PO02 – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

FIRMA ELECTRÓNICA AVANZADA

Versión	Realizado por	Revisado	Aprobado	Fecha
1.1	Encargado de Seguridad de la Información	Gerente de Operaciones	Gerente General	22-05-2024

CONTROL DE VERSIONES

Versión	Cambios de la versión	Fecha
0.0	Emisión del documento	04-02-2023
1.0	Formalización del Proceso.	03-07-2023
1.1	Se complementa respecto de privacidad y derechos de propiedad intelectual.	22-05-2024

Contenido

1. Introducción

Un Prestador de Servicios de Certificación (CA), por definición, es una institución o persona, ya sea pública o privada que presta servicios de firma electrónica y pueda emitir certificados, que expresamente actúa como tercera parte de confianza entre las personas o instituciones que participan en un acto de identificación, autenticación, firma y gestión documental, utilizando certificados digitales para firma electrónica.

Firma.digital posee dos instrumentos para gestionar su autoridad de registro, los cuales son la "CP" o las Políticas de Certificación y la "CPS" o Declaración de Prácticas de Certificación, definidos a continuación.

Política de Certificación (CP) es el conjunto de reglas de alto nivel, que definen los alcances de uso y aplicación de un certificado en un ecosistema de plataformas electrónicas, con requisitos de seguridad y utilización comunes, es decir, en general una CP o Política de Certificación define la funcionalidad según tipos de certificado para determinadas aplicaciones que exigen requisitos de seguridad y formas de usos.

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aún así es muy importante su interrelación.

Una Declaración de Prácticas de Certificación detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes. En definitiva, una Política define "qué" requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Prácticas de Certificación nos dice "cómo" se cumplen los requerimientos de seguridad impuestos por la Política.

1.1. Alcance

Detallar las condiciones de prestación de servicios de **Firma.digital**, para la emisión de sus certificados de Firma Electrónica Avanzada (FEA).

1.2. Glosario

- PSC: firma.digital, constituida legalmente como Trust Service Provider SpA, RUT 76.467.322-0
- Representación Digital: Es un documento representado en forma binaria, sin hacer referencia a su medio de almacenamiento o soporte, susceptible de ser firmado electrónicamente.

- Documento Electrónico: Es toda representación digital que dé testimonio de un hecho, una imagen o una idea.

- Firma Electrónica: El sustituto digital de la firma ológrafa que permite al receptor de un documento digital, verificar con certeza la identidad proclamada por el emisor del mismo, mantener la integridad del contenido del documento digital transmitido e impedir al signatario desconocer la autoría del documento digital o repudiarlo en forma posterior.

- Certificado Digital: Es un documento digital firmado y emitido electrónicamente por un Prestador de Servicios de Certificación, que asocia una clave pública con su titular durante el período de vigencia del certificado y que, debidamente almacenado y publicado en un repositorio o registro público electrónico, se utiliza como referencia para acreditar la identidad digital del contribuyente, que es titular de dicha clave, junto a sus datos de identificación, utilizando sistemas que garanticen la seguridad técnica y criptográfica de los procesos de certificación.

- Suscriptor: Es la persona que actúa en nombre propio o en el de otra persona natural o jurídica la que representa, y que, habiendo obtenido previamente un certificado digital de un Prestador de Servicios de Certificación debidamente acreditado ante el Servicio, tiene la capacidad de firmar un documento digital.

- Tercera parte interesada: cualquier persona que reciba documentos firmados por el suscriptor, utilizando un certificado digital emitido por la PSC, o que desee validar una firma electrónica emitida por la PSC.

- Clave Privada: Es aquella que se utiliza para firmar electrónicamente, utilizando un criptosistema asimétrico seguro.

- Clave Pública: Clave que es publicada y que al ser incorporada en un certificado digital válidamente emitido y almacenada en un repositorio, es utilizada para verificar las firmas electrónicas, basadas en su correspondiente o correlativa clave privada.

- Criptosistema Asimétrico Seguro: Es un método criptográfico que utiliza un par de claves compuesto por una clave privada utilizada para firmar electrónicamente y su correspondiente clave pública, utilizada para verificar esa firma electrónica, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desencriptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública.

1.3. Antecedentes

El modelo de Confianza adoptado por **Firma.digital** se basa principalmente, en implementar una infraestructura de confianza basada en PKI (Public Key Infraestcruture). Esta PKI utiliza tecnología estándar y segura basada en certificados compuestos de un par entre llave pública y llave privada.

El modelo de Confianza de **Firma.digital** se basa en el tercero que confía (Trusted Third Party). Esto hace que un tercer elemento, ya sea, persona, empresa o aplicación pueda confiar en otra sin necesidad que la conozca.

La Confianza se basa en la identificación, autenticación, integridad, privacidad y no repudio, por lo tanto, es necesario que el tercero que confía tenga la certeza de que el usuario es la persona que dice ser y que su identidad se encuentra correctamente registrada.

Por otro lado, es necesario que el tercero que confía tenga la certeza de que la información que recibe no ha sido modificada por ningún tercero, ya que esto podría generar una consecuencia jurídica para el tercero que confía.

La privacidad es una característica que permite al tercero que confía, tener la certeza de que la información recibida sólo puede ser leída por la persona autorizada, ya que de lo contrario, podría ser modificada por un tercero, generando una consecuencia jurídica.

2. Obligaciones y responsabilidades

2.1. Obligaciones

2.1.1. PSC (Firma.Digital)

a) Cumplir y respetar procedimientos de esta CPS y CP para emitir certificados.
b) Cumplir con las obligaciones establecidas en la Ley 19.799, Decreto Supremo 181/2002 del Ministerio de Economía, Fomento y Turismo y normas técnicas dictadas.
c) Aprobar o rechazar certificados solicitados, directa o indirectamente a través de autoridades de registro, según la CPS.
d) Apoyar la emisión de certificados con las tecnologías que permitan el resguardo de las llaves privadas de los suscriptores.
e) Configurar y mantener un Registro de Acceso Público de Certificados, con información del estado de éstos (vigente, suspendido o revocado), siempre en cumplimiento con las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada.
f) Notificar al suscriptor de la emisión de su certificado.
g) Notificar al suscriptor de la revocación o suspensión de sus certificados.
h) Realizar esfuerzos razonables para comunicar a los suscriptores cualquier hecho conocido por Firma.Digital que pueda afectar la validez del certificado.
i) Delegar la función de autoridad de registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.
j) Poner a disposición de los usuarios los certificados que componen la(s) cadena(s) de confianza de Firma.Digital.

2.1.2. Autoridad de registro (AR)

a) Comprobar fehacientemente la identidad de los solicitantes de un certificado de conformidad al procedimiento establecido en esta CPS, y en la Política de Certificación (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 la Política de Certificación (CP) y en especial en el artículo 12 letra b) de la Ley Nº19.799.
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) Aplicar medidas de seguridad adecuadas y suficientes para salvaguardar la llave privada del titular, al momento de generación del certificado.
f) Llevar a cabo cualquier otra función que le corresponda, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.
g) Obtener la aceptación en forma inequívoca de los términos y condiciones del servicio por parte del solicitante.
h) Prestar cualquier otro servicio que la PSC (Firma.Digital) le solicite.

Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro por cuenta y riesgo de la PSC (Firma.Digital).

2.1.3. Obligaciones del suscriptor

a) Solicitar la emisión del certificado aceptando los términos y condiciones descritos en esta CPS.
b) Elegir si los datos de creación de firma serán almacenados en un Token o en un dispositivo masivo criptográfico custodiado por Firma.Digital, estableciendo el PIN de protección de éstos. En el caso de elegir el almacenamiento en un dispositivo masivo criptográfico custodiado por Firma.Digital 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.
c) No revelar la clave privada ni el código de activación (PIN) del certificado.
d) 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 Firma.Digital, 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 Firma.Digital 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 Firma.Digital 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, la CPS y en la Política de Certificación (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 Firma.Digital 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 Firma.Digital así se lo solicite y haya sido revocado previamente el certificado.

2.1.4. Obligaciones de las terceras partes interesadas

Las terceras partes interesadas que decidan en forma libre y espontánea confiar y usar los certificados emitidos por la PSC (Firma.Digital), 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 generales

Los usuarios de los servicios de certificación de Firma.Digital se obligan a conocer y aceptar los términos, condiciones y límites contenidos en estas CPS y en la Política de Certificación (CP), los que en conjunto con la normativa vigente regulan la prestación de los servicios de certificación de firma electrónica.

2.2. Responsabilidades

2.2.1. PSC (Firma.Digital)

1. Emitir los certificados cumpliendo todas las exigencias establecidas en estas CPS y de conformidad con la información proporcionada por el suscriptor.
2. Que el certificado no contenga errores de transcripción de los datos proporcionados por el suscriptor durante el proceso de comprobación de la identidad.
3. Que la información incluida o incorporada por referencia en el certificado sea exacta.
4. Publicar el certificado en el registro de acceso público de certificados.
5. La aplicación correcta del procedimiento empleado.

Firma.Digital 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 Firma.Digital hubiera sido advertido de la posibilidad de producción de tales daños.

Firma.Digital 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.

Limitación de responsabilidad de Firma.Digital

Las responsabilidades que afectan la operación de Firma.Digital se encuentran limitadas a lo establecido en el artículo 14 de la Ley 19.799.
En todo caso, la responsabilidad de Firma.Digital cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a Firma.Digital, 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 Firma.Digital 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.

Fuerza mayor

Firma.Digital 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, dolo o culpa grave de la PSC.
Las obligaciones de Firma.Digital 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 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 labores del personal de Firma.Digital o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

2.2.2. Autoridad de registro (AR)

a) Comprobar la identidad del solicitante de acuerdo con esta CPS y la Política de Certificación (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 la Política de Certificación (CP).
c) Realizar con la diligencia y el debido cuidado las funciones que conforme a esta CPS le correspondan como Autoridad de Registro o que Firma.Digital le solicite.

2.2.3. Suscriptor

a) La veracidad de la información entregada a Firma.Digital 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 su certificado de FEA.
f) Indemnizar Firma.Digital 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.

2.2.4. 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.

2.3. Ley aplicable

2.3.1. Ley aplicable

Esta CPS y la Política de Certificación (CP) cumplen con las obligaciones establecidas por la Entidad Acreditadora y los requerimientos descritos en la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" – EA103 Versión 2.4, en la ley 19.799 de 2002, ley 19.799 de 2007, el Decreto 181 de 2002, que reglamenta la citada ley modificación del Decreto 181 de 2012, y a cualquier otro reglamento que modifique o complemente alguna de las leyes o decretos anteriores y las normas técnicas emanadas de la Subsecretaría de Economía y Empresas de Menor Tamaño, a través de su Entidad Acreditadora.

2.3.2. Separación y divisibilidad de cláusulas

En el evento que alguna disposición contenida en esta CPS o en las Políticas de Certificación (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.

2.3.3. 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 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 los convenios internacionales ratificados por el Estado chileno.
b) Lo establecido en esta CPS, en la Política de Certificación (CP) y en los contratos que se firmen entre Firma.Digital o sus autoridades de registro y el suscriptor.

Los certificados Firma.Digital no podrán ser alterados y deberán utilizarse tal y como son suministrados por Firma.Digital.

2.4. Tarifas

El solicitante se obliga a pagar a Firma.Digital y/o a las Autoridades de Registro las tarifas establecidas para los certificados cuya emisión se solicite.
El costo por la emisión o renovación de los certificados serán puestos a disposición de los solicitantes en www.firma.digital, donde se podrán establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

2.5. Publicaciones y repositorio

Firma.Digital mantiene permanentemente a disposición de cualquier interesado esta CPS en https://psc.firma.digital/cps

La información respecto al estado de vigencia de los certificados emitidos por Firma.Digital se encuentra disponible en el registro de acceso público de certificados, al que se puede acceder desde https://consulta-estado.firma.digital

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. Seguridad de los sistemas informáticos

La seguridad de los sistemas informáticos es continuamente revisada y mejorada tanto por equipos internos como por proveedores externos competentes en el campo de la seguridad informática. Lo anterior con el objetivo de dar cumplimiento a lo dispuesto en los requisitos de seguridad en los dominios PS01 al PS07, que determinan los niveles de seguridad que dispone el PSC.

2.7. Protección de datos personales

La información de los titulares de certificados es de carácter confidencial, salvo la contenida en el certificado digital, a la cual se podrá acceder mediante un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada y lo relativo al Titular en su rol de consumidor, las disposiciones de la ley N.º 19.496, Sobre Protección a los Derechos de los Consumidores.

2.8. Derechos de propiedad intelectual e industrial

Pertenece a Firma Digital, 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. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva del PSC sin la autorización expresa por su parte.

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

3. Identificación y Autenticación

3.1. Solicitud de certificado

La identificación de los solicitantes se realiza de conformidad con las normas y procedimientos establecidos en esta CPS y la Política de Certificación (CP) vigente.

La solicitud de un certificado de firma electrónica avanzada deberá realizarla el solicitante compareciendo en forma personal y directa a las oficinas de la autoridad de registro de Firma.Digital o a través de la página web de la PSC.

3.1.1. Validación de identidad del solicitante

La comprobación fehaciente de la identidad del solicitante de firma electrónica avanzada se realizará conforme a lo establecido en el Art. N° 12, letra e) de la Ley N° 19.799 y su Reglamento. En especial, el solicitante deberá concurrir presencialmente a las oficinas de Firma.Digital, presentando su Cédula Nacional de Identidad chilena.

El operador de AR pedirá al solicitante que presente su Cédula de Identidad Chilena, original y vigente . Con los datos de la CI se procederá a consultar la validación de los datos en el servicio de Registro Civil e Identificación. El solicitante deberá entregar todas las facilidades necesarias para la realizar las validaciones que correspondan, permitiendo comprobar fehacientemente su identificación.

3.1.2. Aceptación de la solicitud

Una vez superado el proceso de comprobación de solicitud de forma satisfactoria, siempre y cuando no existan circunstancias que de alguna manera afecten a la seguridad del servicio de certificación, la AR procederá a la aprobación de la solicitud.

3.1.3. Rechazo de la solicitud

En el caso que el proceso de comprobación de identidad no sea superado satisfactoriamente, debido a que la documentación del suscriptor no esté vigente, o que no concuerdan todos los antecedentes, o cualquier otra causal por la que el suscriptor no cumpla con los requisitos establecidos, la solicitud será rechazada.

3.2. Solicitud de suspensión y revocación

La solicitud de suspensión o revocación podrá ser realizada por el suscriptor:

- **Vía email**: La solicitud de revocación o suspensión podrá ser realizada por el suscriptor a través de un email a la dirección de correos de soporte@firma.digital, indicando motivo, nombre completo, RUN y firmada con el certificado digital que se desea revocar. Luego de esta solicitud, el suscriptor deberá concurrir a las oficinas de Firma Digital con su cédula de identidad vigente, para ratificar su solicitud, en un plazo no mayor a 48 hrs hábiles, desde que inició el trámite.
- **Revocación presencial**: Si el suscriptor no tiene acceso al su certificado digital, o no logra aportar los antecedentes necesarios, deberá acudir a las oficinas de Firma Digital con su cédula de identidad vigente, para llenar el formulario de revocación, una vez completado el formulario, se validará la identidad de la persona a través de validación de identidad.

Una vez revocado o suspendido el certificado digital el suscriptor será notificado de la revocación.

Firma Digital no soporta la revocación o suspensión por otros medios tales como: teléfono, facsímil, cartas, u otros. Deberá comparecer en forma personal y directa ante la AR de Firma Digital, donde se validará su identidad de acuerdo al procedimiento descrito en el punto 3.1.1.

3.3. 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 la PSC de Firma Digital.

A. Con certificado de firma electrónica avanzada vigente. En este caso, el suscriptor podrá solicitar la renovación directamente en la web https://www.firma.digital utilizando para ello el certificado digital y la clave secreta asignada, la cual es solicitada por el navegador web en el proceso de verificación de identidad, junto a otros elementos como verificación de cédula de identidad, email a modo de asegurar que el suscriptor es el mismo que tiene en poder el certificado digital válido previamente emitido.

B. Sin certificado de firma electrónica avanzada vigente. En este caso, el suscriptor deberá comparecer de forma personal y directa ante la AR de Firma Digital para hacer la solicitud, donde se validará su identidad de acuerdo al procedimiento descrito en el punto 3.1.1.

4. Requerimientos operacionales

4.1. Emisión del certificado

Una vez que todos los antecedentes del solicitante sean aprobados por Firma Digital, la AR generará y ejecutará el procedimiento técnico para emitir certificado, cumpliendo con la generación de clave privada dentro de un dispositivo de almacenamiento seguro (token FIPS 140-2 nivel 3) del suscriptor, protegiendo el contenido mediante PIN, siendo de carácter personal e intransferible a nombre del suscriptor.

El suscriptor puede delegar la custodia de la clave privada de su certificado en la PSC, la que dispondrá de un HSM que cumpla con los mismos estándares FIPS 140-2 nivel 3, aplicando mecanismos y procedimientos seguros para la emisión y posterior uso de las claves, los que tendrán las siguientes características:

- Se aplicarán los procedimientos técnicos pertinentes al dispositivo criptográfico utilizado para asegurar que la clave privada nunca estará expuesta, generando en el dispositivo criptográfico en modo no exportable y protegiéndola con un PIN de exclusivo dominio del suscriptor.
- Se aplicará un mecanismo de transporte encriptado del PIN del suscriptor mediante claves RSA emitidas dentro del dispositivo criptográfico, para la comunicación entre el dispositivo criptográfico y la aplicación o servicio de captura del PIN, tanto para su establecimiento como uso posterior.
- El dispositivo criptográfico tipo HSM no deberá estar expuesto a la red pública.
- Las aplicaciones o servicios que con posterioridad requieran el uso de la clave privada deberán contar con una autorización del suscriptor mediante su PIN y proveerán a la PSC toda la documentación y evidencia necesaria para la certificación del cumplimiento del procedimiento de su captura y transporte.

4.2. Aceptación del certificado por parte del suscriptor

Se entiende que un certificado ha sido aceptado por el suscriptor una vez que este haya sido disponibilizado por Firma Digital, aún cuando el certificado no haya entrado en vigencia.

4.3. Vigencia del certificado

Todos los certificados se consideran vigentes desde el momento de su emisión y hasta la fecha de 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.

4.4. Suspensión y Revocación de certificados

4.4.1. Suspensión de certificados

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

A. Solicitud del suscriptor
B. Decisión de la PSC en virtud de razones técnicas o de seguridad

4.4.2. 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. El certificado no será revocado.

4.4.3. Término de la suspensión

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

A. Por la decisión de la PSC de revocar el certificado, en los casos previstos en la Ley.
B. Por la decisión de la PSC de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.
C. Por la solicitud del titular del certificado, cuando la suspensión haya sido solicitada por éste.

4.4.4. Revocación de certificados

La revocación de un certificado de firma electrónica avanzada se podrá llevar a cabo cuando la PSC logra constatar las siguientes causas:

- Solicitud del suscriptor.
- Pérdida del certificado o alteración del elemento donde almacena el certificado.
- Fallecimiento del suscriptor.
- Por alguna eventualidad que comprometa la llave privada del suscriptor, ya sea por robo, alteración, divulgación o cualquier otro tipo de causal circunstancial.
- Por incumplimiento de suscripción, por parte de la CA o el suscriptor.
- Por resolución judicial o administrativa.
- Por incumplimiento del Acuerdo de Suscriptor o de cualquiera de las obligaciones del suscriptor contenidas en las CPS.

4.4.5. Efectos de la revocación

El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de éste, conforme a los usos que le son propios e impide el uso legítimo del mismo.

4.4.6. 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 la PSC 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 ésta, mantiene vigente el certificado por todo el tiempo que resta hasta su fecha de término de vigencia original.

4.4.7. Procedimiento para suspender o revocar un certificado

La suspensión o revocación se efectuará tal cual es descrita en el presente documento, y en particular en el párrafo 3.2.

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

4.5. Renovación de certificados

La renovación de los certificados, es un proceso comercial, que se produce cuando un certificado digital vigente previamente emitido, se encuentra próximo a expirar y el suscriptor desea continuar usando el servicio, a través de la obtención de un nuevo certificado digital.

Para renovar el servicio de certificado digital, el suscriptor deberá presentar una nueva solicitud de certificado, en la forma establecida en el apartado 3.3.

Firma Digital podrá enviar al suscriptor, a su correo electrónico 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.

4.6. Procedimiento de auditoría de seguridad

Firma Digital es inspeccionada 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.

Asimismo, anualmente audita sus políticas y procedimientos de seguridad, para verificar que se mantengan actualizados y en ejecución.

4.7. Archivo de registros

Firma Digital 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 del suscriptor. 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.

4.8. Término de la PSC por cese voluntario o cancelación

Se podrán dar por terminadas las actividades de certificación de la PSC por cese voluntario en su actividad o por cancelación de la inscripción en el registro de prestadores acreditados por la Entidad Acreditadora, según indican incisos c) y h), respectivamente, del Artículo 12 de la Ley Nº19.799.

En tales circunstancias, la PSC comunicará la situación a los suscriptores con una antelación de al 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. Controles de Procedimiento, Personal y Físicos

5.1. Controles de Procedimientos

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

5.1.1. Segregación de funciones

La PSC cuenta con una matriz de segregación de funciones según las restricciones de seguridad definidas en la Política General de Seguridad y en la respectiva Política de Seguridad del Personal.

Existen dos niveles de personal, de acuerdo a las citadas restricciones de seguridad:

Personal Sensible:

Todo aquel rol y/o cargo que está relacionado con la emisión de certificados digitales, el acceso a sistemas de información críticos o el acceso a activos críticos. Esto es: Gerentes, Jefaturas, Personal del Área Operaciones, Oficial de Seguridad, Personal del Área Administración y Finanzas, Área Legal y todo aquel que por sus funciones y/o actividades tenga relación con la emisión de certificados digitales, el acceso a sistemas de información crítica o el acceso a activos críticos.

Personal General:

Todo aquel rol y/o cargo que no está relacionado con la emisión de certificados digitales, el acceso a sistemas de información críticos o el acceso a activos críticos. Por ej. Personal de áreas de Marketing, Televentas, Consultores, Vendedores.

5.1.2. Comité de Seguridad de la Información

Firma Digital ha establecido un Comité de Seguridad de la Información que sesiona regularmente con el fin de evaluar y sancionar sobre las políticas y acciones relevantes en el ámbito de la seguridad de la información.

5.1.3. Procedimientos de difusión interna

Firma Digital comunica a las personas de la organización, la información definida por el Sistema de Gestión de Seguridad de la Información, pudiendo ser políticas y/o procedimientos relevantes para cada individuo de la organización.

5.1.4. Auditorías

Con el fin de velar por el correcto uso de los recursos de su propiedad, Firma Digital podrá ejecutar auditorías sin previo aviso, revisiones del cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

En referencia a las revisiones de la seguridad de la información, se consideran revisiones independientes, evaluaciones del cumplimiento de las políticas y normas de seguridad y evidencia que compruebe el cumplimiento.

5.2. Controles de Personal

5.2.1. Requerimiento de antecedentes y experiencia

Firma Digital 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.
- Experiencia 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.

5.2.2. Comprobación de antecedentes

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

5.2.3. Roles de confianza

Los roles de confianza de la PSC son aquellos relacionados con la emisión de certificados digitales, el acceso a sistemas de información críticos o el acceso a activos críticos. Esto es: Gerentes, Jefaturas, Personal del Área Operaciones, Oficial de Seguridad, Personal del Área Administración y Finanzas, Área Legal y todo aquel que por sus funciones y/o actividades tengan relación con la emisión de certificados digitales, el acceso a sistemas de información crítica o el acceso a activos críticos.

5.2.4. Formación y entrenamiento

Los colaboradores de Firma Digital son entrenados en los aspectos de las políticas y procedimientos de seguridad, así como en lo que respecta a requerimientos de seguridad, responsabilidades legales y controles vigentes, herramientas de trabajo, aplicaciones, etc., antes de autorizar su acceso a información.

Los programas de capacitación deben abordar los elementos relevantes para el entorno particular de la persona que está siendo entrenada, incluyendo:

- Principios y mecanismos de seguridad.
- Procedimientos de seguridad asociados a los colaboradores, según área.
- Presentación y manejo de informes de Incidentes.
- Procedimientos de recuperación de desastres y continuidad de negocio.

5.2.5. Requerimientos de contratación

Como parte de los requerimientos de contratación, todo colaborador de la PSC debe firmar un acuerdo de confidencialidad incluido en su contrato.

5.2.6. Término de los contratos

El término de los 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 pública, 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, de ser necesario se notificará a proveedores y entidades externas a Firma Digital de que el individuo ya no representa a Firma Digital.

5.2.7. Procedimiento de verificación de antecedentes

La PSC lleva a cabo revisiones de antecedentes del personal que tiene la calidad de personal sensible o crítico, similar al realizado al momento de su contratación.

La verificación de antecedentes se realiza al menos cada tres (3) años.

Los informes que contienen dicha información deben ser evaluados por el Oficial de Seguridad, quien debe tomar acciones que sean razonables en función de la naturaleza, magnitud y frecuencia de la conducta descubierta por la verificación de antecedentes.

Estas acciones pueden incluir medidas que pueden llegar incluso hasta el término del contrato de trabajo para personal crítico o sensible.

5.2.8. Requisitos de contratista independiente

La PSC puede permitir que contratistas o consultores independientes puedan convertirse en personal sensible o crítico, bajo las siguientes condiciones:

- Se consulte la decisión al Oficial de Seguridad
- Los contratistas o consultores sean de confianza para la entidad en la misma medida como si fueran empleados, habiéndose realizado la misma verificación de antecedentes utilizada para los empleados de la PSC.

De lo contrario, los contratistas y consultores independientes tendrán acceso a dependencias seguras de la PSC sólo en la medida en que son acompañados y supervisados directamente por personal de la organización.

5.3. Controles Físicos

La PSC ha documentado controles físicos detallados y políticas de seguridad de las instalaciones donde se realiza físicamente la operación de la organización. Al menos anualmente se audita el cumplimiento de los controles señalados.

5.3.1. Ubicación de las dependencias físicas

Todas las operaciones de la PSC se llevan a cabo dentro de un ambiente protegido físicamente, que permita disuadir, prevenir y detectar usos no autorizados de acceso o divulgación de información sensible y sistemas.

Tales requerimientos se basan en parte en el establecimiento de niveles de seguridad física.

Un nivel es una barrera, tal como una puerta cerrada o puerta que exige control de acceso obligatorio para las personas y requiere una respuesta positiva para cada persona, que desea pasar a la siguiente zona. Cada nivel

sucesivo proporciona un acceso más restringido y mayor seguridad física contra la intrusión o acceso no autorizado.

6. Controles de Seguridad Técnica

6.1. Manejo de llaves

6.1.1. Generación de llaves de la CA

Se utiliza un dispositivo HSM para el resguardo de las llaves de la CA raíz y la CA de Firma Electrónica Avanzada, el cual cumple con el estándar FIPS 140-2 nivel 3. Para resguardar la integridad y confidencialidad de la parte privada de los certificados, la ceremonia de inicialización del HSM y la generación de la llave de la CA raíz internamente en el HSM fue llevado a cabo en un sitio privado, que cuenta con medidas de control de acceso adecuadas. El acta de inicialización y creación de la clave raíz asegura que las claves se crearon en forma fiable, asegurando en todo momento la seguridad de las claves privadas, cumpliendo con el estándar FIPS 140-2 nivel 3 y con ETSI TS 102 042. Las llaves creadas hacen uso del algoritmo de firma SHA-256, y del algoritmo de cifrado RSA con clave de largo 2048 bits, ambos reconocidos por la industria.

6.1.2. Almacenamiento, respaldo y recuperación de la llave privada

Las claves privadas de los certificados CA raíz y de la CA de Firma Electrónica Avanzada se almacenan durante todo su ciclo de vida en un dispositivo criptográfico (HSM) que cumple con el estándar FIPS 140-2 nivel 3. Las llaves privadas son respaldadas en caso de contingencia.

6.1.3. Distribución de la llave pública

Los componentes públicos de las llaves CA raíz y CA de Firma Electrónica Avanzada se encuentran disponibles para el acceso público en el sitio web de https://psc.firma.digital, y además son entregadas a la Entidad Acreditadora de manera de cumplir con el modelo de confianza que requiere la regulación existente.

6.1.4. Uso de la llave privada

Firma.digital ha definido controles para el uso de la llave de la CA raíz donde se define que sólo puede ser usada para firmar CA's intermedias y no puede ser utilizada para emitir otro tipo de certificados. El repositorio de la CA raíz está resguardada de modo que no es posible acceder a ella desde redes no autorizadas.

De acuerdo a la norma vigente el uso de la llave de la CA de Firma Electrónica Avanzada puede ser utilizada sólo para firmar certificados de usuario final del tipo firma electrónica y para emitir información relacionada con la revocación de certificados.

6.2. Riesgos

La PSC cuenta con una política para detectar oportunamente los riesgos que pueden afectar a TSP, que permitan generar estrategias que se anticipen a ellos y mantener la continuidad del negocio asegurando la adaptabilidad a los cambios del entorno.

6.2.1. Principios de gestión del riesgo

Todos los colaboradores en la PSC son responsables de la identificación y comunicación de los riesgos asociados al desempeño de sus labores. Para la PSC prevalecen la prevención y el autocontrol como mecanismos principales de un oportuno tratamiento a los aspectos que significan vulnerabilidad.
La gestión de riesgos es un proceso orientado a la generación de valor, y conducir las decisiones respecto al

riesgo de acuerdo con niveles establecidos y previamente aceptados por la PSC.
La gestión de riesgos prioriza los niveles de exposición y las consecuencias por su materialización y define su tratamiento en función de estas variables.
La gestión de riesgos de la PSC se integra con las políticas y procesos de la organización; por lo tanto, en todo nuevo proceso que pretenda incorporarse, se debe verificar que el mismo sea coherente con esta política.

Los riesgos se clasifican de acuerdo con su severidad sobre aspectos económicos o financieros, reputacionales o de imagen, seguridad, humanos y sobre la información.
El proceso de gestión de riesgos de la PSC, incluye las siguientes etapas:

- **Contexto**: Corresponde a una primera etapa donde las situaciones identificadas encajan en la realidad de la PSC. Al contextualizar los riesgos u oportunidades es posible desarrollar las actividades siguientes con mayor facilidad.
- **Identificación**: Es una etapa fundamental, que permite a la PSC listar, entender y definir sus riesgos.
- **Análisis**: Una vez identificados los riesgos se debe asociar a estos, información sobre su frecuencia, es decir cada cuanto ocurre el hecho identificado; su severidad, es decir las consecuencias que ese hecho tiene sobre la PSC en términos económicos, de imagen, seguridad y de la información y se debe determinar entonces la probabilidad de ocurrencia.
- **Plan de Respuesta**: la PSC según la evaluación de riesgos, deberá definir Responsables, Acciones y Estrategias para Evitar, Mitigar, Transferir o Aceptar los riesgos identificados.
- **Monitoreo y Evaluación**: Registrar y actualizar los riesgos y su calificación, informar periódicamente los resultados sobre la gestión de riesgo que realiza cada área de la PSC.
- **Comunicación**: la PSC garantiza los mecanismos para que la información de este proceso fluya adecuadamente dentro de la PSC y sea escuchada por instancias superiores.

6.3. Plan de Seguridad

El Plan de Seguridad permite trabajar en el transcurso del año en aquellos ámbitos de acción establecidos, con el objetivo de proveer protección a los recursos de información, según lo definido en PS02 Política de Seguridad de Información de la organización y en el PS04 - Plan de Seguridad de la Información.

6.4. Plan de Administración de llaves

En el documento PS06 Plan de Administración de Llaves se definen las acciones sobre las llaves criptográficas de Firma Digital, con el fin de resguardarlas y administrarlas durante su ciclo de vida.

6.5. Mantención de la infraestructura

Firma Digital cuenta con servicios de infraestructura contratados a un proveedor que cumple con los requisitos mínimos exigidos por la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” publicados por la Entidad Acreditadora del Ministerio de Economía en su versión vigente.

6.6. Control de acceso

En Firma Digital el control de acceso a la información es de alta importancia, por lo que se regula en base a lo establecido en la “Política de Control de Accesos”.

7. Perfiles de certificados y registro de acceso público

7.1. Contenido del certificado

Los certificados de la CA de Firma Digital están basados en la estructura x509 v3 y cumplen con lo establecido en el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo

El contenido mínimo de los certificados es el siguiente:

A. Identificación de Firma Digital y su clave pública.
B. Código único de Identificación del certificado.
C. Identificación del Suscriptor del Certificado (nombre, RUN, correo electrónico y país).
D. Clave pública del Suscriptor.
E. Algoritmo de firma del Suscriptor y de Firma Digital.
F. Período de Validez del Certificado.
G. Referencia a esta CPS. Tratándose de certificados de firma electrónica avanzada además contendrán los datos de la acreditación otorgada por la Entidad Acreditadora. Vigencia de los certificados

Los certificados emitidos por Firma Digital tendrán una duración de 1, 2 ó 3 años.

7.2. 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 Firma Digital.

7.3. Listas de certificados emitidos por Firma Digital

Firma Digital mantiene publicado en https://consulta-estado.firma.digital un registro de acceso público de los certificados emitidos con expresa indicación de si se encuentran vigentes, suspendidos o revocados.

A su vez publicará cada 24 una CRL actualizada con la lista de certificados revocados, la cual puede ser consultada en http://crl.firma.digital/firmadigitalFEA-G1.crl.

8. Confidencialidad

La PSC garantiza que la información solicitada a los usuarios en la página web de la empresa es mantenida por la misma para los fines de informativos y no se divulga a terceras partes. La información recopilada de los usuarios b

ajo ningún punto de vista es compartida, vendida, cedida, o transferida a terceros, salvo autorización expresa del usuario.

Con el fin de impedir un acceso no autorizado, mantener la exactitud de los datos y salvaguardar la confidencialidad de los datos personales de los usuarios, se han dispuesto procedimientos físicos, electrónicos y administrativos apropiados para proteger y asegurar la información que se procesa y almacena en bases de datos, pudiendo estar datos estadísticos o paramétricos disociados del identificador principal del titular. Entre estas medidas se encuentra la limitación de acceso a los datos a los colaboradores de la empresa, proveedores y/o contratistas autorizados que necesitan conocer la información para poder operar o mejorar los servicios.

En base a la ley N° 19.628, el usuario en todo momento podrá:

- Solicitar información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.
- Solicitar que se modifiquen sus datos personales cuando ellos no sean correctos o no se encuentren actualizados, si fuere procedente.
- Solicitar la eliminación o cancelación de los datos entregados cuando su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

9. Derechos de propiedad intelectual

Queda expresamente prohibido a cualquiera de las partes involucradas, sea Solicitante, Titular, terceros, u otros, controlar, interferir, realizar ingeniería inversa, o cualquier otro acto que afecte la ejecución técnica de los sistemas, la propiedad intelectual de la PSC, en particular respecto de los desarrollos informáticos utilizados para emitir y administrar los certificados digitales.

10. Administración de la CPS

Las Prácticas de Certificación de la PSC Firma Digital es revisada en forma anual, teniendo en consideración los cambios en la regulación, en el personal, las tecnologías y los requerimientos del servicio.

10.1. Procedimiento de modificación de la CPS

Firma Digital podrá modificar las estipulaciones de la presente CPS y CP específicas, cada vez que:

- Se estime necesario para asegurar que se mantengan tecnológicamente vigentes y mejorar el ejercicio de la actividad de certificación, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación.
- Existan incidentes de seguridad que así lo aconsejen.
- Entren en vigencia modificaciones normativas que requieran su modificación.
- Surjan necesidades de negocio que requieran cambios al texto de dichos documentos.

Las modificaciones a la CPS y CP, serán aprobadas por el Comité de Seguridad de la organización, publicadas en el sitio web de la PSC, indicando la fecha de entrada en vigencia. Una vez sean publicadas, se informará a la Entidad Acreditadora del Ministerio de Economía.

10.2. Procedimiento de publicación de la CPS

Las modificaciones efectuadas sobre la CPS o la CP se darán a conocer a los interesados, en la página web pública de la PSC https://psc.firma.digital/politicas/versiones donde se incluirá un listado de las sucesivas versiones de estos documentos con una antigüedad de hasta a 1 año.

10.3. Procedimiento de notificación de las publicaciones

La modificación de esta CPS será notificada a los suscriptores de certificados de Firma Digital mediante correo electrónico, enviado al correo contenido en el certificado de firma electrónica, con 15 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.

11. Referencias

Cómo referencia se consideraron las principales normas técnicas registradas por la Entidad de Acreditación, vinculados desde https://www.entidadacreditadora.gob.cl/normas-tecnicas/

- ETSI TS 102 042 V1.1.1 (2002-04). Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06) .RTS/ESI-000043.Keywords e-commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05). Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).
- NCh.2820/1.Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general.
- NCh2832.Of2003 Tecnología de la información – Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
- RFC 2559 BOEYEN, S. et al., “Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2”, Abril 1999.
- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical.