

70E

DECLARACIÓN DE  
PRÁCTICAS DE  
CERTIFICACIÓN

# Índice

<b>I. Control de Cambios</b> .....	<b>2</b>
<b>II. Introducción</b> .....	<b>3</b>
Generalidades	
<b>III. Alcance</b> .....	<b>4</b>
<b>IV. Referencias y estándares Internacionales</b> .....	<b>6</b>
<b>V. Glosario</b> .....	<b>8</b>
<b>VI. Aplicabilidad y Comunidad de Usuarios</b> .....	<b>8</b>
Comunidad de Usuarios	
Aplicabilidad	
<b>VII. Tipos y usos de Certificados</b> .....	<b>10</b>
Contenido de los certificados:	
<b>VIII. Detalle de contacto</b> .....	<b>10</b>
Dirección de Contacto. Contacto Telefónico. Contacto Web.	
<b>IX. Requerimientos Generales y Operacionales</b> .....	<b>11</b>
Obligaciones de CA Raíz	
Obligaciones de CA	
Obligaciones con los suscriptores	
Obligaciones del suscriptor	
Obligaciones generales de TOC S.A. como PSC	
Obligaciones del Solicitante	
Certificados de firma electrónica avanzada:	
Certificados de firma electrónica tributaria	
Certificados de firma electrónica Simple:	
Confianzas en las Firmas	
Confianza en los certificados	
<b>X. Protección de información</b> .....	<b>15</b>
Información que puede entregar	
Casos particulares de entrega de información de titulares de certificados	
<b>XI. Declaración Operacional</b> .....	<b>16</b>
<b>Declaración de Prácticas de Acreditación</b>	
Registro Inicial	
Reemisión de certificados	
Revocación	
Posibles causas de Revocación:	
Formas de Revocación	
Canales de atención para la revocación de Certificados:	
Publicación de Revocación	
Caducidad de los Certificados	
Renovación de los Servicios de Certificación	
Solicitud Renovación	
Procedimiento de Renovación	
Termino de actividades de la PSC	
Auditorias	
Administraciones y modificaciones	
Publicación de Modificaciones	

## Control de Cambios

Versión	Fecha	Revisión	Observaciones
1.0	31/10/2017	1.0	Primer Documento
1.1	30/01/2023	1.0	Revisión

Observaciones	Fechas
Elaborado por: Comité de Seguridad de la Información	31/10/2017
Consultora de Seguridad de la Información	
Revisado por: Comité de Seguridad de la Información	
Autorizado por: Gerente General TOC PERÚ S.A.C.	
Fecha Publicación	
Representante Legal	
Oficial de Seguridad	
Gerente Operaciones/TI	

## Introducción

---

TOC PERÚ S.A.C. 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 (PKI). Esto principalmente se debe a que su infraestructura es regida con todos los estándares internacionales en referencia con este tipo de tecnología y los estándares de Seguridad de la Información.

Un prestador de servicios de Certificación (PSC), por definición, es una institución o persona, ya sea pública o privada que presta servicios de certificación y pueda 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.

### Generalidades

La política de certificación, es la descripción detallada de las normas y prácticas, como administra los servicios de certificados de firma electrónica, como 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.

De igual forma describiremos 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 Entidades de Registro, Suscriptores y Usuarios dentro del ámbito que regula la PSC de TOC.
- ✓ Revisiones de Auditoria, 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 auditoria, 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

## Alcance

---

Detallar las Prácticas de Certificación, utilizando la infraestructura de llave pública (PKI) de TOC, que a nivel internacional viene obligada al cumplimiento de requerimientos marcados en la legislación vigente como prestadora de servicios de certificación digital. En este contexto se podrá certificar como Entidad de Certificación dentro de todo aquel país que valide que el proceso de certificación en el cual TOC fue acreditado, es absolutamente equivalente para que pueda emitir certificados de firma electrónica avanzada, como lo son

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

En estas políticas de acreditación se encuentran todas las actividades, declaraciones que rigen las siguientes normas y reglamentos:

- ✓ Ley N° 27269.- Ley de Firmas y Certificados Digitales.
- ✓ Ley N° 27310.- Modificatoria de la Ley N° 27269.
- ✓ Ley N° 28403.- Dispone la recaudación de un aporte por supervisión y control anual por parte del INDECOPI de las Entidades de Certificación y de Verificación/Registro de Firmas.
- ✓ Decreto Supremo N° 052-2008-PCM.- Reglamento de la Ley de Firmas y Certificados Digitales.
- ✓ Decreto Supremo N° 070-2011-PCM.- Decreto Supremo que modifica el Reglamento de la Ley 27269 y establece normas aplicables al Procedimiento Registral en virtud del Decreto Legislativo N° 681 y ampliatorias.
- ✓ Decreto Supremo N° 105-2012-PCM.- Decreto Supremo que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N° 052-2008-PCM.
- ✓ Decreto Supremo N° 026-2016-PCM.- Aprueban medidas para el fortalecimiento de la Infraestructura Oficial de Firma Electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado
- ✓ Resolución de la Presidencia del Consejo Directivo del INDECOPI Nro. 39-2017-INDECOPI/COD
- ✓ Aprueban el Reglamento de Infracciones y Sanciones aplicable a los Prestadores de Servicios de Certificación Digital

- ✓ Resolución N° 123-2016/CFE-INDECOPI de la Comisión Transitoria para la Gestión de la IOFE.- Se establecen los plazos de vigencia del algoritmo SHA-1 dentro del marco de la IOFE
- ✓ Resolución N° 042-2016/CFE-INDECOPI de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica.- Se establece un plazo de vigencia de cuatro años para los certificados digitales que cuenten con claves de 2048 bits de longitud, siempre que en el proceso de cifrado se utilice el algoritmo de encriptación SHA-256.
- ✓ Procedimiento para Auditoria Anual de los Prestadores de Servicios de Certificación Digital.-Procedimiento para Auditoria Anual de los Prestadores de Servicios de Certificación Digital – PE CFE-01
- ✓ Procedimiento para la Evaluación, Calificación y Registro de Auditores de los Prestadores de Servicios de Certificación Digital.- Procedimiento para la Evaluación, Calificación y Registro de Auditores de los Prestadores de Servicios de Certificación Digital - PE-CFE-02
- ✓ Guías de Acreditación de las Prestadoras de Servicios de Certificación Digital:
- ✓ El Reglamento de Firmas y Certificados Digitales, aprobado por el Decreto Supremo N° 019-2002-JUS, designó al INDECOPI como la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Digital. Esta condición fue ratificada por el Reglamento que reemplazó a aquel, aprobado por el Decreto Supremo N° 004-2007-PCM publicado el 14 de enero de 2007 en el diario oficial El Peruano, así como por el Reglamento vigente, sancionado por el Decreto Supremo N° 052-2008-PCM, publicado el 19 de julio de 2008. En tal condición, el INDECOPI –a través de la Comisión de Reglamentos Técnicos y Comerciales– ha aprobado: 1) la Guía de Acreditación para Entidades de Certificación Digital; 2) la Guía de Acreditación para Entidades de Verificación/ Registro de Datos; 3) la Guía de Acreditación para Prestadoras de Servicios de Valor Añadido. Cada guía contiene el conjunto sistematizado de requisitos a ser cumplidos por la empresa u organismo que desee obtener, de la Comisión de Normalización de Fiscalización de Barreras Comerciales No Arancelarias de INDECOPI, su acreditación como Entidad de Certificación Digital, como Entidad de Registro/Verificación de Datos o como Prestadora de Servicios de Valor Añadido. Las guías fueron elaboradas por un equipo de consultores que fue contratado gracias al financiamiento del Programa de Modernización y Descentralización del Estado de la Presidencia del Consejo de Ministros. Entre sus principales características destacan: Se encuentran ajustadas a la Ley de Firmas y Certificados Digitales (N° 27269), al Reglamento de la misma y a las normas técnicas internacionales sobre la materia. Cada uno de los requisitos de acreditación señalados en las guías contiene la referencia correspondiente a la ley, al reglamento y las normas técnicas internacionales pertinentes; Recogen las

principales observaciones formuladas por el Registro Nacional de Identificación y Estado Civil (RENIEC), que fue la única institución que presentó observaciones durante el período de discusión pública de los proyectos; El documento principal –el proyecto de Guía de Acreditación de Entidades de Certificación Digital– fue revisado por la consultora canadiense ENTRUST, que tuvo participación en el diseño de la Infraestructura de Firma Digital de la administración del Estado del Canadá. Se debe indicar que las sugerencias de ENTRUST compatibles con la normativa peruana sobre la materia fueron incorporadas al proyecto. Finalmente, es pertinente recordar que, según la Ley y el Reglamento de Firmas y Certificados Digitales, los documentos electrónicos (contratos, ofertas, oficios, cartas, etcétera) que lleven firma digital basada en un certificado digital emitido por una entidad acreditada ante el INDECOPI, tendrán el mismo efecto jurídico que un documento manuscrito. Guías de Acreditación para Entidades de Certificación Digital y Entidades Conexas. Toda referencia que en ellas se efectúe a la Comisión de Reglamentos Técnicos y Comerciales, deberá entenderse realizada a la Comisión de Normalización y Fiscalización de Barreras Comerciales No Arancelarias del INDECOPI.

Todos los procedimientos definidos en este Alcance se aplican a la Entidades de Certificación, Entidad de Registro PSC, Solicitantes y Titulares, para la emisión de Certificados por parte de TOC PERÚ S.A.C.

## Referencias y estándares Internacionales

---

### 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.

**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.

**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.

**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.



## 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 irreplicable 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.
- ✓ **Subscriber de un Certificado:** Corresponde a la persona o empresa a la cual se emitió el certificado. Este subscriber posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el subscriber es la persona que tiene en su absoluto control el certificado de firma electrónica.
- ✓ **Entidad de Registros o Verificación:** Es la persona o empresa que puede verificar la identidad de los solicitantes.
- ✓ **Entidad de certificación (EC):** persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
- ✓ **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por TOC PERÚ S.A.C. y hace uso de ellos.

## Aplicabilidad y Comunidad de Usuarios

---

### 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 TOC requerirá asegurar la identidad del interesado o suscriptor requiriendo identificar completamente ante la Entidad de Registro, con presencia física.

## Aplicabilidad

Los certificados emitidos por la Entidad Certificadora TOC PERÚ S.A.C. 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.

Los certificados emitidos por TOC PERÚ S.A.C. 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 Entidad 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 PERU S.A.C 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 Entidad de Registro TOC PERU S.A.C permite validar que el elemento firmado no cambia su contenido entre el origen y el destino.
Privacidad	Los certificados emitidos por la Entidad de Registro TOC PERU S.A.C, permiten cifrar elementos que solo pueden ser visualizados por el Titular de los datos de Creación de Firma Electrónica

## Tipos y usos 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, también emite certificados de firma electrónica tributaria y también certificados de firma simple.

Los certificados de firma electrónica definidos por TOC son:

- ✓ Certificados de firma electrónica acreditada
- ✓ Certificados de firma electrónica tributaria
- ✓ Certificados de firma electrónica simple

### Contenido de los certificados:

La estructura de los certificados emitidos por la Entidad de Registro TOC PERU S.A.C cumple y es compatible con el estándar ISO/IEC 9594-8 y el contenido de cada certificado cumple con el Reglamento de la LEY N° 27269.

Estructura de los Certificados emitidos por TOC :

- ✓ DNI
- ✓ Correo electrónico
- ✓ Nombre Completo
- ✓ Tipo de certificado
- ✓ Datos de la acreditación de TOC.

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

## Detalle de contacto

---

### Dirección de Contacto

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

TOC PERU SAC tiene su oficina en Malecón Costa Sur 400, Int 102, Chorrillos, Lima, Peru

## **Contacto**

Pueden contactar al equipo de TOC PERU SAC al email: contacto@toc.pe

## **Requerimientos Generales y Operacionales**

---

*Obligaciones:*

### **Obligaciones de Entidad Certificadora 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 EC, 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 este caso, TOC PERU S.A.C. o cualquier otra entidad de certificación subsiguiente (Sub EC) a la jerarquía de certificación de TOC S.A., éste último firmará los certificados emitidos por TOC S.A.

### **Obligaciones de Entidad de Certificación.**

TOC PERU S.A.C como cumple con las obligaciones necesarias y legales para prestar servicio de certificación electrónica avanzada, como, por ejemplo:

- ✓ 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 claros 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 PERU S.A.C emitirá certificados que sean solicitados, previa aprobación de los antecedentes necesarios de la persona o representante de una empresa.
- ✓ Administración de llaves:
  - TOC PERU S.A.C emite en forma automática toda llave pública y privada que se le entrega a cada titular de certificado. Con el hecho de que las llaves se generan automáticamente, esto garantiza su total confidencialidad.

### 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
- ✓ Tener disponibilidad de la lista de certificados revocados que está constantemente actualizada.
- ✓ Tener los procedimientos y políticas adecuadas para resguardar la llave privada de cada suscriptor.

### Obligaciones del suscriptor

- ✓ Conservar y dar uso adecuado del certificado
- ✓ 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 PERU S.A.C está autorizada para cualquier modificación, si es necesaria cualquier modificación debe ser informada a TOC PERU S.A.C en sus oficinas Malecon Costa Sur 400, Int N° 102, Chorrillos, Lima, Peru.
- ✓ Informar a la PSC inmediatamente por cualquier situación que afecte directamente la validez del certificado.
- ✓ Realizar el uso adecuado del certificado, según lo descrito en el contrato de suscriptor

**Obligaciones generales de TOC PERU S.A.C como PSC**

- ✓ TOC PERU S.A.C tiene políticas claras en cuanto al uso de infraestructura de llaves públicas (PKI) para firma electrónica avanzada y se encuentran publicada en [www.toc.pe](http://www.toc.pe), y de este modo están disponible al público en general.
- ✓ TOC PERU S.A.C si decide 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, y en este caso su certificado quedará en estado revocados.
- ✓ TOC PERU S.A.C cumplirá todas las leyes que rigen este tipo de actividades, por ejemplo, el Código de Protección y Defensa del Consumidor (Ley N° 29571) y sus modificaciones, así como Ley de protección de datos personales - PCM. (Ley 29.733)
- ✓ TOC PERU S.A.C mantiene 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, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma. Este registro lo tendrá disponible electrónicamente por acceso público en el sitio [www.toc.cl](http://www.toc.cl)
- ✓ TOC PERU S.A.C. da cumplimiento en el punto 6 de la resolución exenta N° 9 del 15 de Febrero del 2001 del SII, para certificados para facturación electrónica.
- ✓ TOC PERU S.A.C. debe publicar todas las resoluciones de la entidad acreditadora. Esta publicación será en [www.toc.cl](http://www.toc.cl)
- ✓ TOC PERU S.A.C. informará 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.
- ✓ Cada certificado emitido por TOC PERÚ S.A.C. de firma electrónica avanzada representa la identidad del solicitante, y es por esto que cada solicitud de firma requiere la comparecencia presencial de la persona o representante legal si es persona jurídica, ante sí, notario u oficial de registro civil.
- ✓ TOC PERÚ S.A.C. se compromete a pagar anualmente el arancel de supervisión que realiza la entidad acreditadora.
- ✓ TOC PERÚ S.A.C. se compromete a mantener vigente el seguro de responsabilidad civil que exige ley de firma electrónica acreditada 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.

### **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 PERU S.A.C

El solicitante del certificado deberá cancelar la tarifa establecida y publicada en la web de TOC PERU S.AC. por el certificado que solicite.

#### *Lista de Revocados y estructura de información*

Dentro del sitio corporativo de TOC PERU S.A.C se encuentran el repositorio donde se informan certificados emitidos y revocados, para todos los tipos de certificados que emite la Entidad de Registro TOC PERU S.A.C.

### **Certificados de firma electrónica avanzada:**

Lista de certificados de revocación se encuentra en : [www.toc.cl/dekd](http://www.toc.cl/dekd)

Lista de certificados emitidos se encuentra en: [www.toc.cl/dkekde](http://www.toc.cl/dkekde)

### **Certificados de firma electrónica tributaria**

Lista de certificados de revocación se encuentra en : [www.toc.cl/dekd](http://www.toc.cl/dekd)

Lista de certificados emitidos se encuentra en: [www.toc.cl/dkekde](http://www.toc.cl/dkekde)

### **Certificados de firma electrónica Simple:**

Lista de certificados de revocación se encuentra en: [www.toc.cl/dekd](http://www.toc.cl/dekd)

Lista de certificados emitidos se encuentra en: [www.toc.cl/dkekde](http://www.toc.cl/dkekde)

### **Confianzas en las Firmas**

Las personas que reciben alguna firma electrónica realizada con un certificado emitido por TOC PERU S.A.C 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 utilizo en la firma del elemento, no tenga estado caducado en el momento de la firma.

### **Confianza en los certificados**

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

### **Protección de información**

---

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

#### **Información que puede entregar**

TOC PERÚ S.A.C. 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](http://www.toc.cl)

#### **Casos particulares de entrega de información de titulares de certificados**

TOC PERÚ S.A.C. 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.



## Declaración Operacional

---

### Registro Inicial

Dentro de los procedimientos de suscripción de firma electrónica a los clientes de TOC, se registran los nombres completos, es decir, Nombres y apellido paterno y materno para el caso de personas naturales y/o razón social completa en el caso de empresa.

Junto con lo anterior, se solicita copia de Documento Nacional de Identidad, y para el caso de personas jurídicas, todos los antecedentes legales que corresponden.

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

### Reemisión de certificados

Los certificados emitidos por TOC PERU S.AC. 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 PERU S.A.C

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

### Revocación

Las solicitudes de revocación se realizarán por vía electrónica a certificados@toc.pe o en la página web de la compañía, www.toc.pe. La revocación es un mecanismo que posee la CPS para que por algún motivo se deje de confiar en el certificado.

### Posibles causas de Revocación:

- ✓ 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.

### Formas de Revocación

Principalmente, la revocación es 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

### Canales de atención para la revocación de Certificados:

- ✓ Comunicación telefónica para el contacto inicial y comienzo del proceso de revocación, esto es al número: (+51) 975165669
- ✓ Por mail a: [certificados@toc.pe](mailto:certificados@toc.pe)
- ✓ Vía Web a la dirección: [www.toc.pe/contactanos](http://www.toc.pe/contactanos)

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.

### 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 termino de actividades

de firma electrónica de la PSC, este acto de certificados revocados quedará efectivo inmediatamente después que esto ocurra.

### **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 preventivamente 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.

### **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 PERU S.A.C 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 PERU S.A.C
- ✓ Que el suscriptor solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a TOC PERU S.A.C 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.

### **Solicitud Renovación**

El suscriptor al momento de solicitar la renovación, lo deberá hacer en el formulario para tal efecto, en la página Web [www.toc.pe/contactanos](http://www.toc.pe/contactanos) :

- ✓ 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.

### **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.pe](http://www.toc.pe)
- ✓ 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.

### **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:
  - 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 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.

**Auditorias**

Los procesos y frecuencias de Auditorias esta regidos por las guías de acreditación y auditorias de la entidad acreditadora dependiente del INDECOPI.

**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 CPS o algún cambio en alguna Política que involucre directamente en la operación o cambios en los certificados emitidos, esto 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 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 CPS.