PO01 – POLÍTICA DE CERTIFICACIÓN FIRMA ELECTRÓNICA AVANZADA

Versión	Realizado por	Revisado	Aprobado	Fecha
1.0	Encargado de Seguridad de la Información	Gerente de Operaciones	Gerente General	01-06-2023

CONTROL DE VERSIONES

Versión	Cambios de la versión	Fecha
1.0	Emisión del documento	01-06-2023

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.

2. Alcance

Este documento contiene las reglas de alto nivel, que definen los alcances de uso y aplicación de un certificado digital emitido por la PSC, a través de cualquiera de sus CA, con requisitos de seguridad y utilización comunes.

3. 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.

- **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.

3.1. Titulares (Suscriptores)

Los titulares o suscriptores de un certificado digital son aquellas personas naturales que solicitan, a través de la presentación de antecedentes ante la respectiva autoridad de registro, y se les emite un certificado para firma electrónica, el cual es aceptado por el solicitante.

4. Procedimiento de registro

4.1. Características del procedimiento

El registro es el procedimiento que entrega suficientes garantías de la identidad y autenticación del solicitante del certificado digital. En caso de ser necesario, se podrá requerir uno o más de mecanismos complementarios de autentificación digital de comprobación de identidad. Además, se exigirá que el solicitante haya generado o almacenado la llave privada en un dispositivo acreditado mediante estándar FIPS-140-2 nivel 3.

El procedimiento debe:

- Garantizar que la información suscrita en el certificado es exacta y fiel reflejo de la información entregada por el suscriptor en el acto de emisión del certificado, utilizando si es necesario todas las herramientas de verificación a su alcance.
- Hacer uso de la tecnología adecuada, tanto en Hardware como Software, para la emisión de los certificados.
- Informar preventivamente la proximidad de la caducidad de los certificados.
- Disponer la revocación de los certificados que no cumplan con las prácticas adecuadas de firma electrónica, o a petición del suscriptor.
- Disponibilizar lista de certificados revocados, la cual debe ser constantemente actualizada.
- Poseer procedimientos y políticas adecuadas para el resguardo de la llave privada del suscriptor.

4.2. Solicitud de certificado

La solicitud de un certificado de firma electrónica avanzada debe ser realizada por el solicitante mediante un procedimiento que permita identificarlo, al menos formalmente.

4.3. Validación de identidad

Deberá comprobarse fehaciente la identidad del solicitante de firma electrónica avanzada, conforme a lo establecido en el Art. N° 12, letra e) de la Ley N° 19.799 y su Reglamento. Esto podrá ser realizado mediante la comparecencia personal del solicitante a las oficinas de Firma.Digital, a un notario u oficina del Servicio de Registro Civil e Identificación.

5. Tipos y usos de certificados

Firma.digital emite certificados de firma electrónica avanzada compatibles con el estándar ISO/IEC 9594-8, cuya estructura y contenido cumple con el Reglamento de la Ley 19.799.

La estructura contiene al menos los siguientes datos:

- RUT del suscriptor.
- Correo electrónico del suscriptor.
- Nombre completo del suscriptor.
- Tipo y usos de certificado.
- Datos del emisor Firma.digital.

Estos certificados podrán ser utilizados para:

A. Firmar documentos electrónicos

B. Identificar la identidad del suscriptor ante instituciones o empresas.

C. Autenticarse en sistemas.

6. Obligaciones CA, RA, titular y receptor

6.1. Obligaciones de la CA

Los certificados digitales, se organizan en una jerarquía de confianza, denominada cadena de certificación, comenzando desde la CA raíz o Root CA, esto permite ser utilizado para firmar los certificados de las entidades certificadoras subordinadas o Sub CA necesarias, en estos términos Firma.digital se define como entidad raíz y una entidad intermedia, porque ha emitido un certificado par ser utilizado por el mismo para su cadena de certificación.

En el caso que otras entidades de certificación se quieran subordinar (Sub CA) a la jerarquía de certificación de Firma.digital, éste último firmará los certificados emitidos.

Se considerarán al menos las siguientes obligaciones por parte de la CA:

- Identificar y autenticar correctamente al suscriptor o usuario de firma electrónica usando correctamente los procedimientos de CA para estos efectos.
- Controles de Seguridad Física.
- Emitir certificados a quienes lo soliciten.
- Administrar un sistema tipo infraestructura de llaves públicas (PKI) para hacer operativa la certificación digital.
- Emitir y mantener una lista de certificados revocados.
- Emisión de Certificados:
    - Firma.digital emitirá certificados que sean solicitados previa validación y aprobación de los antecedentes necesarios de una persona natural.
- Administración de llaves:
    - Firma.digital puede emitir, de forma automática o gestionada, la llave pública y privada que se le entrega al titular, o manual dentro de un dispositivo seguro de almacenamiento, garantizando en ambos casos la confidencialidad de la llave privada.

- Firma.digital puede almacenar la llave privada de un titular, bajo su expreso consentimiento y autorización dentro de un dispositivo de almacenamiento seguro permitido, cumpliendo los mismos estándares de seguridad y asegurando mediante los mecanismos adecuados que solo el titular tendrá acceso a su llave personal.

- Si decide dar término a sus funciones de firma electrónica avanzada, dará a conocer su decisión a todos sus suscriptores activos, y en lo posible, transferir todos sus certificados a otro prestador de firma electrónica compatible. Los suscriptores pueden negarse a dicha transferencia, en cuyo caso el certificado quedará en estado revocado.
- Debe conservar registros de todos sus certificados emitidos y revocados durante el período que exige y que rige la actividad de firma electrónica avanzada, ley Nº 19.799. Este registro estará disponible para el acceso público en el sitio web firma.digital.

6.2. Obligaciones del suscriptor

Se considerarán al menos las siguientes obligaciones por parte del suscriptor:

- Conservar y dar uso adecuado al certificado digital, según lo descrito en el contrato de suscripción.
- Dar correcta custodia al certificado, resguardar su clave privada y no dar mal uso al mismo.
- Proteger el uso de su certificado mediante PIN o autorizar su custodia a la PSC en dispositivos de almacenamiento seguro, que cumplan con estándares de confianza mínimos al suscriptor.
- Informar a Firma.digital inmediatamente por cualquier situación que afecte directamente la validez del certificado, o si su clave privada se ve comprometida.
- Entregar toda la información de identificación personal o de su empresa que se le solicite, a través de cualquier medio, tecnología o evidencia que se necesite para su correcta identificación y validación.
- El solicitante deberá cancelar la tarifa establecida y publicada en la página web https://firma.digital por el certificado que solicite.

6.3. Obligaciones de los terceros que confían

Los terceros que confían están obligados a:

- Que el certificado que utilizó en la firma del documento electrónico haya estado vigente al momento de la firma.
- Que el certificado utilizado para firmar no haya sido revocado, para lo cual podrá utilizar la Lista de certificados revocados (CRL) o el servicio de OCSP

7. Declaración de las garantías, seguros y responsabilidades de las partes

7.1. Garantías

La organización responsable de la Política tiene las siguientes obligaciones, de acuerdo a esta Política, las Declaraciones de Prácticas de Certificación, y la normativa vigente:

a. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma español.
b. Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto. A dicho registro podrá accederse por medios electrónicos de manera continua y regular.
c. Conservar los datos del registro público antes señalado por a lo menos durante seis años desde la emisión inicial de los certificados.
d. En el caso de cesar voluntariamente en su actividad, deberá comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por la organización y, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.
e. Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten.
f. En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica.
g. Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores.
h. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vaya a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.
i. En caso de cancelación de la inscripción en el registro de prestadores acreditados, comunicar inmediatamente esta circunstancia a cada uno de los usuarios y traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere.

j. Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos.

k. Cumplir con las demás obligaciones legales, especialmente las establecidas en la ley N° 19.799, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.

7.2. Eximentes de responsabilidad

En ningún caso la Autoridad Certificadora será responsable de los daños que tengan origen en el uso indebido o fraudulento de un certificado de Firma Electrónica.

Un certificado de Firma Electrónica provisto por la Autoridad Certificadora podrá establecer límites en cuanto a los posibles usos del certificado, en cuyo caso, la Autoridad Certificadora quedará eximida de cualquier responsabilidad por el uso que se dé a dichos certificados y que excedan tales límites.

La Autoridad Certificadora quedará exenta de responsabilidad en caso de guerra, pandemia, desastres naturales o cualquier otro caso de fuerza mayor.

La Autoridad Certificadora no será responsable de los daños derivados de la ejecución defectuosa u omisión de las obligaciones que corresponden al solicitante, suscriptor y/o usuario.

La Autoridad Certificadora no será responsable de la incorrecta utilización de los certificados y las llaves, ni de cualquier daño indirecto que pueda resultar de la utilización del certificado, o de la información suministrada por la Autoridad Certificadora. En particular, el lucro cesante y la pérdida de ingresos o pérdida de datos serán considerados daños indirectos y no darán lugar a indemnización alguna.

La Autoridad Certificadora no será responsable de los daños que se deriven de aquellas operaciones en que se hayan superado las limitaciones de uso que se señalan en estas políticas y las correspondientes Prácticas de Certificación de cada tipo de certificado.

La Autoridad Certificadora no será responsable de las eventuales inexactitudes en el certificado producto de errores en la información que haya sido presentada por el solicitante en su solicitud de certificado.

7.3. Responsabilidades Financieras y Coberturas de Seguros

Firma Digital deberá mantener un nivel razonable de cobertura de seguro por errores y omisiones, ya sea mediante un programa de errores y omisiones de seguros con una compañía de seguros, o una retención auto-asegurada.

7.4. Indemnización por parte de los Suscriptores

En la medida que la legislación lo permita, los suscriptores tienen la obligación de indemnizar a la Autoridad Certificadora, en caso de:

- Falsedad o tergiversación de los hechos relativos a las solicitudes de certificados digitales.
- Incumplimiento por parte del suscriptor en el hecho de transparentar información en la solicitud de certificado, si la falsedad y omisión es consecuencia de negligencia, o con intención de dolo a

cualquiera de las partes que forman parte de la cadena de confianza, Autoridad Certificadora o terceros que confían.

- Fallas en la protección de la llave privada, o para tomar las debidas precauciones necesarias para evitar perjuicios, pérdida o divulgación de la llave privada del suscriptor.
- Infracciones en derechos de propiedad intelectual de la Autoridad Certificadora.

8. Protección de información

Toda la información entregada por los clientes a Firma.digital es de carácter confidencial y la PSC no utilizará esta información en otros aspectos que sean exclusivamente relacionados con sus actividades de certificación. La entrega de esta información a terceros está estrictamente regida de la siguiente forma:

No obstante lo señalado, la siguiente información del certificado es pública:

- RUT del suscriptor.
- Correo electrónico del suscriptor.
- Nombre completo del suscriptor.
- Tipo y usos de certificado.

Firma.digital entregará información de titulares sólo en los casos que permite la ley que rige la firma electrónica, y esto es, por el titular del certificado o en algún tribunal en virtud de algún procedimiento judicial.

9. Suspensión y revocación de los certificados

9.1. Revocación

La PSC permite revocar el certificado al suscriptor, para el caso que estime que se ha puesto en compromiso su seguridad. De igual manera, lo revoca

Las solicitudes de revocación de los certificados emitidos por Firma.digital deberán contar con autenticación, ya sea física o electrónica, del solicitante.

9.1.1. Posibles causas de revocación

- Solicitud del suscriptor.
- Pérdida del certificado o alteración del elemento donde almacena el certificado.
- Fallecimiento del suscriptor o de algún representado, término de la representación de la persona jurídica.
- 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 cualquier otro motivo, que exponga claramente o ponga en riesgo la llave privada del suscriptor, o no se cumpla de alguna forma el contrato de suscripción.

9.1.2. Formas de revocación

La revocación se genera mediante solicitud previa, por cualquiera de los canales que posee la CPS para estos efectos o por la concurrencia del suscriptor del certificado, o en su defecto, la persona jurídica a la cual fue emitido el certificado.

9.1.3. Canales de atención para la revocación

• Vía correo electrónico a revocacion@firma.digital o a soporte@firma.digital

• Vía formulario en sitio Web

Sólo el suscriptor debe realizar esta tarea, si es el caso de que la solicitud sea realizada por otra persona, esto se deberá realizar por carta certificada a Firma.digital. Utilizando el formulario respectivo registrado en el sitio web, previa firma e impresión de huella dactilar en la misma.

9.1.4. Publicación de la revocación

El acto de revocación será comunicado al suscriptor, así como el origen de la decisión de la misma, vía correo electrónico. Cualquier forma de acción o solicitud de revocación será publicada en la lista de certificados revocados (CRL), disponible en **http://crl.firma.digital/firmadigitalFEA-G1.crl**

Al ser publicado el certificado caducado, eso inmediatamente generará cambios en la CA con la imposibilidad de reutilizar el certificado. En el caso de término de actividades de firma electrónica de la CA, este acto de certificados revocados quedará efectivo inmediatamente después que esto ocurra.

9.2. Caducidad

Luego de finalizado el período de vigencia del certificado, éste caducará de forma automática. Se informará al suscriptor del certificado de forma anticipada y vía email a la fecha de caducidad para que pueda decidir preventivamente su total caducidad o renovación. La caducidad del certificado produce su invalidez de forma automática, caducando también los servicios de certificación.

9.3. Renovación

El procedimiento de renovación, se ejecuta cuando el certificado está próximo a caducar y el suscriptor decide su renovación con la misma CA. Para dicho caso, Firma.digital emitirá un nuevo certificado y se generarán nuevas llaves, requiriendo verificar previamente la vigencia de la validación del suscriptor, cuya vigencia es a lo más de 3 años, o bien generar una nueva verificación de identidad. Los certificados emitidos por Firma.digital tienen una vigencia que no podrá exceder de tres años contados desde la fecha de emisión; y para su renovación se debe cumplir:

- Que exista actividad de certificación previa en esta CA por parte del suscriptor y emitido por Firma.digital.
- Que el suscriptor solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a Firma.digital en los procedimientos declarados para esos efectos.
- Que la CA verifique que no exista una revocación previa del certificado original.
- Que el suscriptor pueda hacer todas las actividades necesarias para solicitar la emisión de un certificado.

9.3.1. Solicitud de renovación

Para renovación de certificados digitales, se utilizará el mismo proceso de solicitud de certificado, desde la página web. Si se cumplen los requisitos para la emisión.

9.3.2. Procedimiento de renovación

Una vez recibida la solicitud y verificado que cumple con los requisitos. Se procesará la solicitud de la misma forma como se procesan los demás certificados.

- La CA emitirá el certificado solicitado
- La emisión del certificado generará un correo electrónico al solicitante. En el correo se informará que el certificado está disponible y que puede operar con su certificado en línea o ser descargado desde el sitio web.

Cabe destacar que para la verificación del suscriptor se realizará lo siguiente:

- Se verificará la vigencia de la verificación de identidad almacenada, que confirma la identidad del suscriptor, requiriendo un nuevo procedimiento de enrolamiento si se considera vencida.
- Si está vencida se considera el mismo procedimiento descrito en el apartado de registro inicial.

9.4. Suspensión

La Suspensión procede en el caso que el suscriptor no se encuentre en condiciones de tener acceso a su llave privada, en forma temporal, no habiéndose visto comprometida la seguridad de ésta.

Aceptada una solicitud de suspensión, la PSC procederá a revocar el o los certificados indicados.

Cuando termine el período de suspensión, sin que se haya confirmado que hayan existido causales de revocación, la PSC procederá a enviar un código, vía email, para que el suscriptor pueda generar nuevamente el certificado. El certificado nuevo tendrá la misma fecha de expiración que el suspendido.

9.5. Concordancia de la Política de Certificación con los procedimientos operacionales

Los procedimientos operacionales de la PSC se hayan estructurados para dar cumplimiento a las declaraciones y garantías de la Declaración de Prácticas de Certificación (CPS). Ésta, a su vez, es la concreción de la Política de Certificación aplicada a las distintas CA de la PSC.

De esta manera, los procedimientos operacionales consideran, entre otros:

- **Política de Seguridad**: elaborada para alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Política de Gestión del Riesgo**: elaborada para alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Plan de Recuperación de Desastres**: elaborado para mantener la continuidad operacional declarada por la PSC en este documento.
- **Plan de Seguridad de la Información**: elaborado para alcanzar el nivel de seguridad de la información declarado por la PSC en este documento.
- **Implementación del Plan de Seguridad de la Información**: elaborado para alcanzar el nivel de seguridad de la información declarado por la PSC en este documento.

- **Plan de Administración de Llaves Criptográficas**: elaborado para que la gestión de las llaves criptográficas de la PSC pueda cumplir con los estándares de seguridad y continuidad declarados en este documento.
- **Plan de Seguridad Física**: elaborado para que las instalaciones de la PSC permitan alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Manual de Operaciones de la Autoridad Certificadora**: elaborado para alcanzar el nivel de seguridad y de continuidad operacional de la certificación digital, revocación y suspensión declarado por la PSC en este documento.
- **Manual de Operaciones de la Autoridad de Registro**: elaborado para alcanzar el nivel de seguridad y de continuidad operacional de la certificación digital, revocación y suspensión declarado por la PSC en este documento.
- **Procedimiento de Contratación de Personal**: elaborado para que el personal de la PSC pueda asegurar el nivel de seguridad declarado por la PSC en este documento.

9.6. Término de actividades de la CA

En el caso del cese de actividades de la CA se declaran las siguientes medidas:

- Comunicación preventiva del cese de actividades:
    - Notificación vía Web.
    - Publicación de anuncio de cese en al menos dos diarios de divulgación nacional.
    - Toda información se realizará con al menos 60 días antes de la fecha indicada de cese definitivo.
- Se transferirán todas las obligaciones y derechos de los certificados a otra PSC existente, bajo el pleno consentimiento del suscriptor.
- Si no es posible transferir los certificados, se revocarán.
- Se indemnizará a los suscriptores que lo soliciten por sus certificados revocados con fecha anterior a la fecha de vigencia del mismo, con tope el costo del servicio descontando los días de vigencia hasta la fecha de revocación.

9.7. Auditorías

Firma.digital podría contar con procesos de auditoría internos y de terceros cada vez que permitan asegurar, mantener y mejorar contínuamente los altos niveles de seguridad en sus procesos.

Los procedimientos y frecuencia de las Auditorías de la Entidad Acreditadora dependiente del Ministerio de Economía están regidos por las guías de acreditación y a lo informado en la página web www.entidadacreditadora.gob.cl.

9.8. Administración y modificaciones

Firma.digital podrá hacer cambios en sus procedimientos, manteniendo siempre los estándares exigidos a una entidad emisora de certificados de firma electrónica. Estos cambios podrían ser justificados desde un punto de vista Técnico, Comercial y/o Jurídico, las veces que estime conveniente.

9.9. Publicación de modificaciones

Todo cambio en la CP o CPS que involucre directamente la operación de los certificados, podría ser informado vía Web a sus suscriptores y solicitantes en un período no superior a 15 días, desde la aplicación de los cambios.

Luego del comunicado, y si no se recibe ninguna declaración por escrito de suscriptores o solicitantes, en contra de lo comunicado, las modificaciones se declararán como aceptadas por la comunidad de suscriptores.

9.10. Información de contacto

Para consultas respecto del contenido del presente documento, pueden ser realizadas vía correo o de forma presencial:

- Nombre: “Prácticas Firma.digital”
- Dirección de contacto: Avenida Kennedy 5488, Torre Sur, oficina 203, comuna de Vitacura, Santiago, Región Metropolitana.
- Correo electrónico: soporte@firma.digital

10. Referencias

Cómo referencia se consideraron las principales normas técnicas registradas por la Entidad de Acreditación, aunque si bien es cierto aplican sólo para certificados de firma electrónica avanzada (FEA), son usados como marco de trabajo referencial en certificados digitales para firma simple (FES), 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.