Declaración de Prácticas de Certificación

Documento

Identificación del Documento

Código del documento	DOC-09
Nombre del documento	Declaración de prácticas de Certificación de la EC
Versión vigente	1.0
Clasificación	Pública
Responsable de aprobación	Gerente General

Control de cambios

Versión	Fecha	Observaciones
1.0	31/10/2017	Primer Documento
1.1	30/01/2023	Revisión
1.2	15/08/2024	• Actualización de los apartados “Aplicabilidad y Comunidad de usuarios”, “Aplicabilidad” y “Registro Inicial” para asegurar coherencia con documentos de la ER (en los que ahora se permite la validación de identidad de manera remota a partir de la flexibilización de requisitos de Indecopi del 23/3/2020) • Eliminación a mención al cifrado de certificados, incluida por error en versión previa. • Eliminación de términos no usados en la legislación peruana (Certificados de firma electrónica acreditada, Certificados de firma electrónica tributaria, Certificados de firma electrónica simple, servicio de certificación electrónica avanzada, firma electrónica avanzada, RUT) • Eliminación de alusiones a legislación chilena incluidas por error en versión previa (“resolución exenta No9”; “SII”; “ley No. 19799”) y actualización, cuando corresponde, a referencias a la legislación peruana • Se eliminaron enlaces desactualizados: www.toc.cl/dekd y www.toc.cl/dkekde y se traslada la info correspondiente a la sección 9.3. • Se incluye la URL para solicitar la revocación de certificados https://www.toc.pe/contactanos , el correo electrónico y el link para la CRL correspondiente (sección 9.3 “Revocación”) • Se incluye un procedimiento de obtención de reportes de disponibilidad para el repositorio de CRL y OCSP (sección 9.12 “Disponibilidad del repositorio de CRL y OCSP”) . • Se agregar la sección 9.13. “Pautas para manejo de incidentes y compromisos de operaciones” Ahí se incluye, recogiendo recomendaciones de la auditoría de seguimiento de EC de 2023, un procedimiento para el caso de compromiso de llaves. (9.13.2, página 16)

Contenido

1. 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

2. Alcance

El presente documento detalla 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 digitales. Como 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 Nº 27269.- Ley de Firmas y Certificados Digitales.
- Ley Nº 27310.- Modificatoria de la Ley Nº 27269.
- Ley Nº 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 Nº 052-2008-PCM.- Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo Nº 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 Nº 681 y ampliatorias.
- Decreto Supremo Nº 105-2012-PCM.- Decreto Supremo que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo Nº 052-2008-PCM.
- Decreto Supremo Nº 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
- 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 Nº 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

- Comunicado de Indecopi del 23 de marzo de 2020 por la pandemia de Covid (que permite que la validación de identidad de las personas pueda hacerse de manera remota por causa de la emergencia sanitaria, en https://repositorio.indecopi.gob.pe/handle/11724/7385)
- Guías de Acreditación de las Prestadoras de Servicios de Certificación Digital:
- El Reglamento de Firmas y Certificados Digitales, aprobado por el Decreto Supremo Nº 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 Nº 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 Nº 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 (Nº 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.

3. 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.

4. 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.

- ✓ **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.
- ✓ **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.

5. 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 identificarlo completamente ante la Entidad de Registro, ya sea de manera presencial o remota.

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 uso que pueda derivar en fallecimiento, lesiones a personas, al medio ambiente o infrinja la ley.

Los certificados emitidos por TOC PERÚ S.A.C. podrán ser usados en las siguientes necesidades de seguridad:

Necesidad	Detalle
Autenticación	Dar suficientes garantías respecto a la Identidad del Titular solicitante del certificado. Para esto se debe, o bien requerir la presencia física del futuro suscriptor ante la Entidad de Registro, o bien usar un procedimiento virtual (reunión remota con videollamada y presentación de documentos de identidad) que permita comprobar la identidad del solicitante. Se debe 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, se ponen únicamente a disposición del Titular de los datos de Creación de Firma Electrónica

6. Detalle de contacto

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

7. 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 PERÚ S.A.C se

define como entidad raíz y una entidad intermedia, porque ha emitido un certificado par ser utilizado por el mismo.

Obligaciones de Entidad de Certificación.

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

- ✓ Identificar y autenticar correctamente al suscriptor o 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 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.
- ✓ 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, 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 El Código de Protección y Defensa del Consumidor (Ley Nº 29571) y sus modificaciones, asi como Ley de protección de datos personales - PCM. (Ley 29733)
- ✓ 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.
- ✓ 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 por el certificado que adquiere.

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 que:

- 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

8. 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:

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.

9. Declaración Operacional

9.1. Registro Inicial

Dentro de los procedimientos de suscripción 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 a TOC PERÚ S.A.C., ya sea de manera física o virtual. En ambos casos se realiza una validación de la identidad del solicitante de acuerdo al ordenamiento legal.

9.2. 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.

9.3. Revocación

Las solicitudes de revocación se realizarán por vía electrónica a certificados@toc.pe o en el formulario web https://www.toc.pe/contactanos. La revocación es un mecanismo que posee la CPS para que por algún motivo se deje de confiar en el certificado. La lista de certificados revocados (CRL) es accesible en la URL www.toc.peru/f

9.4. 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.

9.5. 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

9.6. Canales de atención parea 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
- ✓ Vía Web a la dirección: 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.

9.7. 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.

9.8. 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.

9.9. 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.

9.10. 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 :

- ✓ 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.

9.11. 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.
- ✓ 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.

9.12. Disponibilidad del repositorio de CRL y OCSP

TOC PERU implementará una solución para obtener reportes de disponibilidad de CRL y OCSP (según recomendación de auditoría complementaria de seguimiento de EC de 2024).

Para el primer caso, se trata de un script que revisará cada 15 minutos que la CRL esté en línea ejecutando una consulta *GET* del archivo.
Para el segundo se generará un script que con OpenSSL consulte el estado de un certificado *dummy.*

9.13. Pautas para manejo de incidentes y compromiso de operaciones

El Plan de Recuperación de Desastres de TOC PERU S.A.C. incluye procedimientos para la gestión de contingencias en caso de falla o interrupción de algún servicio En el procedimiento se establecen mecanismos de comunicación, registro y respuesta ante incidentes, indicando la acción que ha de emprenderse. Los incidentes son comunicados, tan pronto se haya tomado conocimiento, al Oficial de Seguridad de Información de la empresa, para que se tomen acciones para reducir el impacto de estos.

9.13.1. Acciones en caso de corrupción de datos, software y/o recursos computacionales

Se encuentran identificadas fuentes alternativas de recursos computacionales, software y datos para su uso en los casos de adulteraciones o fallas.

9.13.2. Procedimiento en caso de compromiso de llave privada

En caso de que alguna llave privada que administra la EC resultase comprometida de manera real o potencial, el certificado digital será inmediatamente revocado, notificándose el hecho en un lapso máximo de 24 horas a la AAC. Todos los certificados digitales subordinados emitidos en el periodo comprendido entre el compromiso de la llave y la cancelación del certificado serán también cancelados, lo cual se comunicará a los suscriptores afectados.

9.14. Término 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.

10. Auditorias

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

11. 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.

12. 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.