# Declaración de Prácticas de Certificación

Política

TOC

# Contenido

# 1. Información del documento y Control de Cambios

| Versión | Fecha | Revisión | Observaciones |
|---|---|---|---|
| 1.0 | 26/10/2015 | 1.0 | Primer Documento |
| 2.0 | Abril 2019 | 2.0 | Actualización de documento |

| | |
|---|---|
| Elaborado por | Gustavo Veliz Estrada, Oficial Seguridad de Información |
| Revisado por | Ricardo Navarro Luft, CEO<br>Tomás Castañeda Puschel, Jefe de Investigación, Desarrollo e Innovación<br>Nicolás Aguilera Muñoz, Gerente de Operaciones |
| Autorizado por | Ricardo Navarro Luft, CEO |
| Fecha Publicación | Mayo 2019 |

| Canales de Difusión |
|---|
| Distribución:<br>Ministerio de Economía<br>Sitio Web |

| DOCUMENTOS EXTERNOS |
|---|
| • Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y lo servicios de certificación de dicha firma, del Ministerio Economía.<br>• Ley N° 19.628 protección de datos de carácter personal<br>• Guías de Evaluación<br>• Guía de evaluación de las acreditaciones de Prestadores de Servicios de Certificación de Septiembre 2002, del Ministerio de Economía |

# 2. Introducción

El presente documento tiene como objetivo detallar el procedimiento que TOC S.A. ejecuta en su rol de prestador de servicios de certificación (PSC) en el proceso de emisión y gestión de certificados de firma electrónica avanzada. Además define su uso, emisión, suspensión y revocación; controles de vigencia y seguridad del proceso y la configuración del ciclo de vida de un certificado de firma electrónica avanzada.

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.

De igual forma se describen los niveles de seguridad utilizados en su rol de PSC, incluyendo las normas de RA y también los siguientes procedimientos:

- Obligaciones de Prestador de Servicios de Certificación, las Autoridades de Registro, Suscriptores y Usuarios dentro del ámbito que regula la PSC de TOC.
- Revisiones de Auditoría, de Seguridad y de cumplimiento de "Prácticas" considerados.

- Métodos usados para identificar a los suscriptores
- Procedimientos asociados al ciclo de vida los certificados, esto es, Solicitud, Emisión, Revocación, Suspensión y Renovación.
- Procedimientos para registros de auditoría, retención de registro de información, contingencia y recuperación de desastre.
- Prácticas de seguridad física, del personal y del manejo de claves de la PSC
- Contenidos y estructura de certificados emitidos, vigentes y revocados

# 3. Alcance

La Declaración de Prácticas de Certificación (CPS) detalla las condiciones, procedimientos y normas que se aplican en el proceso servicios de certificación para la emisión de sus certificados de firma electrónica avanzada.

# 4. Referencias y estándares internacionales

## a. 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.

## b. Referencias

- 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.
- Guía de evaluación de las acreditaciones de Prestadores de Servicios de Certificación de Septiembre 2002, del Ministerio de Economía.
- Actualización de Guías de evaluación de Procedimiento de Acreditación de Prestadores de Servicios de Certificación, Ministerio de Economía.
- Ley N° 19.628 Protección de datos de carácter personal.
- Ley N° 27.269 Firmas y certificados digitales
- Resolución Exenta N° 9 del 15 de Febrero del 2001, emitida por el Servicio de Impuestos Internos
- Ley N°20.217, de Noviembre 2007. Modificación del código de procedimiento civil y la DSN°181, de Julio del 2002.
- Resolución Exenta N° 280 del 11 de Febrero del 2013, emitida por el Ministerio de Economía, Fomento y Turismo.
- Resolución Exenta N° 172 del 30 de Enero del 2013 emitida por el Ministerio de Economía, Fomento y Turismo
- Aprobación Norma Técnica para la Prestación del Servicio de Certificación de Firma electrónica Avanzada (Núm. 24.- Santiago, 22 de febrero de 2019)

Todos los procedimientos definidos en este alcance se aplican a la Autoridad Certificadora, Autoridad de Registro PSC, Solicitantes y Titulares, para la emisión de Certificados por parte de TOC SA.

## c. 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.

## d. 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.

## e. 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.

# 5. Glosario

- **Hashing**: Secuencia de caracteres que representan un documento. Esta secuencia 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.

- **Subscriptor de un Certificado:** Corresponde a la persona o empresa a la cual se emitió el certificado. Este subscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el subscriptor 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:** Es la empresa o institución que llevara el registro electrónico de los Certificados emitidos por la Autoridad de registro. Este registro se realiza encargándose de la detección, comercialización y administración de las solicitudes de todos los tipos de certificados que comercializa TOC S.A.

- Usuarios: El usuario del certificado es la persona que decide usar los certificados emitidos por TOC S.A. y hace uso de ellos.

# 6. Aplicabilidad y Comunidad de Usuarios

## a. Comunidad de Usuarios

TOC S.A. emitirá sus certificados digitales en el estándar ITU-T Recommendation X.509, y serán emitidos a toda persona natural o representantes legales de empresas públicas o privadas. Para ello TOC requerirá asegurar la identidad del interesado o suscriptor

requiriendo identificar completamente ante la autoridad de registro, con presencia física.

- **Solicitante**: Persona natural que a través de los mecanismos de enrolamiento de TOC S.A. (CPS), solicita un certificado de firma electrónica avanzada. En este proceso el solicitante debe verificar su identidad mediante los mecanismos dispuestos por TOC, a través de los cuales se obtiene la información personal, luego la CPS a través de sus controles establecidos comprobará la identidad del mismo.
- **Autoridad de Registro (AR):** Es quien recepciona, procesa y gestiona las solicitudes de certificados de firma electrónica avanzada, esto lo puede realizar en forma directa o mediante un mandatario autorizado. En este proceso la autorizada de registro debe comprobar la identidad del solicitante.
  Si esta actividad es ejecutada por terceros, esta deberá ejecutarse de acuerdo al contrato de mandato y lo indicado en este documento (Declaración de Prácticas de Certificación).

- **Prestador de servicios de Certificación (PSC):** Se refiere a TOC S.A. en su rol de prestador de servicios de certificados de firma electrónica avanzada.
  Lo anterior basado en lo expuesto en la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y servicios de certificación de dicha firma.

- **Entidad Acreditadora**: Se refiere a la Subsecretaría de Economía, de acuerdo a la Ley 19.799 el TOC S.A. en su rol de prestador de servicios de certificación de Firma Electrónica está sujeto a ser evaluado y comprobar que cuentas con los recursos tecnológicos para cumplir dicho rol y otorgar los certificados de firma electrónica avanzada.

## **b.** Aplicabilidad

Los certificados emitidos por TOC S.A. podrán ser utilizados según lo expuesto en este documento y en conformidad a la Ley 19.799
Los certificados emitidos por TOC S.A. podrán ser uso en las siguientes necesidades de seguridad:

| Necesidad | Detalle |
|---|---|
| Autenticación | Debemos dar suficientes garantías respecto a la identidad del titular solicitante del certificado. Para esto debemos requerir la presencia física del futuro suscriptor ante la Autoridad de Registro. Junto con la presencia del futuro suscriptor, debemos requerir Solicitud del Certificado, que acrediten su identidad. |

| | |
|---|---|
| No Repudio | Las firmas electrónicas producidas con Certificados emitidos la Entidad de Registro TOC S.A. tiene la evidencia necesaria frente a 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 S.A. 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 S.A., permiten cifrar elementos que solo pueden ser visualizados por el Titular de los datos de Creación de Firma Electrónica |

## c. Tipos y usos de Certificados

TOC S.A. tiene la infraestructura para emitir varios tipos de certificados, de acuerdo a las necesidades de los solicitantes y del ámbito donde se utilice.

Los certificados de firma electrónica definidos por TOC S.A. son:

- Certificados de firma electrónica al vuelo
- Certificados de firma electrónica en dispositivo token
- Certificados de firma electrónica tributaria (simple)

## d. Contenido de los certificados

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

Estructura de los Certificados emitidos por TOC S.A.:

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

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

# 7. Detalle de contacto

## a. Dirección de Contacto

TOC S.A. tiene sus oficinas principales en Avenida Santa María 2670, oficina 403, Providencia.

## b. Contacto

Pueden contactar al equipo de TOC S.A. en correo electrónico contacto@toc.cl

# 8. Requerimientos Generales y Operacionales

## a. Obligaciones de 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 entidades certificadoras subordinadas o Sub CA, en estos términos TOC S.A. se define como entidad raíz y una entidad intermedia, porque ha emitido un certificado par ser utilizado por el mismo.

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

## b. Obligaciones de CA

TOC S.A. cumple con las obligaciones legales para prestar servicio de certificación electrónica:

- 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.
- Controles de seguridad física
- Procedimientos claro y necesarios para realizar la actividad
- Emitir certificados a quienes lo soliciten
- Administrar el sistema de llaves (PKI) para hacer operativo la certificación y firma electrónica.

- Emitir y mantener la lista de certificados emitidos y revocados
- Cumplimiento a todas las obligaciones legales necesarias para el ejercicio de esta actividad.
- Emisión de Certificados: TOC S.A. emitirá certificados que sean solicitados, previa aprobación de los antecedentes necesarios de la persona o representante de una empresa.
- Administración de llaves: TOC S.A. emite en forma automática toda llave pública y privada que se le entrega a cada titular de certificado. Las llaves se generan automáticamente, esto garantiza total confidencialidad.

## c. Obligaciones de TOC S.A. (PSC)

- 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
- 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.
- Para Firma Electrónica al Vuelo, resguardar que se cumplan los requerimientos de seguridad necesarios.
- Establecer políticas claras respecto al uso de infraestructura de llaves públicas (PKI) para firma electrónica avanzada y publicarlas en www.toc.cl..
- TOC S.A. en caso de dar término a sus funciones de firma electrónica, debe dar a conocer su decisión a todos sus suscriptores activos, y transferir todos a otro prestador de firma electrónica. Los suscriptores actuales pueden negarse a esa transferencia, en este caso su certificado quedará en estado revocados.
- Cumplir todas las leyes que rigen este tipo de actividades, por ejemplo la ley del consumidor N° 19.496 y 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 debe estar disponible electrónicamente con acceso público en el sitio www.toc.cl
- Publicar todas las resoluciones de la entidad acreditadora en www.toc.cl
- 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 o cambio de giro.

- Cada certificado emitido por TOC S.A. de firma electrónica avanzada representa la identidad del solicitante, y es por esto que cada solicitud de firma requiere la comparecencia personal de la persona o representante legal si es persona jurídica, ante sí, notario u oficial de registro civil.
- 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, guardada en algún lugar seguro y el periodo de tiempo que exige la Ley.

### d. 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
- Proteger el uso de su certificado mediante password o PIN (si el certificado utilizado puede residir en su PC o e-token).
- Informar a la PSC inmediatamente por cualquier situación que afecte directamente la validez del certificado.

### e. Obligaciones del Solicitante

Entregar toda la información de identificación personal o de su empresa si es para estos efectos, exigida por la PSC TOC S.A.
El solicitante del certificado deberá cancelar la tarifa establecida y publicada en www.toc.cl.

## 9. Enrolamiento (RA)

A través de los siguientes mecanismos TOC realizará los registros de los suscriptores de certificados de FEA.

## a. Enrolamiento con servicio “Clave Única”

Se realiza una validación de la identidad a través del mecanismo digital “ClaveÚnica” para obtener los datos del suscriptor del certificado. Además como segundo factor de autenticación el suscriptor deberá elegir una de las siguientes opciones:

- Validación biométrica de la identidad con cédula de identidad
- Ingreso de OTP o clave de coordenadas de otras instituciones integradas y aprobadas por TOC.

## b. Enrolamiento Biométrico

Se realiza una validación de la identidad y se obtienen los datos del suscriptor a través de las tecnologías de verificación de identidad de TOC, remotas o presenciales, utilizando como sustento la cédula de identidad nacional. Considerando que se necesita la comparecencia del suscriptor (presencial) al Servicio de Registro Civil e Identificación para obtener su cédula de identidad, se da cumplimiento a lo reglamentado en la letra e) del artículo 12 de la ley Nº 19.799 sobre 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 trata de

persona jurídica. Para este método de enrolamiento biométrico además se utilizan como segundo factor una prueba de vida al momento de obtener la característica biométrica del suscriptor y también la validación de vigencia y/o bloqueo de la cédula de identidad utilizando el convenio de servicios vigente entre TOC y el Servicio de Registro Civil e Identificación.

## c. Enrolamiento en oficinas de TOC

El suscriptor se debe presentar en oficinas de TOC (Avenida Santa María 2670, comuna de Providencia) o en dependencias de alguno de sus representantes a lo largo del territorio nacional. Se realiza una comprobación del documento de identidad del suscriptor, se realiza una validación de la identidad y se obtienen los datos del suscriptor a través de las tecnologías de verificación de identidad de TOC, se valida vigencia de la cédula de identidad y se registran sus datos. Se genera certificado y se almacena en dispositivo token, finalmente el suscriptor firma ficha de enrolamiento y recibe el dispositivo con certificado digital

### d. Enrolamiento en Notarías

El suscriptor se presenta ante un notario, presentando una ficha de solicitud de enrolamiento valida y autorizada por TOC. El suscriptor debe incluir sus datos (de su cédula de identidad) en la ficha, esto deben ser validados y la ficha firmada por el notario. El suscriptor debe enviar esta ficha por correo a oficinas de TOC a través de una carta certificada.
Se realiza una comprobación de los datos que contiene la ficha, se valida la identidad y datos se realiza registro del suscriptor. Se genera certificado y se almacena en dispositivo token, finalmente se entrega dispositivo en la dirección particular del suscriptor y este firma documento donde este último manifiesta su conformidad.

## 10. Lista de certificados revocados y estructura de información

Dentro del sitio corporativo de TOC S.A. www.toc.cl se encuentran disponible y con acceso público el registro de certificados emitidos y revocados, incluye todo los tipos de certificados que emite la Autoridad de Registro TOC S.A.

### a. Lista de Certificados de revocación

- FEA G1: https://firma.toc.cl/pki_certificados_revocados.php
- FEA G2: http://firma.toc.cl/crl
- FEA BIO GE: http://firma.toc.cl/crl_fea_bio_g1.crl
- FES: http://firma.toc.cl/crl_fes

### b. Confianzas en las Firmas

Las personas que reciben alguna firma electrónica realizada con un certificado emitido por TOC

S.A. 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.

### c. Confianza en los certificados

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

## 11. Protección de información

TOC S.A. tiene por definición como confidencial, toda la información relevante a sus suscriptores, solicitante y se compromete a no utilizar esta información en otros aspectos que sean exclusivamente relacionados con su actividades de certificación. La entrega de esta información a terceros está estrictamente regida de la siguiente forma.

### a. Información que puede entregar

TOC S.A. emite certificados según la ley 19.799 y todos sus procedimientos técnicos exigidos, por lo que en cada certificado emitido, en ellos se encuentran:

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

Para el caso de la información de certificados emitidos y revocados emitidos por TOC S.A. se encuentran disponibles en www.toc.cl

### b. Casos particulares de entrega de información de titulares de certificados

TOC S.A. 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

# 12. Declaración Operacional

## a. Registro Inicial

Dentro de los procedimientos de suscripción de firma electrónica a los clientes de TOC, para personas naturales se registra el nombre completo, en formato, "Nombres" más "Apellido Paterno" y "Apellido Materno", exigiendo copia de cedula identidad Nacional .

En caso de personas jurídicas se deben registrar todos los antecedentes legales correspondientes y exigidos por la ley.
Para realizar una identificación fehaciente de los solicitantes, esta documentación debe ser presentada personalmente en las oficinas de TOC S.A.
TOC S.A. publica los requisitos para gestionar cada tipo de certificado.

## b. Reemisión de certificados

Los certificados emitidos por TOC S.A. tendrán dos estados:

- Vigentes
- Revocados

La reemisión de llaves no está permitida con el claro objetivo de mantener el no repudio de los certificados emitidos por TOC S.A.

Lo mismo ocurre para el caso de los certificados revocados, no reemitirá llaves con un certificado en este último estado.

## c. Revocación

Las solicitudes de revocación se realizarán a través de un correo electrónica a soporte@toc.cl o en la página web de TOC S.A, www.toc.cl. La revocación es un mecanismo de seguridad que posee la CPS para dejar de confiar en un certificado digital, y responde a distintas causas:

- Solicitud del Suscriptor
- Perdida del certificado o alteración física del dispositivo que almacena el certificado.
- Que la actual CPS comience el proceso de término de acreditación de emisor de certificados de firma electrónica avanzada.
- Fallecimiento del suscriptor o de algún representado, termino 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.

## d. Formas de Revocación

El proceso de revocación es activado o ejecutado por solicitud previa, por cualquiera de los canales que posee la CPS para estos efectos, o por la concurrencia de:

- El suscriptor del certificado
- La persona jurídica a la cual fue emitido el certificado

## e. Canales de atención para la revocación de Certificados

- Comunicación telefónica para el contacto inicial y comienzo del proceso de revocación, al número: **(+562) 2946 5752**
- Mediante correo electrónico: **soporte@toc.cl**
- Vía servicio web: 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.

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

## g. Caducidad de los Certificados

Luego de finalizado el periodo de vigencia del certificado, éste caducará en forma automática, indicando por la PSC al suscriptor en forma anticipada la fecha de caducidad del mismo, para que el suscriptor tenga en pleno conocimiento del estado de su certificado y que decida en forma preventiva que decisión, la 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.

## h. Renovación de los Servicios de Certificación

El procedimiento de renovación se ejecuta cuando el Certificado del suscriptor este próximamente a caducar y el Suscriptor 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 S.A. tienen un plazo de vigencia de un año. Para la renovación, se deben cumplir algunos requisitos:

- Existencia de actividad de certificación previa en esta PSC por parte del suscriptor y emitido por TOC S.A.
- El suscriptor solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a TOC S.A. en los procedimientos declarados para esos efectos.
- 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.

## i. Solicitud Renovación

El suscriptor al momento de solicitar la renovación, lo deberá hacer en 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, básicamente, es la emisión de un nuevo certificado que reemplace por el certificado vencido o próximo a vencer.
- El certificado anterior, no es necesario la revocación, ya que por restricciones de fechas imposibilitará su uso.

## j. Procedimiento de Renovación

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

- La PSC emitirá el certificado solicitado
- La emisión del certificado emitirá un correo electrónico al solicitante.
- En el correo se informará que el certificado está disponible y que puede ser descargado desde el sitio Web www.toc.cl
- 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 la PSC siguen el mismo estado de la contratación o emisión anterior, y además las políticas de certificación vigentes.

## k. Termino de actividades de la PSC

Con el claro objetivo de hacer el menor daño posible a los 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:
  - **i.** Notificar con correo certificado o correo ordinario el cese de las actividades
  - **ii.** Publicación de anuncio de cese de actividades en dos diarios de divulgación nacional.
- Todas las actividades 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 y que alguna PSC existente posea los procedimientos de transferencias de obligaciones, esto se realice 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, dar como 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.

## l. Auditorías

Los procesos y frecuencias de auditorías esta regidos por las guías de acreditación y auditorias de la entidad acreditadora dependiente del Ministerio de Economía.

## m. 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.

## n. Publicación de Modificaciones

Toda modificación en la operación de la CPS o en alguna política que involucre directamente la operación o cambios en los certificados emitidos, debe ser informada 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. Si el comunicado no recibe alguna declaración por escrito de los suscriptores o solicitantes, manifestándose contrarios a las modificaciones anunciadas, éstas se declararán como aceptadas por la comunidad usuarios de la CPS.