lo que deberá adoptar los resguardos para prevenir la perdida, compromiso, revelación, mal uso o uso no autorizado de los mismos. Para ello, deberá proteger el acceso al dispositivo

en que éstos son contenidos (eToken o dispositivo masivo criptográfico custodiado por e-certchile) mediante PIN. Tratándose de datos de creación de firma custodiados en dispositivos masivos criptográfico de e-certchile además deberán ser protegidos con un segundo factor de seguridad en la forma especificada en la Política Específica de Certificados (CP) aplicable a los certificados de firma electrónica avanzada on-line.

3.1.10. Uso de claves.

En el evento que el suscriptor entregue el acceso a sus datos de creación de firma a terceros, los documentos electrónicos y/o las autenticaciones realizadas por ellos serán de su exclusiva responsabilidad, puesto que el titular sigue siendo el responsable por el uso que de ella se haga. Lo anterior, es sin perjuicio del derecho de e-certchile de accionar civil, administrativa o penalmente contra los terceros que hubieren hecho uso de los datos de creación de firma.

3.2. Identificación frente a otras solicitudes.

3.2.1. Solicitud de suspensión y revocación.

Frente a una solicitud de suspensión o revocación existen tres formas de proceder:

a. Compareciendo en forma personal y directa ante e-certchile o una de sus autoridades de registro para hacer la solicitud.
b. Comunicación con e-certchile o una de sus autoridades de registro por medios electrónicos para efectuar un procedimiento de identificación que permita formar la convicción de respecto de su identidad. Dentro del plazo de 24 horas el solicitante deberá comparecer en forma personal y directa ante e-certchile o una de sus autoridades de registro para ratificar la solicitud.
c. Compareciendo en www.e-certchile.cl solicitando la suspensión o revocación y acreditando la identidad con la clave única provista por el Registro Civil al solicitante.

3.2.2. Solicitud de renovación.

Frente a una solicitud de renovación existen dos formas de proceder dependiendo si el suscriptor tiene un certificado de firma electrónica avanzada vigente emitido por e-certchile.

a. Sin certificado de firma electrónica avanzada vigente. Es necesario realizar todo el proceso de registro como si el solicitante nunca hubiere tenido un certificado de firma electrónica con e-certchile.
b. Con Firma Electrónica Avanzada Vigente. Mientras se encuentre vigente una firma electrónica avanzada emitida por e-certchile el suscriptor podrá solicitar otro certificado, sin necesidad de realizar todo el proceso de registro inicial. Para ello, deberá acceder a www.e-certchile.cl y seguir el procedimiento.

## 4. Requerimientos operacionales.

4.1. Solicitud de certificados.

4.1.1. Presentación solicitud certificados.

Toda persona natural y mayor de 18 años que desee obtener un certificado en e-certchile deberá llenar y enviar el formulario de Solicitud de Certificado disponible en www.e-certchile.cl.

e-certchile podrá autocompletar la solicitud con la información que ya se encuentra en su poder o que le proporcione el Sistema Clave Única cuando Ud. opta por dicho mecanismo para la comprobación de su identidad. Con todo, el formulario autocompletado sólo debe ser considerador una propuesta siendo responsabilidad del solicitante cotejar la exactitud de la información sugerida y corregir aquella que sea inexacta o incompleta.

Tratándose de una solicitud un certificado de firma electrónica avanzada el solicitante además deberá comparecer personal y directamente ante una oficina de e-certchile, ante una autoridad de registro o en www.e-certchile.cl mediante su clave única provista por el Registro Civil e Identificación.

En caso de que se trate de un certificado de firma electrónica avanzada Auxiliar de la Administración de Justicia adicionalmente deberá acompañar la certificación correspondiente expedida por la Corte de Apelaciones respectiva.

4.1.2. Comprobación de solicitudes.

e-certchile y/o sus autoridades de registro procederán a verificar la información proporcionada en la solicitud y que deben ser contenidos en el certificado respectivo.

Asimismo, e-certchile realizará verificaciones de información con terceros de confianza en la forma señalada en el apartado 3.1.4.

El solicitante otorga su consentimiento expreso para que e-certchile trate sus datos personales con la finalidad de hacer las comprobaciones necesarias que permitan emitir el certificado de firma electrónica en la forma exigida por la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo, específicamente para comprobar el número de cédula de identidad, el número de documento o de serie de la cédula de identidad, el nombre completo, el correo electrónico, que la cédula de identidad se encuentra vigente, que el solicitante no ha fallecido, asimismo, la información necesaria para emitir el correspondiente instrumento tributario de cobro.

4.1.3. Aceptación de la solicitud.

Si el proceso de validación y comprobación de antecedentes resultó exitoso e-certchile o la autoridad de registro, aceptará la solicitud de emisión de certificado.

4.1.4. Rechazo de la solicitud.

Aquellos solicitantes que no dispongan de la adecuada información, que no acrediten su identidad en la forma exigida en el apartado 3.1. o que los antecedentes que presenta no sean concordantes, se les rechazará la solicitud sin expresión de causa.

El rechazo se comunicará por correo electrónico dirigido a la casilla individualizada en la solicitud. En caso de que los defectos encontrados sean subsanables, se le otorgará al solicitante un plazo de siete días para corregir bajo apercibimiento de tener por confirmado el rechazo.

El solicitante siempre podrá con posterioridad iniciar un nuevo proceso de solicitud de certificado.

4.2. Emisión de certificados.

Aprobada la solicitud e-certchile procederá a la emisión del certificado.

e-certchile sólo emite certificados con el consentimiento del suscriptor, por lo que se entiende que éste fue otorgado por el sólo hecho de que se presente una solicitud de certificado.

El certificado y su contenido son propiedad de e-certchile y se emite con carácter personal e intransferible a nombre del suscriptor.

4.3. Aceptación del certificado por parte del suscriptor.

Se entiende que un certificado ha sido aceptado por el suscriptor una vez que:

a. Este haya sido emitido por e-certchile, aun cuando el certificado no haya entrado en vigor por contener una fecha de inicio de operación posterior a su fecha de emisión.
b. No se haya formulado un reclamo por error o inexactitud en la emisión, al momento de su recepción;
c. Haya sido utilizado por el suscriptor, se utilice la clave de confirmación comunicada por e-certchile para retirar el certificado, se haya instalado en el dispositivo de generación de firma o se haya dejado en custodia para la posterior utilización.

4.4. Vigencia del certificado.

Todos los certificados se consideran vigentes desde el momento de su emisión y hasta la fecha de expiración, suspensión o revocación, salvo que el propio certificado indique una fecha de entrada en vigor posterior a la fecha de emisión, en cuyo caso el certificado entrará en vigor en dicha fecha.

4.5. Suspensión y revocación de certificados.

4.5.1. Suspensión de certificados.

Procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

a. Solicitud del titular del certificado.
b. Decisión de e-certchile en virtud de razones técnicas.
c. Solicitud de un tercero cuando haya encontrado extraviado el soporte en que se contiene el certificado.

4.5.2. Efectos de la 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.

4.5.3. Término de la suspensión.

La suspensión del certificado terminará: por cualquiera de las siguientes causas:

a. Por la decisión de e-certchile de revocar el certificado, en los casos previstos en la Ley.
b. Por la decisión de e-certchile 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.

4.5.4. Revocación.

La revocación tendrá lugar cuando el prestador de servicios de certificación constate alguna de las siguientes circunstancias:

a. Lo haya solicitado el suscriptor.
b. Lo haya solicitado un tercero cuando:
    - Haya encontrado extraviado el soporte en que se contiene el certificado.
    - Haya fallecido el suscriptor.

- Se haya declarado la incapacidad total o parcial del suscriptor.
- El certificado contenga inexactitudes.

c. Haya fallecido el suscriptor.

d. Haya una resolución judicial ejecutoriada que lo ordene.

e. El suscriptor al momento de solicitar el certificado nos haya proporcionado datos de su identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.

f. El suscriptor no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.

g. El titular del certificado no ha actualizado sus datos al cambiar éstos.

4.5.5. Efectos de la revocación.

El efecto de 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.

4.5.6. Fecha de inicio de efectos de la suspensión o revocación.

La suspensión y la revocación comenzarán a producir efectos a partir de la publicación por parte de e-certchile en el registro de acceso público de certificados.

En ningún caso la suspensión o revocación afectará el valor de los certificados y los derechos y obligaciones constituidas bajo su vigencia, en un momento anterior a dicha verificación.

El término de la suspensión por levantamiento de la ésta mantiene vigente el certificado por todo el tiempo que resta hasta su fecha de término de vigencia original.

4.5.7. Procedimiento para suspender o revocar un certificado.

Deberán solicitar la suspensión o revocación de un certificado el suscriptor o la autoridad de registro en cuanto tomen conocimiento por cualquier medio de la concurrencia de alguna de las circunstancias contempladas en el apartado 4.6.1 o 4.5.8.

La suspensión o revocación se efectuará una vez que se valide la identidad de quien la solicita, mediante una comunicación enviada por quien la solicita a sclientes@e-certchile.cl.

En caso de que la suspensión o revocación que se solicita sea de un certificado de firma electrónica avanzada además se requerirá que comparezca personal y directamente ante:

a. Una oficina de e-certchile.
b. Una autoridad de registro de e-certchile.
c. www.e-certchile.cl mediante la clave única provista por el Registro Civil al solicitante de la suspensión o revocación.

Tratándose de certificados de firma electrónica avanzada auxiliar de la administración de justicia además será necesario que al solicitar la suspensión o revocación se presente copia del aviso de extravío dado a la Corte de Apelaciones respectiva.

Una vez recibida y comprobada la identidad de quien solicita la suspensión o e-certchile procederá a efectuar la revocación efectiva del certificado.

La decisión de suspender o revocar un certificado siempre corresponde a e-certchile.

La decisión de suspender o revocar el certificado será comunicada por e-certchile al suscriptor mediante el envío de un correo electrónico a la casilla individualizada en el certificado de firma electrónica.

4.6. Renovación de certificados.

La renovación de los certificados se produce cuando éste se encuentra próximo va a expirar y el suscriptor desea continuar usando un certificado.

Para renovar el certificado el suscriptor deberá presentar una solicitud de renovación en la forma establecida en el apartado 3.2.2.

e-certchile podrá enviar al suscriptor en el correo electrónicos establecido en el certificado un aviso informando que el certificado se encuentra próximo a expirar y que con ello perderá su vigencia, para los efectos de facilitar el proceso de renovación.

4.7. Procedimiento de auditoría de seguridad.

e-certchile es inspeccionado anualmente por la Entidad Acreditadora para los efectos de velar porque las instalaciones, sistemas, programas informáticos y los recursos humanos

necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento se mantienen permanentemente vigentes.

Adicionalmente, se realizan periódicamente auditorias para mantener las certificaciones ISO 9.001 y ISO/IEC 27.001.

Anualmente se auditan aleatoriamente una muestra estadísticamente representativa de las autoridades de registro para los efectos de comprobar que están cumpliendo cabalmente con la tarea que les encomienda e-certchile.

4.8. Archivo de registros.

e-certchile mantiene almacenada toda la información que sirve de base a la emisión de un certificado por un plazo de 6 años contados desde la fecha en que se realizó la comprobación de identidad.

La información se mantiene custodiada en forma electrónica para ser entregada a requerimiento de la Entidad Acreditadora o de una autoridad administrativa o judicial competente.

4.9. Cesación de actividad de e-certchile.

En caso de que e-certchile cese voluntariamente en la prestación los servicios de certificación de firma electrónica comunicará tal situación a los suscriptores 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 usuario ha consentido en la transferencia de estos.

En caso de que el suscriptor se oponga a la transferencia del certificado a otro prestador de servicios de certificación, éste será revocado y e-certchile restituirá la parte del precio que corresponda por tiempo en que el servicio no será prestado, no teniendo el suscriptor derecho a algún tipo de compensación o indemnización de naturaleza diferente.

## 5. Control físico, procedimientos y personal.

### 5.1. Control físico.

La ubicación física de la unidad que otorgue los servicios de certificación no será publicada en esta Práctica de Certificación e-certchile "CPS e-certchile" por motivos de seguridad, sin perjuicio que nos puede ubicar en Monjitas 392, Piso 17, comuna y ciudad de Santiago de Chile.

El acceso físico a e-certchile dispone de un esquema de control de acceso. Asimismo, el acceso físico a la unidad que otorga los servicios de certificación será bajo estrictas normas de seguridad y monitoreo incluyendo esquemas electrónicos de identificación y control, adicionalmente, este lugar dispone de elementos adecuados para la operación tales como aire acondicionado, sistema de detección y prevención de incendios, almacenamiento seguro de material confidencial, esquema seguro de respaldos externos para eventuales catástrofes.

### 5.2. Procedimientos de control.

El control de las funciones se efectuará por medio de disponer de:

- Adecuada segregación de funciones.
- Control dual de las funciones críticas.
- Identificación y autenticación de cada rol.

### 5.3. Compromiso de seguridad y recuperación de desastres.

#### 5.3.1. Alta disponibilidad.

En el eventual escenario de no disponibilidad por la falla de una o más componentes, se evitarán las consecuencias negativas en el servicio mediante una configuración de alta disponibilidad, por medio de la duplicación de los servicios y equipos necesarios para otorgar los servicios críticos asociados a la emisión de los certificados de firma electrónica. Dentro de los elementos duplicados para los sistemas críticos se incluyen servidores, conexiones de red, switches y routers. Adicionalmente, se consideran conexiones a

diferentes prestadores de acceso a Internet que utilicen diferentes redes troncales de modo de asegurar el acceso expedito desde diferentes proveedores de acceso.

5.3.2. Soporte de desastres.

Tratándose de un caso de desastre, para los sistemas críticos se dispone de un sitio alternativo remoto de procesamiento, para asumir las funciones, con indicación de los niveles de servicio y tiempo de recuperación comprometidos para continuar con los servicios de certificación de firma electrónica.

Para los servicios no críticos se dispone de un Plan de Contingencia probado que permite restablecer dichos servicios en un plazo adecuado a los tiempos involucrados con la emisión de Certificados.

Complementario a la solución de alta disponibilidad nuestro sistema de respaldo no permite minimizar la pérdida de información.

Para asegurar la adecuada reposición de los servicios, en caso de fallas, se cuenta con Manuales que permitan superarla de manera estructurada.

5.4. Control del personal.

5.4.1. Requerimiento de antecedentes y experiencia.

e-certchile requiere que todo el personal asociado a la certificadora cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, lo cual incluye:

- Conocimientos y formación sobre entornos de certificación digital y sellos de tiempo.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la certificadora.

5.4.2. Comprobación de antecedentes.

e-certchile realiza una comprobación de los antecedentes del personal para asegurar que cumpla con las formación y experiencia necesaria para asumir un rol de confianza en la certificadora.

5.4.3. Roles de confianza.

e-certchile declara que sus roles de confianza al cumplir su función de PSC corresponden a:

- Oficial de seguridad: Responsable de la administración e implementación de las prácticas de seguridad.
- Administrador de Sistemas: Responsable de instalar, configurar y mantener los sistemas de confianza de la certificadora, para la administración de sello de tiempo. Además, es responsable por la operación de los sistemas y autorizado para realizar el respaldo y recuperación.
- Administrador de Seguridad: Responsable de verificar la mantención de los sistemas de confianza de la certificadora.
- Auditor: Responsable de revisar archivos y log de auditoría de la certificadora.

5.4.4. Requerimientos de formación y reentrenamiento.

Como parte de las recomendaciones en que e-certchile ha trabajado, se considera para el personal asociado a la certificadora, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de e-certchile para la certificadora de firma electrónica. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

5.4.5. Sanciones.

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

5.4.6. Requerimientos de contratación.

Como parte de los requerimientos de contratación, todo trabajador de la certificadora debe firmar un acuerdo de confidencialidad.

5.5. Documentación entregada al personal.

5.5.1. El personal de la certificadora tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación e-certhile (CPS e-certchile).
- Declaración de Prácticas de Certificación Biometría e-certhile (CPSB e-certchile).
- Declaración de Prácticas de Certificación Sellado de Tiempo e-certhile (CPST e-certchile).
- Políticas de Certificación.
- Políticas de Tratamiento de Datos Personales.
- Políticas de Seguridad de la Información.
- Organigrama y funciones del personal

5.6. Control de cumplimiento.

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

5.7. Finalización de contratos.

La finalización de contratos cuenta con un procedimiento en el cual se suprimen los privilegios de acceso del individuo a las instalaciones e información de la organización, a excepción de la considerada publica, una vez informado el individuo de su marcha y de su pérdida de privilegios, se verifica la devolución del material entregado y se le informa al resto de la organización, a los proveedores y entidades externas a e-certchile de que el individuo ya no representa a e- certchile.

## 6. Controles de seguridad técnica.

### 6.1. Generación del par de claves e instalación.

Los datos de creación de firma asociados a los certificados siempre son generados por un mecanismo que se encuentra bajo el exclusivo control del suscriptor, sea porque se creen y almacenen en un e-Token o en un dispositivo masivo criptográfico custodiado por e-certchile.

#### 6.1.1. eToken.

Los eToken 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 e-certchile cumplen con la norma FIPs-140-2 Nivel 3.

Lea cuidadosamente las indicaciones de generación de claves y almacenamiento de los datos de creación de firma.

#### 6.1.2. Custodia en dispositivo masivo criptográfico.

e-certchile permite que los suscriptores generen y almacenen sus datos de creación de firma en un dispositivo masivo criptográfico custodiado por e-certchile. El dispositivo cumple con la norma FIPs-140-2 Nivel 3.

El dispositivo masivo criptográfico se encuentra basado en hardware que genera, almacena y protege múltiples claves criptográficas. Por lo tanto, este Hardware está diseñado y certificado para almacenar y proteger los datos de creación de firma de los certificados de los suscriptores frente al acceso no autorizado de terceras personas a tales dispositivos criptográficos.

Con la finalidad de asegurar que sólo el respectivo suscriptor pueda utilizar sus datos de creación de firma el acceso a éstos se protege con un PIN y un segundo factor de seguridad, siendo deber del suscriptor custodiarlos.

6.2. Protección de la clave privada.

Respecto de la protección de los datos de creación de firma se debe considerar:

a. Protección del suscriptor: los datos de creación de firma deben ser protegidos permanentemente por el suscriptor, incluso si el certificado está suspendido.
b. e-certchile en ninguna circunstancia mantiene, custodia, protege o accede a los datos de creación de firma pertenecientes a un suscriptor, cuando estos han sido generados y almacenados en un eToken.
c. En el caso que el suscriptor haya escogido generar y almacenar sus datos de creación de firma en un dispositivo masivo criptográfico custodiado por e-certchile la activación de los datos de creación de firma solo será autorizada por el PIN y segundo factor de seguridad definidos por el suscriptor.

6.3. Otros aspectos de manejo de clases.

El cuidado de los datos de creación de firma deben ser una prioridad para el suscriptor, por lo que debe prevenir que ésta no sea vista al momento de ingresarla, ni copiarla del contenedor, ni adulterarla, para lo cual el suscriptor debe tener a lo menos las siguientes precauciones:

a. Mantener los datos de creación de firma bajo un PIN considerada segura, esto es de un mínimo de 6 y un máximo de 8 caracteres que idealmente no sea pronunciable, que contenga letras y números.
b. Mantener solamente registrado en la memoria el PIN utilizado para proteger los datos de creación de firma.
c. No copiar el PIN en un papel u otro medio fácilmente legible.
d. En caso de que utilice sea exigido por e-certchile un segundo factor de seguridad para proteger el acceso a los datos de creación de firma, mantenerlo permanentemente accesible.

6.4. Controles de seguridad computacional.

6.4.1. Seguridad de redes.

e-certchile limita el acceso de sus redes al personal debidamente autorizado. Para lograr ello, se implementan controles para proteger la red interna de acceso por terceras partes, los datos sensibles son cifrados al momento ser intercambiado a través de redes no seguras y se garantiza que los componentes locales de red están ubicados en entornos seguros.

6.4.2. Seguridad tecnológica.

e-certchile hace uso de procedimientos de pruebas y paso a producción de cualquier cambio que afecta al software de la certificadora. Estos cambios están regulados por un procedimiento de control de cambio administrado por la Gerencia de Operación, Seguridad y Tecnología. Asimismo, la aplicación del procedimiento para el almacenamiento seguro del hardware criptográfico y los materiales de activación se materializa después de la ceremonia de generación de claves.

6.4.3. Protección de la clave raíz.

El HSM en que se almacena la clave raíz, es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los HSM de e-certchile cumplen el estándar FIPS 140-2 Nivel 3.

La clave raíz utilizadas por e-certchile y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 3 personas de un total de 8 para modificar el ambiente criptográfico.

La clave raíz está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.

Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la clave raíz que se puede aplicar en caso de contingencia. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.

La clave raíz se crea en el módulo criptográfico HSM en el momento de su creación.

La clave raíz de e-certchile se activan mediante la inicialización del software de la certificadora y la activación del hardware criptográfico que contiene las contiene.

Un Administrador puede proceder a la desactivación de la clave raíz, mediante la detención del software de la certificadora.

Finalmente, existe un procedimiento de destrucción de la clave raíz.

## 7. Perfiles de certificados y CRL.

### 7.1. Perfil del certificado.

#### 7.1.1. Clases de certificados.

e-certchile siguiendo sus políticas, normas y procedimientos emite certificados de:

- Firma Electrónica Simple.
- Firma Electrónica Avanzada.
- Firma Electrónica Avanzada Auxiliar Administración de Justicia.
- Firma Electrónica Avanzada de un solo uso.
- Firma Electrónica Avanzada on-line.

#### 7.1.2. Contenido de los certificados.

Los certificados emitidos por e-certchile cumplen con lo establecido en el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y la Resolución Exenta N° 9, de 15 de Febrero del 2001, del Servicio de Impuestos Internos.

El contenido mínimo de los certificados es el siguiente:

a. Identificación de e-certchile y su clave pública.
b. Código de Identificación del Certificado.
c. Identificación del Suscriptor del Certificado (nombre, RUT y correo electrónico).
d. Clave pública del Suscriptor o bien un elemento de verificación de firma que corresponda a un elemento de creación de firma.
e. Algoritmo de firma del Suscriptor y de e-certchile.
f. Período de Validez del Certificado.
g. Referencia a la “CPS e-certchile”.

Tratándose de certificados de firma electrónica avanzada además contendrán los datos de la acreditación otorgada por la Entidad Acreditadora.

7.1.3. Vigencia de los certificados.

Los certificados emitidos por e-certchile pueden tener las siguientes vigencias.

- Firma electrónica simple: 1, 2 o 3 años.
- Firma electrónica avanzada.
  - Firma electrónica avanzada: 1, 2 o 3 años.
  - Firma electrónica avanzada Auxiliar Administración Justicia: 1, 2 o 3 años.
  - Firma electrónica avanzada de un solo uso: Un proceso de suscripción documental o 30 días contados desde la fecha de su emisión, con independencia de si se uso o no.
  - Firma electrónica avanzada on-line: 1, 2 o 3 años.

7.1.4. Caducidad.

Los certificados caducarán por el transcurso de su período de vigencia.

La caducidad de un certificado produce el término de la relación contractual entre el Suscriptor y e-certchile.

7.2. Perfil de CRL.

e-certchile mantiene publicado en www.e-certchile.cl un registro de acceso público de los certificados emitidos con expresa indicación de si se encuentran vigentes, suspendidos o revocados.

## 8. Administración de la CPS.

8.1. Procedimiento de Modificación de la CPS.

Las “CPS e-certchile” pueden ser modificadas cada vez que se estime necesario para asegurar que se mantengan tecnológicamente vigentes, así como, para alterar la forma en que se desarrolla la actividad por la introducción de mejoras en las instalaciones, sistemas, programas informáticos y los recursos humanos empleados por e-certchile.

Cualquier modificación que se haga a esta "CPS e-certchile" deberá tener una fecha de entrada en vigor no inferior a los 30 días desde la fecha en que se publica en www.e-certchile.cl.

8.2. Políticas de publicación y notificación.

La modificación de esta "CPS e-certchile" será notificada a los Suscriptores de certificados de e-certchile mediante correo electrónico enviado al correo contenido en el certificado de firma electrónico con 30 días de anticipación a la fecha en que entren en vigor las modificaciones introducidas.

El Suscriptor tendrá el plazo indicado para objetar la modificación, en cuyo caso los contratos firmados se entenderán resueltos.

Transcurrido dicho plazo sin que medie comunicación se entenderá que el Suscriptor acepta los cambios introducidos.

8.3. Procedimiento de aprobación de las CPS.

Cualquier nueva versión de una "CPS e-certchile" estará sujeta a un procedimiento de aprobación que considera:

- Elaboración y aprobación interna de la nueva ".
- Presentación de las "CPS e-certchile" al Directorio de e-certchile.
- Una vez pasada las aprobaciones anteriores, se publicarán las nuevas "CPS e-certchile" indicando la fecha de entrada en vigor.

Una vez publicadas las "CPS e-certchile" se informará de éstas a la Entidad Acreditadora.

| NORMA(S) QUE APLICA(N) | |
|---|---|
| **Norma** | **Referencia Normativa** |
| ISO 9001:2015 | 5.2 Política \| 8.2.2 Determinación de los requisitos relacionados con los productos y servicios |
| ISO 27001:2013 | 5.2 Política |
| Guía de Acreditación (Minecon) FEA | PO02 Declaración de Prácticas de Certificación – PO01 Política de Certificados de Firma Avanzada |
| Guía de Acreditación (Minecon) BIO | N/A |
| Guía de Acreditación (Minecon) TSA | N/A |

| CONTROL DE CAMBIOS | | |
|---|---|---|
| **N° DE VERSIÓN** | **FECHA** | **DESCRIPCIÓN DE CAMBIOS** |
| **0** | Julio/2020 | Creación del documento, se recomienda la lectura completa del documento |