POLÍTICA DE CERTIFICACIÓN

Contenido

1 Identificación del Documento 4

2 Control de Versiones 4

3 Introducción 4

4 Alcance 5

5 Referencias y estándares Internacionales 5

5.1 Prácticas de Certificación: 5

5.2 Seguridad 6

5.3 Estructura de Certificados 6

5.4 Repositorio de Información 6

6 Glosario 6

7 Aplicabilidad y Comunidad de Usuarios 7

7.1 Comunidad de Usuarios 7

7.2 Aplicabilidad 7

8 Tipos y usos de Certificados 8

8.1 Tipos de Certificados 8

8.2 Contenido de los certificados 8

9 Contacto 8

10 Requerimientos Generales y Operacionales 8

10.1 Obligaciones de Autoridad de Certificación Raíz (CA Raíz) 8

10.2 Obligaciones de la Autoridad de Certificación, CA 9

10.3 Obligaciones con los suscriptores 9

10.4 Obligaciones del suscriptor 9

10.5 Obligaciones generales de TOC como PSC 9

10.6 Obligaciones del Solicitante 10

11 Certificados 10

11.1 Lista de Revocados y estructura de información 10

11.1.1 Certificados de firma electrónica avanzada 10

11.1.2 Certificados de firma electrónica tributaria 10

11.1.3 Certificados de firma electrónica simple 10

11.2 Confianzas en las Firmas 10

11.3 Confianza en los certificados 11

12 Protección de información 11

13 Declaración Operacional 11

13.1 Registro Inicial 11

13.2 Reemisión de certificados 11

13.3 Revocación de certificados 12

13.3.1 Posibles causas de Revocación de Certificados 12

13.3.2 Formas de Revocación de Certificados 12

13.3.3 Canales de atención para la revocación de certificados: 12

13.3.4 Publicación de la Revocación 12

13.4 Caducidad de los Certificados 12

13.5 Renovación de los Servicios de Certificación 13

13.5.1 Solicitud de Renovación 13

13.5.2 Procedimiento de Renovación 13

13.6 Término de actividades de la PSC 14

14 Auditoría 14

15 Administraciones y modificaciones 14

Publicación de Modificaciones 14

1 Identificación del Documento

Identificación del documento	Política de Certificación
Documento(s) relacionado(s)	Guía de Acreditación sección 17 PO01
Responsable de aprobación (anual)	Directorio - Comité de Riesgo
Dueño funcional	Gerente de Riesgo
Período de revisión	Anual
Actualización	Anual

2 Control de Versiones

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
2.0	Revisión Anual; cambio formato	CEO	Gte Riesgo	Comité de Riesgo y Directorio	Jul18	Jul18

3 Introducción

TOC S.A., en adelante TOC, tiene como objetivo la autenticación de identidad con tecnología biométrica, y de igual forma tiene implementados todos los servicios de seguridad para la infraestructura de llave pública (Public Key Infraestructure, PKI). Su infraestructura es regida con todos los estándares internacionales en referencia con este tipo de tecnología y por los estándares de Seguridad de la Información (ISO 27001).

Un Prestador de Servicios de Certificación (PSC), por definición, es una institución o persona, ya sea pública o privada que presta servicios de firma electrónica y puede emitir certificados, que expresamente actúa como tercera parte de confianza entre las personas que participan en un acto de firma o legalidad documental, utilizando firma electrónica.

La Política de Certificación, es la descripción detallada de las normas y prácticas, cómo administra los servicios de certificados de firma electrónica, cómo emite y administra certificados digitales en su rol de PSC. Las Prácticas de Certificación, en conjunto con las políticas de la emisión de certificados, son las formas para solicitar, validar, entregar, emitir y revocar certificados.

A continuación, se describen los niveles de seguridad utilizados en su rol de PSC, incluyendo las normas de la Autoridad de Registro (RA):

- Obligaciones de Prestador de Servicios de Certificación (PSC), las Autoridades de Registro (RA), Suscriptores y Usuarios dentro del ámbito que regula la PSC de TOC.
- Auditorías de Seguridad y de Cumplimiento, sobre las las prácticas de certificación.
- Métodos usados para identificar a los suscriptores.

- Procedimientos del Ciclo de Vida los Certificados (solicitud, emisión, revocación, suspensión y renovación).
- Contenidos y estructura de certificados emitidos, vigentes y revocados.
- Auditorías sobre la retención de registro de información, contingencia y recuperación de desastre.
- Procedimiento de Seguridad de Informacición (Seguridad Física y del Entorno, de Recursos Humanos y del Control de Accesos manejo de claves de la PSC).

4 Alcance

En la Política de Certificación se encuentran todas las actividades, declaraciones que rigen las siguientes normas y reglamentos:

- Ley 19.799 de Abril 2002, sobre documentos electrónicos, firma electrónica y servicios de certificación de la firma, que es regido por la entidad acreditadora del Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- Guía de evaluación de las acreditaciones de Prestadores de Servicios de Certificación de Septiembre 2002, del Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- Actualización de Guías de evaluación de Procedimiento de Acreditación de Prestadores de Servicios de Certificación, Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- Aprobación de Guías de Evaluación y de inspección de Prestadores de Servicios de Certificación de Firma electrónica avanzada, Febrero 2013, del Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- Ley N° 20.217, de Noviembre 2007, modificación del código de procedimiento civil y la ley N° 19.799 sobre documentos electrónicos, firma electrónica y lo servicios de certificación de dicha firma, del Ministerio Economía, Fomento y Turismo del Gobierno de Chile.
- DS N° 181, de Julio del 2002. Reglamento ley N° 19.799 sobre documentos electrónicos, firma electrónica y certificación de dicha firma, del Ministerio Economía, Fomento y Turismo del Gobierno de Chile.
- Resolución Exenta N° 9 del 15 de Febrero del 2001, emitida por el Servicio de Impuestos Internos.
- Resolución Exenta N° 280 del 11 de Febrero del 2013, emitida por el Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- Resolución Exenta N° 172 del 30 de Enero del 2013, emitida por el Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.

Adicionalmente se desciben las Prácticas de Certificación utilizando la infraestructura de llave pública (PKI) de TOC a nivel nacional y dentro de aquel país que valide el proceso de acreditación chileno. En este contexto se podrá certificar:

- Las claves públicas de las personas físicas
- Las claves públicas de las entidades intermedias

Todos los procedimientos definidos en este alcance se aplican a la Autoridad Certificadora (CA), a la Autoridad de Registro PSC (RA), Solicitantes y Titulares (Suscriptores), para la emisión de certificados.

5 Referencias y estándares Internacionales

5.1 Prácticas de Certificación:

- 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.

5.2 Seguridad

- 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.
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos.

5.3 Estructura de Certificados

- 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.
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos.

5.4 Repositorio de Información

- 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.

6 Glosario

- **Hashing:** Son una secuencia de caracteres que representan un documento. Estas secuencias son de tamaño fijo y reducido. La principal característica es que es una representación única del documento original y que si existe una alteración mínima el resultado es absolutamente distinto y deja de representar al documento original.
- **Certificado:** Es todo registro que evidencie el vínculo entre un firmante y los datos de creación de Firma Electrónica.

- **Firma electrónica:** Es un vínculo único e irrepetible representado en una secuencia de caracteres. Este vínculo es el resultado entre el algoritmo hash al contenido del documento y la llave privada del firmante. De esta forma se genera una asociación directa entre quien firmó el documento y el documento en sí y que se pueda detectar cualquier cambio posterior.
- **Suscriptor de un Certificado:** Corresponde a la persona o empresa a la cual se emitió el certificado. Este suscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el suscriptor es la persona que tiene en su absoluto control el certificado de firma electrónica.
- **Certificador:** Es la persona o empresa que puede verificar la identidad de los solicitantes.
- **Autoridad de registro (AR o RA, por su sigla en inglés, Registry Authority):** Es la empresa o institución que controla la generación de certificados llevando un registro electrónico de los mismos, para los miembros de una entidad. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes. Este registro se realiza encargándose de la detección, comercialización y administración de las solicitudes de todos los tipos de certificados que comercializa TOC.
- **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por TOC y hace uso de ellos.

7 Aplicabilidad y Comunidad de Usuarios

7.1 Comunidad de Usuarios

TOC emitirá sus certificados digitales en el estándar ITU-T Recommendation X.509, y serán emitidos a toda persona física o representantes legales de empresa pública o privada. Para ello requerirá asegurar la identidad del interesado o suscriptor requiriendo su completa identificación ante la Autoridad de Registro, con presencia física.

7.2 Aplicabilidad

Los certificados emitidos por la Autoridad Certificadora TOC (AC o CA, por su sigla en inglés Certification Authority) no han sido diseñados, ni tampoco se autoriza su uso, para cualquier efecto que al ser usado éste se deriva en muerte, lesiones a personas o al medio ambiente o infrinja la ley de la República de Chile.

Los certificados emitidos por TOC, podrán ser usados en las siguientes necesidades de seguridad:

Necesidad	Detalle
Autenticación	Debe dar suficientes garantías respecto a la Identidad del Titular solicitante del certificado. Para esto debe requerir la presencia física del futuro suscriptor ante la Autoridad de Registro TOC. Junto a la presencia del futuro suscriptor, debe requerir la Solicitud del Certificado que acredite su identidad.
No Repudiación	Las firmas electrónicas producidas con certificados emitidos por la Entidad de Registro TOC tienen la evidencia necesaria pa enfrentar que una persona deniegue la autoría de la firma digital, o el contenido de éste, que se haya firmado digitalmente con el certificado emitido a la persona.
Integridad	La información firmada con un certificado digital emitido por la Autoridad de Registro TOC permite validar que el elemento firmado no cambia su contenido entre el origen y el destino.
Privacidad	Los certificados emitidos por la Autoridad de Registro TOC, permiten cifrar elementos que solo pueden ser visualizados por el titular de los

	datos de creación de Firma Electrónica.

8 Tipos y usos de Certificados

8.1 Tipos de Certificados

TOC tiene la infraestructura para emitir varios tipos de certificados, de acuerdo a las necesidades de los solicitantes, dependiendo del ámbito donde se utilice. Los certificados de firma avanzada son de Clase 3, al igual que los certificados de firma electrónica avanzada.

Los certificados de firma electrónica definidos por TOC son:

- Certificados de firma electrónica avanzada.
- Certificados de firma electrónica tributaria.
- Certificados de firma electrónica simple.

8.2 Contenido de los certificados

El contenido de cada certificado cumple con el Reglamento de la Ley 19.799 y, para el caso de firma electrónica tributaria, cumple la resolución exenta N° 9 del 15 de Febrero del 2001 del SII.

La estructura de los certificados emitidos por la Autoridad de Registro TOC cumple y es compatible con el estándar ISO/IEC 9594-8. Estructura de los certificados:

- RUT
- Correo electrónico
- Nombre Completo
- Tipo de certificado
- Datos de la acreditación de TOC

Para el caso de los certificados tributarios, contendrá en un campo con la glosa “Certificado para uso Tributario”

9 Contacto

- Dirección: Avenida Santa María 2670, oficina 403, Providencia.
- Correo electrónico contacto@toc.cl

10 Requerimientos Generales y Operacionales

10.1 Obligaciones de Autoridad de Certificación Raíz (CA Raíz)

Entendiendo que un certificado raíz puede generar una jerarquía de confianza, esto es, que se puede utilizar para firmar los certificados de la entidad certificadora subordinada o Sub CA, en estos términos TOC se define como entidad raíz y una entidad intermedia, porque ha emitido un certificado para ser utilizado por el mismo.

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

10.2 Obligaciones de la Autoridad de Certificación, CA

Las obligaciones de TOC para prestar el servicio de certificación electrónica, son:

- Cumplir a todas las obligaciones legales necesarias para el ejercicio de esta actividad.
- Administrar el sistema de llaves (PKI) para hacer operativo la certificación y firma electrónica.
- Adminsitración de llaves:
    - TOC emite en forma automática toda llave pública y privada que se le entrega a cada titular de certficado. Con el hecho de que las llaves se generan automáticamente se garantiza su total confidencialidad.
- Identificar y autenticar correctamente al suscriptor o usuario de firma electrónica, o en su defecto a la institución a la cual represente, usando correctamente los procedimientos de esta CA para estos efectos.
- Emisión de Certificados:
    - TOC emitirá certificados que sean solicitados, previa aprobación de los antecedentes necesarios de la persona o representante de una empresa.
- Emitir y mantener la lista de certificados emitidos y revocados.
- Emitir certificados a quienes lo soliciten.
- Establecer procedimientos claros para realizar la actividad.
- Implementar controles de Seguridad física.

10.3 Obligaciones con los suscriptores

- Garantizar que toda información suscrita en el certificado entregado es exacta y es fiel reflejo de la información entregada por el suscriptor en el acto de emisión de certificado.
- Hacer uso de tecnologías adecuadas para la emisión de certificados electrónicos de cada caso.
- Informar preventivamente la proximidad de la caducidad de su certificado.
- Revocar los certificados que no cumplan las prácticas adecuadas de firma electrónica.
- Disponibilizar lista de certificados revocados que está constantemente actualizada.
- Tener los procedimientos y políticas adecuadas para resguardar la llave privada de cada suscriptor.

10.4 Obligaciones del suscriptor

- Conservar y dar uso adecuado del certificado, según lo descrito en el contrato de suscriptor.
- Dar correcta custodia al certificado, resguardar su clave privada y no dar mal uso al mismo.
- Proteger el uso de su certificado mediante password o PIN dependiendo si el certificado utilizado puede residir en su PC o e-token.
- Para el caso de firma electrónica avanzada, la emisora de certificados digitales TOC está autorizada para cualquier modificación. Si es necesario, cualquier modificación debe ser informada a TOC en sus oficinas Avenida Santa María 2670, oficina 403, Providencia, en horarios de lunes a viernes de 9:00 a 18:00 Hrs.
- Informar al Prestador de Servicios de Certificación, PSC, inmediatamente por cualquier situación que afecte directamente la validez del certificado.

10.5 Obligaciones generales de TOC como PSC

- Mantener políticas claras en cuanto al uso de infraestructura de llaves públicas (PKI) para firma electrónica avanzada y publicarlas en https://www.toc.cl/politica-y-privacidad y de este modo estarán disponibles al público en general.
- Al decidir dar término a sus servicios de firma electrónica debe dar a conocer su decisión a todos sus suscriptores activos, y transferir todos los certificados a otro prestador de firma electrónica. Los suscriptores actuales pueden negarse a esa transferencia, y en este caso su certificado quedará en estado revocado.
- Cumplir todas las leyes que rigen este tipo de actividades, entre ellas la Ley del Consumidor N° 19.496 y la de Protección a la Vida Privada N° 19.628.

- Mantener actualizado el registro de todos los certificados emitidos y revocados durante el periodo que exige y que rige la actividad de firma electrónica avanzada, Ley N° 19.799. Este registro lo tendrá disponible electrónicamente por acceso público en el sitio https://firma.toc.cl/indexpki.php
- Dar cumplimiento al punto 6 de la Resolución Exenta N° 9, del 15 de Febrero del 2001 del SII, para certificados para facturación electrónica.
- Publicar todas las resoluciones de la Entidad Acreditadora. Esta publicación será en https://www.toc.cl/politica-y-privacidad
- Informar preventivamente a la Entidad Acreditadora cualquier evento que afecte directamente la continuidad como entidad acreditada para PSC, ya sea iniciación de proceso de quiebra, cambio de giro.
- Requerir la comparecencia física de la persona o representante legal si es persona jurídica, ante sí, notario u oficial de registro civil, para cada solicitud de firma y emisión de cada certificado de firma electrónica avanzada, ya que representa la identidad del solicitante.
- Pagar anualmente el arancel de supervisión que realiza la Entidad Acreditadora.
- Mantener vigente el seguro de responsabilidad civil que exige ley de firma electrónica avanzada y documentos electrónicos, ley N° 19.799
- Mantener constantemente el registro electrónico de los antecedentes de los suscriptores.
- Almacenar en forma segura la documentación que evidencie la emisión de un certificado electrónico a algún suscriptor, en un lugar seguro y el periodo de tiempo que exige la Ley.

10.6 Obligaciones del Solicitante

El solicitante de un certificado debe entregar toda la información de identificación personal o de su empresa si es para estos efectos, exigida por la PSC TOC.

El solicitante del certificado deberá cancelar la tarifa establecida y publicada en https://firma.toc.cl/documentos/Lista_de_precios_TOC.pdf por el certificado que solicite.

11 Certificados

11.1 Lista de Revocados y estructura de información

Dentro del sitio corporativo de TOC, https://firma.toc.cl/indexpki.php se encuentra la información de los certificados emitidos y revocados, para todos los tipos de certificados que emite la Autoridad de Registro TOC.

11.1.1 Certificados de firma electrónica avanzada

- Lista de certificados de revocación se encuentra en : https://firma.toc.cl/pki_certificados_revocados.php http://firma.toc.cl/crl
- Lista de certificados emitidos se encuentra en: https://firma.toc.cl/pki_consulta.php

11.1.2 Certificados de firma electrónica tributaria

- Lista de certificados de revocación se encuentra en : http://firma.toc.cl/crl_fes
- Lista de certificados emitidos se encuentra en: https://firma.toc.cl/pki_consulta.php

11.1.3 Certificados de firma electrónica simple

- Lista de certificados de revocación se encuentra en: http://firma.toc.cl/crl_fes
- Lista de certificados emitidos se encuentra en: https://firma.toc.cl/pki_consulta.php

11.2 Confianzas en las Firmas

Las personas que reciben alguna firma electrónica realizada con un certificado emitido por TOC, tendrán derecho en confiar en ello:

- La operación que se utilizó para firmar tiene todos los resguardos de seguridad y uso de las llaves privadas y públicas del suscriptor.
- Que el certificado que utilizó en la firma del elemento, no tenga estado caducado en el momento de la firma.

11.3 Confianza en los certificados

Las personas que utilicen o reciben un elemento firmado por un certificado emitido por TOC tendrá derecho de confiar en el certificado.

12 Protección de información

TOC define como confidencial, toda la información relevante a sus suscriptores y solicitantes, y se compromete a no utilizar esta información en otros aspectos que no sean exclusivamente relacionados con su actividad de certificación.

La entrega de esta información a terceros está estrictamente regida de la siguiente forma: TOC emite certificados según la Ley 19.799 y todos sus procedimientos técnicos exigidos, por lo que en cada certificado emitido se encuentran:

- RUT
- Correo Electrónico
- Nombre
- Tipo de certificado
- Datos de la acreditación

Casos particulares de entrega de información de titulares de certificados: TOC entregará información de titulares solo 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.

13 Declaración Operacional

13.1 Registro Inicial

El procedimiento de suscripción de firma electrónica registra los siguientes datos:

- Personas Naturales: nombre completo, apellido paterno y materno, y copia de Cédula de Identidad nacional.
- Persona Jurídica: la razón social completa y todos los antecedentes legales que corresponda.

Para realizar una identificación fehaciente de los solicitantes, esta documentación debe ser presentada personalmente en las oficinas de TOC. Para mayor información de información solicitada en cada caso, TOC publica los requisitos en cada tipo de certificado.

13.2 Reemisión de certificados

Los certificados emitidos por TOC tendrán solo dos estados, Vigentes y Revocados. La reemisión de llaves no está permitida con el claro objetivo de mantener el no repudio en el caso de los certificados emitidos por TOC. Lo mismo ocurre para el caso de los certificados revocados, no reemitirá llaves con un certificado en este último estado.

13.3 Revocación de certificados

Las solicitudes de revocación se realizarán por vía electrónica a soporte@toc.cl o en la página web de la compañía, https://firma.toc.cl/pki_revocar.php La revocación es un mecanismo que posee la PSC para que por algún motivo se deje de confiar en el certificado.

13.3.1 Posibles causas de Revocación de Certificados

- Solicitud del Suscriptor
- Pérdida del certificado o alteración física del dispositivo que almacena el certificado.
- Que la actual PSC comience el proceso de término de acreditación de emisor de certificados de firma electrónica avanzada.
- Fallecimiento del suscriptor o de algún representado, término de la representación o extinción de la persona jurídica.
- Por alguna eventualidad se vea expuesta la llave privada del suscriptor, ya sea por robo, alteración, divulgación, o cualquier otro tipo de causal circunstancial.
- Por incumplimiento de suscripción, ya sea por parte de la PSC o el suscriptor.
- Por resolución judicial o administrativa.
- Por cualquier otro motivo, que se vea claramente expuesta o en riesgo la llave privada del suscriptor o no se cumpla de alguna forma el contrato de suscripción.

13.3.2 Formas de Revocación de Certificados

La revocación es por solicitud previa mediante los canales que posee la PSC para estos efectos, o por la concurrencia del suscriptor del certificado o de la persona jurídica a la cual fue emitido el certificado.

13.3.3 Canales de atención para la revocación de certificados:

- Para contacto inicial y comienzo del proceso de revocación: (+562) 2946 5752
- Por mail a: soporte@toc.cl
- Vía Web a la dirección: https://firma.toc.cl/pki_revocar.php

Solo el suscriptor debe realizar esta tarea, si es el caso de que la solicitud sea realizada por otra persona, esto se deberá realizar dirigiéndose a las oficinas de TOC. Utilizando el formulario respectivo, se generará la solicitud, previa firma e impresión de huella dactilar en la misma.

13.3.4 Publicación de la Revocación

La decisión de revocación y la acción propiamente tal será comunicada al suscriptor vía correo electrónico. Para el caso que la solicitud de revocación sea vía Web, esta operación será comunicada por la misma vía que se realizó la solicitud, indicando en forma automática el número único de revocación.

Cualquier forma de acción o solicitud de revocación será publicada en la lista de certificados revocados (CRL).

Al publicar el certificado revocado la PSC queda impedida de reutilizar el certificado. En el caso del término de actividades de firma electrónica de la PSC, los certificados revocados quedarán efectivos inmediatamente después que esto ocurra.

13.4 Caducidad de los Certificados

Finalizado el periodo de vigencia de un certificado, éste caducará en forma automática. La PSC indicará al suscriptor en forma anticipada la fecha de caducidad del mismo, para que el suscriptor tenga pleno conocimiento del estado de su certificado y que decida preventivamente su total caducidad o renovación.

La caducidad del certificado produce la invalidez del certificado en forma automática, y de igual forma también caducan los servicios de certificación.

La caducidad del certificado no permite el uso legítimo de él por parte del suscriptor.

13.5 Renovación de los Servicios de Certificación

El procedimiento de renovación se ejecuta cuando el certificado del suscriptor este próximamente a caducar y este decide utilizar nuevamente los servicios de certificación de la misma PSC. Para el caso de la renovación la PSC emitirá un nuevo certificado y se generarán nuevas claves, requiriendo nuevamente el proceso de verificación de identidad del suscriptor.

Los certificados emitidos por TOC tienen un plazo de vigencia de un año.

Para la renovación, se deben cumplir algunos requisitos:

- Que exista actividad de certificación previa en esta PSC por parte del suscriptor y emitido por TOC.
- Que el suscriptor solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a TOC en los procedimientos declarados para esos efectos.
- Que la PSC pueda verificar positivamente que no existe ninguna actividad de revocación previa.
- Que el suscriptor pueda hacer todas las actividades necesarias para solicitar la emisión de un certificado.
- Que la solicitud del certificado sea por el mismo tipo que el emitido inicialmente.

13.5.1 Solicitud de Renovación

Al momento de solicitar la renovación el suscriptor debe completar el formulario para tal efecto, en la página Web https://firma.toc.cl/pki_solicitud.php

- El suscriptor enviará el formulario a la PSC.
- El suscriptor realizará todos los procedimientos adecuados para la ejecutar la solicitud.
- El procedimiento consiste en la emisión de un nuevo certificado que reemplaza el certificado vencido o próximo a vencer.
- No es necesario revocar el certificado anterior puesto que por las restricciones de fechas se imposibilitará su uso.

13.5.2 Procedimiento de Renovación

Una vez que la PSC reciba la solicitud de renovación, esta será procesada de la misma forma que una solicitud como los demás certificados.

- La PSC emitirá el certificado solicitado.
- La emisión del certificado será informada mediante un correo electrónico al solicitante.
- En el correo se informará que el certificado está disponible y que puede ser descargado desde el sitio Web https://firma.toc.cl/indexpki.php
- Para el caso de un certificado de firma avanzada, el proceso de descarga directa no aplica.
- Con la renovación, las obligaciones, derechos y deberes, tanto del suscriptor como de la PSC siguen el mismo estado de la contratación o emisión anterior, y además las políticas de certificación vigentes.

13.6 Término de actividades de la PSC

Con el objetivo de provocar el menor impacto a usuarios y suscriptores, y para el caso de cese de actividades de la PSC, se declaran las siguientes medidas:

- Comunicación preventiva del cese de actividades:
  - Notificar con correo certificado o correo ordinario el cese de las actividades.
  - Publicación de anuncio de cese de actividades en dos diarios de divulgación nacional.
  - Todas las acciones de informar el cese de las actividades que realice la PSC deben realizarse como mínimo 60 días de anticipación al cese definitivo de las actividades.
- Si es posible que alguna PSC existente posea los procedimientos de transferencia de obligaciones, esto se realizará transmitiendo todas las obligaciones y derechos dentro de las entidades y sistemas de certificación. Para hacer posible esta transferencia, se debe tener pleno consentimiento del suscriptor de manera expresa para tal efecto.
- Si no es posible la transferencia, se darán por revocados todos los certificados, una vez transcurrido los 60 días de la comunicación de cese de actividades.
- Indemnizar adecuadamente a aquellos suscriptores que lo soliciten cuando sus certificados sean revocados con anterioridad al plazo previsto, pactándose como tope para la indemnización el costo del servicio, descontando los días de vigencia y pleno uso del certificado desde el momento de su certificación.

14 Auditoría

Los procesos y frecuencias de Auditorias están regidos por las guías de acreditación y auditorias de la Entidad Acreditadora dependiente del Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.

15 Administraciones y modificaciones

La PSC podrá hacer cambios en sus procedimientos, manteniendo siempre los estándares exigidos a una entidad emisora de certificados de firma electrónica. Estos cambios se deben justificar desde el punto de vista técnico, comercial y jurídico.

Publicación de Modificaciones

Toda modificación en la operación de la PSC o algún cambio en alguna política que involucre directamente la operación o cambios en los certificados emitidos debe ser informado por los canales adecuados a todos sus suscriptores y solicitantes en un periodo no superior a 15 días, luego de la aplicación de los cambios efectuados.

Luego del comunicado, y si no se recibe alguna declaración por escrito de los suscriptores o solicitantes en contra de las modificaciones anunciadas, éstas se declararán como aceptadas por la comunidad usuario de la PCS.