Firmado digitalmente por:
ALEXANDER PASCUAL DE FEUDIS KOCKOVA
Área: RUC:20547367112
Empresa: TOC PERU S.A.C.

Entidad de Certificación

OID 1.3.6.1.4.1.53748.1.1.002

Políticas de Certificación y Declaración de Prácticas de Certificación de TOC PERU S.A.C.

Información del documento

Nombre	POLÍTICA DE CERTIFICACIÓN
Realizado por	TOC PERU S.A.C.
Dirigido a	INDECOPI
Versión	2.0
OID	1.3.6.1.4.1.53748.1.1.002
Actualización	Anual
Fecha	22/12/2021

Historial de versiones

Versión	Fecha	Descripción
1.0	02/10/2018	Elaboración de documento inicial.
2.0	30/12/2021	Actualización. Se agrupó en un solo documento las: Políticas de Certificación y Declaración de Prácticas de Certificación de TOC PERU S.A.C.
2.0	30/09/2022	Revisión

Contenido

1. INTRODUCCIÓN

TOC PERU S.A.C. (en adelante TOC PERÚ) es una empresa peruana dedicada a propiciar el aumento de la productividad y eficiencia de las empresas, instituciones y comunidades del país a través del uso de herramientas tecnológicas de alta confiabilidad en telecomunicaciones y gestión de la información. TOC PERÚ aprovecha la capacidad de Internet y las redes de telecomunicación en general, así como modernas técnicas de seguridad informática, para realizar transacciones e intercambio de información a distancia de manera ágil, eficiente y segura.

Para llevar a cabo los servicios de certificación digital, TOC PERÚ cuenta con el respaldo de TOC SA (en adelante TOC SA), quien provee los servicios de emisión, distribución y revocación de certificados digitales.

Dentro de los servicios que ofrece TOC PERÚ se encuentra la autenticación de sus clientes, tanto en el caso de personas jurídicas como naturales; y el registro de evidencias de dicha verificación.

2. OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza TOC PERÚ para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

3. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por TOC PERÚ a través de la infraestructura provista y administrada por la empresa TOC SA.

TOC PERÚ representa a TOC SA para todos los aspectos de mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación TOC SA.

La responsabilidad y garantías por los servicios de certificación digital son asumidas por TOC SA.

4. DEFINICIONES Y ABREVIACIONES

A efectos del documento de Prácticas de Certificación, las expresiones que se pasan a indicar a continuación tendrán el alcance y/o significado que se pasa a indicar en cada caso:

4.1. Definiciones

- **Prestador de Servicios de Certificación:** Es aquella entidad que en conformidad con la
- legislación vigente emite certificados de firma electrónica y/o digital.
- **Autoridad de Registro:** Es TOC PERU personalmente o representada a través de un mandatario, para la comprobación fehaciente de la identidad de los solicitantes de certificados.
- **Certificado:** Certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica

- **Certificado raíz:** Certificado cuyo suscriptor es TOC PERÚ y pertenece a la jerarquía que TOC PERÚ presenta como Prestador de Servicios de Certificación.
- **Clave:** Secuencia de símbolos.
- **Datos de creación de firma:** Son datos únicos que el suscriptor utiliza para crear la Firma electrónica y que se encuentran inequívocamente unidos a la clave pública contenida en el certificado de firma electrónica o digital.
- **Clave Pública:** Son los datos que se utilizan para verificar la Firma electrónica y que se
- encuentran inequívocamente unidos a los datos de creación de firma.
- **Declaración de Prácticas de Certificación:** Declaración de TOC PERÚ, respecto a aquellas prácticas, a nivel de sistemas y de personal, que en base a sus buenas prácticas dan seguridad y confianza a los certificados y servicios provistos por TOC PERÚ.
- **Firma electrónica o digital:** Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría (esto último en caso de firmas digitales)
- **Listas de Revocación de Certificados:** Registro de acceso público de certificados, en el que quedará constancia de los certificados que han perdido su vigencia por haber sido revocados.
- **Número de serie de Certificado:** Valor entero y único que está asociado inequívocamente con un certificado expedido por TOC PERÚ.
- **OCSP (Online Certificate Status Protocol):** Protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- **Prestador de Servicios de Certificación (PSC):** Es aquella entidad que en conformidad con la legislación, emite certificados de firma electrónica.
- **Política de Certificación:** Es el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes y que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por TOC PERÚ para emitir Certificados.
- **Solicitante:** Persona que solicita la emisión de un certificado de firma electrónica o digital
- dando cumplimiento a las exigencias establecidas en la Ley y en esta Declaración de Prácticas de Certificación.
- **Suscriptor:** Es la persona cuya identidad personal ha quedado vinculada a los datos de creación de firma, a través de una clave pública certificada por el Prestador de Servicios de Certificación TOC PERÚ.
- **Terceras partes que confían:** Aquellas personas que voluntariamente depositan su confianza en un certificado de TOC PERÚ, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.

4.2. Acrónimos

- EC: Entidad Certificadora
- ACR: Autoridad Certificadora Raíz
- ER: Entidad de Registro
- CA: Certification Authority
- CP: Certificate Policy

- CP-FA: Políticas de Certificado de Firma Electrónica y Digital
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- DNI: Documento Nacional de Identificación
- FIPS: Federal Information Processing Standard
- HSM: Hardware Security Module

5. PARTICIPANTES

5.1. ENTIDAD DE CERTIFICACIÓN TOC PERÚ (EC TOC PERU)

TOC PERÚ, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

5.2. ENTIDAD DE REGISTRO TOC PERÚ (ER TOC PERÚ)

TOC PERÚ brinda también los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

5.3. PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (TOC SA)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación TOC S.A, cuando la Entidad de Certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que se ofrecen son provistos por TOC SA.

5.4. TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS de TOC SA.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por TOC SA como prestador de servicios de TOC PERÚ.

5.5. SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad del suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.6. SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo esta CPS.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

5.7. TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden confiar en los certificados digitales emitidos por la Entidad de Certificación TOC SA a un titular. El Tercero que confía, a su vez puede ser o no titular.

5.8. ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

6. SERVICIOS DE CERTIFICACIÓN DIGITAL

TOC PERÚ brinda los servicios de emisión, revocación y distribución de los certificados de TOC SA.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y la Política de Certificación de TOC SA: https://firma.toc.cl/indexpki.php

6.1. TIPOS DE CERTIFICADO

TOC SA emite para TOC PERU S.A.C los siguientes tipos de certificado:

6.1.1. Personas Naturales

Los certificados de Firma Electrónica se emitirán según el estándar X.509v3 [1] y deberán incluir la siguiente información individual:

Campo	Descripción/Observación	Valor de Ejemplo
Versión (versión)	**Versión correspondiente a estándar X.509 del certificado de Firma Electrónica del Titular**	**V3 (0X2)**
Número de Serie (serial Number)	**Número de Serie Único del certificado X509**	**[NÚMERO DE SERIE ÚNICO]**
Algoritmo de Firma (Signature)	**Identificados del Algoritmo y función de Hash utilizada por la Autoridad Certificadora al firma el Certificado X509**	**SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)**
Emisor (Issuer)	**Nombre Distintivo (DN) del emisor.**	**[DN de la Subordinada que Firma el Certificado Final]**
Vigencia	**Fecha y Hora de inicio y fin vigencia del Certificado de Firma Electrónica en formato utc Time.**	**[FECHA DE INICIO]** **[FECHA DE EXPIRACIÓN]**

Sujeto (Titular)	**Nombre Distintivo del Titular.** ● **SerialNumber se utilizará para incorporar el DNI del Titular.**	**CN = [Nombre Completo Titular]** **email Address = [Email Declarado]** **SerialNumber = [DNI en el siguiente formato: DNI:[XXXXXXX]** **Location = [CIUDAD]** **C = PE**
Clave Pública	**Clave Pública del Titular del Certificado**	**RSA Encryption (1.2.840.113549.1.1.1)** **Largo: 2048 bits o superior**
Extensión - Uso de Clave	**Uso de Clave RSA (2.5.29.15)**	**Digital Signature, Non-Repudiation**
Extensión – Lista de Revocación punto de publicación	**URI de la Lista de Distribución**	**CRL Distribution Points (2.5.29.31)** **URI =**

6.1.2. Representantes Legales

Los certificados de Firma Electrónica para Representantes Legales se emitirán según el estándar X.509v3 y deberán incluir la siguiente información individual:

Campo	Descripción/Observación	Valor de Ejemplo
Versión (versión)	**Versión correspondiente a estándar X.509 del certificado de Firma Electrónica del Titular**	**V3 (0X2)**
Número de Serie (serial Number)	**Número de Serie Único del certificado X509**	**[NÚMERO DE SERIE ÚNICO]**
Algoritmo de Firma (Signature)	**Identificados del Algoritmo y función de Hash utilizada por la Autoridad Certificadora al firma el Certificado X509**	**SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)**
Emisor (Issuer)	**Nombre Distintivo (DN) del emisor.**	**[DN de la Subordinada que Firma el Certificado Final]**
Vigencia	**Fecha y Hora de inicio y fin vigencia del Certificado de Firma Electrónica en formato utc Time.**	**[FECHA DE INICIO]** **[FECHA DE EXPIRACIÓN]**

Sujeto (Titular)	**Nombre Distintivo del Titular.** ● **serialNumber se utilizará para incorporar el DNI ante.del Represent**	**CN = [Nombre Completo Titular]** **email Address = [Email declarado]** **SerialNumber = [DNI en el siguiente formato: DNI:XXXXXXX]** **O = [Nombre de la Institución Representada]** **OU = [RUC de la Institución Representada formato: RUC:XXXXX]** **OU = [Cargo del Represente]** **OU = Validado por TOC Peru SAC** **Location = [CIUDAD]** **C = PE**
Clave Pública	**Clave Pública del Titular del Certificado**	**RSA Encryption (1.2.840.113549.1.1.1)** **Largo: 2048 bits o superior**
Extensión - Uso de Clave	**Uso de Clave RSA (2.5.29.15)**	**Digital Signature, Non-Repudiation**
Extensión – Lista de Revocación punto de publicación	**URI de la Lista de Distribución**	**CRL Distribution Points (2.5.29.31)** **URI =**

6.1.3. Empresas

Los certificados de Firma Electrónica para Empresas emitirán según el estándar X.509v3 y deberán incluir la siguiente información individual:

Campo	Descripción/Observación	Valor de Ejemplo
Versión (versión)	**Versión correspondiente a estándar X.509 del certificado de Firma Electrónica del Titular**	**V3 (0X2)**
Número de Serie (serial Number)	**Número de Serie Único del certificado X509**	**[NÚMERO DE SERIE ÚNICO]**
Algoritmo de Firma (Signature)	**Identificados del Algoritmo y función de Hash utilizada por la Autoridad Certificadora al firma el Certificado X509**	**SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)**
Emisor (Issuer)	**Nombre Distintivo (DN) del emisor.**	**[DN de la Subordinada que Firma el Certificado Final]**
Vigencia	**Fecha y Hora de inicio y fin vigencia del Certificado de Firma Electrónica en formato utc Time.**	**[FECHA DE INICIO]** **[FECHA DE EXPIRACIÓN]**

Sujeto (Titular)	**Nombre Distintivo del Titular.** ● **SerialNumber se utilizará para incorporar el RUC de la Empresa.**	**CN = [Nombre Empresa]** **email Address = [Email declarado del Suscriptor]** **SerialNumber = [RUC en el siguiente formato: RUC:XXXXXXX]** **O = [Nombre Completo del Suscriptor]** **OU = [TIPO DE DOCUMENTO y NÚMERO del Suscriptor en Formato TIPODOC:XXXXXX]** **OU = [Cargo del Representante]** **OU = Validado por TOC Peru SAC** **Location = [CIUDAD]** **C = PE**
Clave Pública	**Clave Pública del Titular del Certificado**	**RSA Encryption (1.2.840.113549.1.1.1)** **Largo: 2048 bits o superior**
Extensión - Uso de Clave	**Uso de Clave RSA (2.5.29.15)**	**Digital Signature, Non-Repudiation**
Nombre Alternativo del Sujeto - Email	**2.5.29.17 RFC 822 Name**	**Email de la Empresa**
Extensión – Lista de Revocación punto de publicación	**URI de la Lista de Distribución**	**CRL Distribution Points (2.5.29.31)** **URI =**

7. RESPONSABILIDADES DE TOC PERÚ

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por TOC SA a sus clientes, TOC PERÚ actúa de la misma manera en el territorio peruano, obteniendo cobertura de seguros sobre sus servicios profesionales, o garantías bancarias que respalden sus operaciones.

TOC PERÚ representa a TOC SA para todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación.

Asimismo, TOC PERÚ brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por TOC SA, son recibidas directamente por TOC PERÚ. La línea telefónica y correo electrónico para la atención a titulares y terceros para consultas relacionadas con el servicio que brinda TOC PERÚ, se indica en la sección Persona de contacto del presente documento.

8. RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por TOC PERÚ, son responsables de revisar la presente CPS y las Políticas de Certificación, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

9. USO DEL CERTIFICADO

9.1. USO PERMITIDO DEL CERTIFICADO

El uso adecuado de los Certificados emitidos se encuentra especificado en la Política General de Certificación de TOC SA cumpliendo con los estándares mínimos exigidos por la AAC conforme a la RFC 3647, los certificados emitidos bajo esta CPS pueden ser utilizados con los siguientes propósitos:

Autenticación del cliente. El Titular del certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.

Firma digital. La utilización del certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.

No repudio. Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

9.2. USO PROHIBIDO DEL CERTIFICADO

En general, cualquier uso que no esté explicado en la sección Uso Permitido del Certificado o en otra sección de este documento es considerado prohibido.

10. PERSONA DE CONTACTO

Datos de la Entidad de Certificación Digital y de Registro:

Nombre: TOC PERU S.A.C.
Dirección: Av. Grau 629 oficina XXX – Barranco
Domicilio: Lima
Teléfono: +51 960114208
Correo electrónico: adefeudis@toc.pe
Página Web: https://www.toc.pe/

Datos de la Entidad Prestadora de Servicios de Certificación Digital:

Nombre: TOC S.A
Dirección: Av. Santa María 2670 - Chile
Teléfono: +562 2946 5752
Correo electrónico: contacto@toc.cl
Página Web: www.tocbiometrics.com

Persona de Contacto

Nombre: Alex de Feudis
Dirección: Av Grau 629 oficina 107 – Barranco
Teléfono: +51 975 165 669
Correo electrónico: adefeudis@toc.pe

11. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y CPS

TOC PERÚ administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la EC de TOC PERÚ.

Para cualquier consulta contactar:

- **Nombre:** Alexander de Feudis
- **Cargo:** Gerente General
- **Dirección de correo electrónico:** adefeudis@toc.pe

12. PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación Digital– CPS de TOC PERÚ, la Política y

Plan de Privacidad, así como la Declaración de Prácticas y Política General de Certificación de TOC PERÚ y otra documentación relevante son publicados en la siguiente dirección: www.toc.pe

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el responsable de la EC de TOC PERÚ antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores de TOC PERÚ, así como la Declaración de Prácticas de las ER con las que tiene filiación serán publicados en la siguiente dirección: www.toc.pe

13. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

En el siguiente enlace se encuentran todo el repositorio referido a las operaciones de TOC SA y TOC PERÚ SAC como EC: https://firma.toc.cl/indexpki.php

14. PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de TOC PERÚ es el encargado de la autorización de la publicación de la CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: www.toc.pe

15. PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación TOC PERÚ durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación TOC PERÚ durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

TOC SA publicará en la página Web, la lista de certificados revocados en los eventos

y con la periodicidad definidas en el numeral Frecuencia de emisión de las CRLs.

Declaración de Prácticas de Certificación (CPS)

Con autorización del Responsable de la Entidad de Certificación de TOC PERÚ y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de la Entidad de Certificación de TOC PERÚ junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

15.1. CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de TOC SA, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de TOC SA, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a TOC SA.

16. IDENTIFICACIÓN Y AUTENTICACIÓN

16.1. TIPOS DE NOMBRES

A todos los suscriptores se les asigna un Nombre Distintivo (DN) de acuerdo con el estándar X.501. Este ADN está compuesto por un Nombre Común (CN), el cual incluye una identificación única del suscriptor como se describe en la sección Certificados del Suscriptor de la Entidad Final, y una estructura de componentes X.501 como se define en sección Reglas para la interpretación de varias formas de nombre.

16.1.1. Certificado raíz de TOC SA como prestador de servicios de TOC PERÚ

La descripción de cada tipo de certificado cubierto por esta CPS, están detallados en la sección Perfiles de certificados, CRL y OCSP.

16.1.2. Certificados de las Subordinadas de TOC SA como prestador de servicios de TOC PERÚ

La descripción de cada tipo de certificado cubierto por esta CPS, están detallados en la sección Perfiles de certificados, CRL y OCSP.

16.1.3. Certificados de titular de TOC SA como prestador de servicios de TOC PERÚ

La descripción de cada tipo de certificado cubierto por esta CPS, están detallados en la sección Perfiles de certificados, CRL y OCSP.

16.2. NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres distintivos (DN) de los certificados emitidos por TOC SA, como prestador de servicios de TOC PERÚ, deben tener significado y la identificación de los atributos asociados al Suscriptor debe encontrarse de forma legible para humanos.

16.3. ANONIMATO Y PSEUDO ANONIMATO DE LOS TITULARES

El uso de anónimos y seudónimos solo se permite en los Nombre Distintivos de la clase de Certificado “FEA”.

16.4. REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

Las reglas utilizadas por TOC SA, como prestador de servicios de TOC PERÚ, para interpretar los nombres distintivos del Emisor y de los Titulares de certificados que emite, es el estándar ISO/IEC 9595 (X.500) Nombre Distintivo (DN).

16.5. SINGULARIDAD DE LOS NOMBRES

Los DN en la TOC SA, como prestador de servicios de TOC PERÚ, deben ser únicos y nunca dar lugar a la ambigüedad entre los suscriptores asociados a una Entidad emisora en particular. Esto se consigue mediante un conjunto de técnicas y procedimientos implementados en varios niveles de la PKI, generalmente mediante la inclusión de una dirección de correo electrónico única por suscriptor.

16.6. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE MARCAS RECONOCIDAS

La inclusión de un nombre en un certificado no implica ningún derecho sobre ese nombre, ni para TOC SA ni la demandante, ni el suscriptor. TOC SA se reserva el derecho de rechazar una solicitud de certificado, o revocar una ya existente, si se detecta un conflicto sobre la propiedad de un nombre.

En cualquier caso, TOC SA no intentará intermediar ni resolver los conflictos respecto a la propiedad de los nombres o marcas.

17. VALIDACIÓN INICIAL DE LA IDENTIDAD

17.1. MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

Si el par de claves es generado por la entidad final (solicitante o futuro suscriptor), a continuación, se solicita una demostración de la posesión de la clave privada asociada a la clave pública. Los medios aceptados son la generación de una solicitud de Firma de certificado (CSR) vinculado a la clave privada, o cualquier otro método aceptado por TOC SA.

Si el par de claves es generado por la EC o la ER, TOC SA define y hace cumplir procedimientos aprobados para transferir de forma segura la clave privada para el suscriptor (es decir, enviar archivos PFX y contraseñas por diferentes canales y eliminar cualquier clave privada de firma una vez que la transferencia es efectiva).

17.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

Los procedimientos de autenticación de la identidad de personas jurídicas son descritos en el documento de Declaración de Prácticas de Registro o Verificación del TOC PERÚ– RPS.

No obstante lo anterior, TOC PERÚ y TOC SA, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

17.3. AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de TOC PERÚ– RPS.

No obstante lo anterior, TOC PERÚ y TOC SA, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

17.4. AUTENTICACIÓN DE LA IDENTIDAD DE SISTEMAS DE INFORMACIÓN

Los procedimientos de autenticación de la identidad de sistemas de información son descritos en el documento de Declaración de Prácticas de Registro o Verificación de TOC PERÚ– RPS.

No obstante lo anterior, TOC PERÚ y TOC SA, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

17.5. INFORMACIÓN DE TITULAR NO VERIFICADA

En general, cualquier información de identidad incluida en el componente Nombre común en el Certificado “FEA”.

Otra información no verificada del suscriptor, si se presenta, se hará relevante como un aviso en un componente de Unidad organizativa (OU) del certificado.

17.6. VALIDACIÓN DE LA AUTORIDAD

Los procedimientos de autenticación de validación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de TOC PERÚ– RPS.

17.7. CRITERIOS PARA LA INTEROPERABILIDAD

TOC SA, como prestador de servicios de TOC PERU, únicamente emitirá certificados

a EC Subordinadas, que estén directamente vinculadas y operadas por TOC SA.

17.8. IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

TOC SA, como prestador de servicios de TOC PERÚ, no admite la renovación de clave de los certificados después de una revocación. El suscriptor debe solicitar un nuevo certificado digital mediante el uso de los procedimientos para su emisión.

18. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La política de identificación para las solicitudes de revocación es la misma que se estipula para el registro inicial. Las solicitudes telemáticas solo serán TOC PERU das si estas incluyen una firma digital utilizando el certificado del suscriptor que solicitó la revocación, o el certificado de un tercero que está autorizado a solicitar la revocación en nombre del suscriptor.

Una Entidad de Certificación puede definir, que durante el proceso de inscripción, un suscriptor puede crear una contraseña que se puede utilizar en las solicitudes de revocación remotas, utilizando un procedimiento online comunicado al usuario cuando se expide el certificado.

TOC SA, como prestador de servicios de TOC PERÚ, puede solicitar la revocación de un certificado si hay conocimiento o sospecha fundada de que la clave privada asociada ha sido comprometida, o razones para creer cualquier otro dato que recomienda esta acción.

19. REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

19.1. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de TOC PERÚ enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de máximo cinco (05) días hábiles, luego de haber sido aprobada la validación de identidad y del pago respectivo.

19.2. SOLICITUD DEL CERTIFICADO

Las Entidades de registro que operan bajo TOC PERÚ son las competentes y responsables de determinar si el tipo de certificado solicitado es adecuado para el solicitante y futuro suscriptor, de conformidad con la Política de Certificación en relación con dicho certificado, y por lo tanto proceder o no con la solicitud del certificado.

19.3. QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Una solicitud de certificado puede ser presentada por el titular del certificado o por un representante autorizado por él.

19.4. SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera. Esto se realiza a través de medios no repudiables, tales como la comparecencia firmada legalmente por el representante legal de la persona que solicita el certificado.

19.5. SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

19.6. SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

SERVICIOS BRINDADOS

La ER de TOC PERÚ brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de emisión, revocación, suspensión, y re-emisión[1] de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de emisión, revocación, suspensión y re-emisión [2] de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a la Entidad de Certificación de TOC PERÚ, que se encuentran publicados en la siguiente dirección: https://www.toc.pe/politicas

19.7. PROCESO DE REGISTRO Y RESPONSABILIDADES

El proceso de registro, incluyendo la información verificada y las atribuciones para ejecutar el proceso se detalla en la Declaración de Prácticas de Registro de TOC PERÚ (RPS).

---

[1] La suspensión y re-emisión dependerá de lo establecido en la Política de Certificación de la EC de TOC PERÚ.

[2] La suspensión y re-emisión dependerá de lo establecido en la Política de Certificación de la EC de TOC PERÚ.

20. TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

20.1. REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Este proceso se detalla en la Declaración de Prácticas de Registro de TOC PERÚ (RPS).

20.2. APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro de TOC PERÚ (RPS).

20.3. PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro de TOC PERÚ(RPS).

21. EMISIÓN DE CERTIFICADOS

21.1. ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

Una Entidad de certificación adherida a TOC SA procede a emitir un certificado sólo después de la ejecución de las medidas necesarias para verificar que la petición recibida por una Entidad de Registro es genuina. Los controles específicos están estipulados en la Política de Certificación correspondiente.

21.2. NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

Después de ser emitido un certificado, la EC notifica a la ER de la emisión y la disponibilidad del certificado, y el nuevo certificado se publica en el repositorio de certificados.

El mecanismo de notificación puede ser acordado específicamente con el suscriptor. En general, para los certificados personales, la ER es responsable de notificar al suscriptor de la disponibilidad de su certificado, enviándole una copia o mediante la especificación de cómo se puede obtener el certificado.

Las notificaciones electrónicas pueden ser firmadas digitalmente por la ER o representante habilitado.

22. ACEPTACIÓN DEL CERTIFICADO

22.1. FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

La aceptación del certificado queda entendida después de que el suscriptor o su

representante lleva a cabo uno o más de los siguientes puntos:

- Se firma el "Acuerdo del suscriptor o titular", que incluye los términos y condiciones asociadas con la política de certificado, y que constituye la aceptación formal de los términos;
- Se descarga y/o instala el certificado, por lo que es técnicamente disponible para el uso;
- No se rechaza explícitamente el certificado una vez que la disponibilidad de la notificación ha sido enviada.

22.2. PUBLICACIÓN DEL CERTIFICADO POR LA EC

Las entidades emisoras que operan bajo TOC SA publican todos los certificados emitidos.

22.3. Servicios de estado del certificado

TOC PERÚ tiene a disposición los servicios de comprobación de estado de certificado directamente a través del sitio web https://www.toc.pe, por una parte, se encuentra la lista de certificados revocados (CRL). Además, se puede verificar el estado actual de un certificado mediante el servicio de OCSP.

22.4. NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

No aplica.

23. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

23.1. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

Los usos específicos permitidos para una clave privada asociada a un tipo de certificado expedido en TOC SA son tal y como se detalla en la sección Uso permitido del certificado del presente documento. En donde no serán utilizadas para ningún otro propósito

En caso de que las claves se vean vulneradas, o bien, expuestas a algún peligro, estas no serán manipuladas. Además, las claves privadas no podrán ser utilizadas al momento de término de su ciclo de vida sin excepciones.

23.2. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

El tercero que confía debe acceder y utilizar la clave pública y certificado conforme a lo estipulado en la presente CPS y tal como se indica en el documento "Acuerdo del tercero que confía", hecho público en la página web https://firma.toc.cl/indexpki.php .

24. MODIFICACIÓN DE CERTIFICADOS

TOC SA, como prestador de servicios de TOC PERÚ, no permite la modificación de los certificados durante su periodo de validez. Si la información contenida en un

certificado deja de ser válido, o las circunstancias del suscriptor cambian de manera tal que las condiciones expresadas en la CPS o CP no se cumplen, entonces el único procedimiento TOC PERÚ do es la revocación de certificados.

25. RE-EMISIÓN DE CERTIFICADOS

25.1. SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES

La ER de TOC PERÚ recibe solicitudes de re-emisión rutinaria. La re-emisión rutinaria es un proceso programado, que puede ejecutarse cada vez que un nuevo par de claves debe ser emitido debido a que la fecha de expiración de un certificado digital es cercana y menor de un plazo máximo de un (01) año. Solamente los titulares de certificados digitales pueden solicitar la re-emisión por certificado digital.

La ER de TOC PERÚ, ante una solicitud de re-emisión, validará para todo tipo de certificado que el certificado previamente emitido se encuentra dentro de su periodo de vigencia y ha sido debidamente revocado. De lo contrario, no se procederá a aprobar la solicitud de re-emisión.

Luego de la expiración de un certificado digital re-emitido, deberá seguirse el proceso de solicitud de emisión de un nuevo certificado digital.

25.2. SOLICITUD DE RE-EMISIÓN CERTIFICADOS DE PERSONA JURÍDICA

25.2.1. SERVICIOS BRINDADOS

La ER de TOC PERÚ brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de re-emisión[3] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
b) Atención de solicitudes de re-emisión de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
c) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
d) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: https://www.toc.pe/politicas

[3] La suspensión y re-emisión dependerá de lo establecido en la Política de Certificación de la EC de TOC PERÚ.

25.2.2. Autorizados para realizar la solicitud

Solo los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de TOC PERÚ, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

25.2.3. Modalidades de atención

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de TOC PERÚ
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, deberá enviar el contrato de suscriptor firmado digitalmente
- por el representante asignado por la persona jurídica, con un certificado válido y vigente.

25.2.4. Solicitud de re-emisión de certificados de atributos

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

25.2.5. Solicitud de re-emisión de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

25.2.6. Identificación y autenticación de solicitantes de re-emisión de certificados de persona jurídica

La ER de TOC PERÚ comprobará que la información del titular y del suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y de los suscriptores en la base de datos del RENIEC.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad, pasaporte o carnet de extranjería.

25.3. Solicitud de re-emisión de certificados de persona natural

25.3.1. Servicios brindados

La ER de TOC PERÚ brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de re-emisión[4] de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de re-emisión[5] de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección:https://www.toc.pe/politicas

25.3.2. Autorizados para realizar la solicitud

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado.

25.3.3. Modalidades de atención

La solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de TOC PERÚ
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, deberá enviar el contrato de suscriptor firmado digitalmente por el representante asignado por la persona jurídica, con un certificado válido y vigente.

25.3.4. Solicitud de re-emisión de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

25.3.5. Identificación y autenticación de solicitantes de re-emisión de certificados de persona natural

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de TOC PERÚ a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de TOC PERÚ no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

---

[4] La suspensión y re-emisión dependerá de lo establecido en la Política de Certificación de la EC de TOC PERÚ.

[5] La suspensión y re-emisión dependerá de lo establecido en la Política de Certificación de la EC de TOC PERÚ.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

26. Procesamiento de la solicitud de re-emisión

26.1. Rechazo de la solicitud de re-emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de TOC PERÚ puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

26.2. Aprobación de la solicitud de re-emisión de un certificado

En caso que una solicitud sea aprobada por la ER de TOC PERÚ realizará lo siguiente:

a) Comunicar a la EC su aprobación para la re-emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.

b) Se requerirá la firma del contrato del suscriptor.

26.3. Registro de documentos

La ER de TOC PERÚ registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

26.4. Método para probar la posesión de la clave privada

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor, en un módulo criptográfico con la certificación FIPS 140-2. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la EC de TOC PERÚ en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

26.5. Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la identidad del solicitante, si el resultado de la validación es positivo, la ER de TOC PERÚ enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de tres (03) días hábiles, luego de haber sido aprobada la validación de identidad y del pago respectivo.

26.6. RE-EMISIÓN DEL CERTIFICADO

La re-emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

TOC SA, como prestador de servicios de TOC PERÚ, no admite la re-emisión de los certificados durante su periodo de validez. En caso de requerirse este procedimiento lo que se deberá hacer es solicitarse un nuevo certificado, siguiente el procedimiento descrito para este caso

27. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

27.1. REQUISITOS DE REVOCACIÓN

La revocación es el mecanismo a través del cual TOC PERÚ deja sin efecto de manera permanente un certificado de firma electrónica y de firma digital emitido por él, cesando permanentemente los efectos jurídicos del certificado conforme a los usos que le son propios impidiendo el uso legítimo del mismo.

Tendrá lugar cuando TOC PERÚ constate alguna de las siguientes circunstancias:

a) Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso el certificado esté emitido para un cargo de dicha empresa).
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.
e) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por TOC PERÚ.
f) Si el titular no actualiza los datos proporcionados a TOC PERÚ al momento de solicitar el certificado.

27.2. CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Una vez TOC PERÚ constate alguna de las siguientes circunstancias:

a) Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso que el certificado esté emitido para un cargo de dicha empresa).
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular haya proporcionado al momento de solicitar el certificado

información inexacta o incompleta.

e) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por TOC PERU SAC.
f) Si el titular no actualiza los datos proporcionados a TOC PERU SAC al momento de solicitar el certificado.

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

Asimismo, la EC que opere bajo TOC SA debe revocar un certificado que ha emitido, sobre la ocurrencia de cualquiera de los siguientes eventos:

- El suscriptor solicita la revocación de su certificado.
- El suscriptor indica que el certificado original no estaba autorizado y no le concede retroactivamente la autorización.
- La EC obtiene evidencia razonable de que la clave privada del suscriptor (correspondiente a la clave pública en el certificado) ha sido comprometida o se sospecha de compromiso, o de lo contrario el certificado ha sido mal utilizado.
- La EC recibe aviso o caso contrario se da cuenta de que un suscriptor ha violado una o más de sus obligaciones fundamentales bajo el contrato de suscriptor o condiciones de uso.
- La EC recibe aviso o caso contrario se da cuenta de que un tribunal o árbitro ha revocado el derecho de un suscriptor para utilizar un nombre (por ejemplo, un nombre de dominio) que aparece en el certificado, o que el suscriptor no ha logrado renovar su derecho a utilizar ese nombre.
- La EC recibe aviso o de lo contrario se da cuenta de un cambio sustancial en la información contenida en el certificado.
- Una determinación, a la sola discreción de la autoridad competente, de que el certificado no ha sido emitido de conformidad con los términos y condiciones derivadas de la política de certificación apropiada
- La EC determina que alguna de la información que aparece en el certificado no es exacta.
- La EC cesa su actividad por cualquier razón y no ha dispuesto otra EC bajo TOC SA para proporcionar soporte de revocación del certificado.

- El derecho de la EC de emitir certificados para una política de certificado expira o es revocado o terminado, a menos que la EC haga los arreglos para seguir manteniendo el repositorio CRL/OCSP.
- La clave privada de cualquier EC en el curso de certificación se sospecha que ha sido comprometida.
- El suscriptor es un participante en el PKI (por ejemplo, Registro Oficial) y pierde su derecho de acceso para seguir actuando como tal.
- La EC recibe aviso o de lo contrario se da cuenta de que un suscriptor se ha añadido como una parte denegada o persona prohibida de una lista negra, o está operando desde un lugar o de una manera que está prohibida en virtud de las leyes y la jurisdicción del país de operación de la EC.

27.3. QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

El suscriptor o representante legal pueden solicitar la revocación de un certificado individual u organizacional.

La ER autorizada o representante titulado pueden solicitar la revocación de un certificado si se presenta alguna de las circunstancias expresadas en el apartado anterior.

27.4. PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

El procedimiento que se utiliza para las solicitudes de revocación de certificados se detalla en el "Contrato de titular/suscriptor", realizándose a través del sitio web https://firma.toc.cl/pki_revocar.php

Una vez TOC PERÚ constate alguna de las siguientes circunstancias:

a) Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso que el certificado esté emitido para un cargo de dicha empresa).

b) Fallecimiento del titular.

c) Resolución judicial ejecutoriada.

d) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.

e) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por TOC PERU SAC.

f) Si el titular no actualiza los datos proporcionados a TOC PERU SAC al momento de solicitar el certificado.

La práctica común para todos los certificados emitidos bajo TOC SA es para las solicitudes de revocación sean aceptadas de forma automática y produzcan una revocación inmediata en el caso de:

- Solicitudes remotas enviadas por correo electrónico o a través de una página web o servicio, debidamente autenticados por el suscriptor o su representante.

- Las solicitudes presenciales dirigidas a un representante de la ER oficial y la identidad del solicitante se demuestran por el mismo medio que el utilizado para el registro de certificados.

- Las solicitudes de revocación enviados por un representante oficial de registro o certificación que opere bajo TOC SA.

Las solicitudes de revocación comunicadas por otros medios (es decir, por no firmar mensajes electrónicos o por teléfono), que no se autentican de manera inequívoca al solicitante va a producir una suspensión temporal del certificado, tal como se define en las secciones relativas a la Suspensión del certificado.

27.5. PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

No se estipula un periodo de gracia para las solicitudes de revocación. El proceso de revocación se iniciará inmediatamente después de la recepción de dicha solicitud por la ER o EC.

27.6. PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Las solicitudes de revocación son procesadas por la EC en el plazo más breve posible, El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 6 horas, considerando lunes a viernes de 9:00 a 18:00 horas

27.7. RECHAZO DE LA SOLICITUD DE REVOCACIÓN EMISIÓN DE UN CERTIFICADO

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de TOC PERÚ puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

27.8. APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

En caso que una solicitud sea aprobada por la ER de TOC PERÚ realizará lo siguiente:

a) Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.

b) Una copia de dicha solicitud firmada será enviada a la EC o almacenada en la ER de TOC PERÚ.

27.9. COMUNICACIÓN DE REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

27.10. REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

TOC SA, como prestador de servicios de TOC PERÚ, requiere que todos los terceros que confían en los certificados expedidos de conformidad con el Modelo de confianza, comprueben el estado de estos certificados en cada solicitud de verificación de firma y autenticación digital utilizando el certificado. Este requisito puede cumplirse mediante la consulta de la CRL más reciente de la EC que emitió el certificado.

La información necesaria para localizar estos servicios de revocación, se incluye en todos los certificados TOC SA, utilizando el estándar CDP y/o extensiones AFP.

27.11. FRECUENCIA DE EMISIÓN DE LAS CRLS

Las frecuencias estipuladas son:

- La EC Raíz de TOC SA emite una CRL completa todos los años, con un periodo de latencia de una semana. Esta CRL contendrá los certificados revocados por la Política de EC de TOC SA o ECs emisoras, según corresponda a la jerarquía. Las nuevas CRLs se publican inmediatamente si una nueva EC subordinada se revoca.

- La Política de EC de TOC SA emite una CRL completa todos los meses, con un periodo de latencia de 3 días. Esta CRL contendrá los certificados, en su caso, revocados para las ECs emisoras de TOC SA. La nueva CRL se publica inmediatamente si una nueva EC subordinada se revoca.

- La Política de ECs emisoras de TOC SA emite una CRL completa cada dos días, con una latencia máxima de dos días adicionales en caso de interrupción del servicio. Esta CRL contendrá los certificados, en su caso, revocados para los usuarios finales/suscriptores de TOC SA.

27.12. TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática, menor a una hora como lo establece el INDECOPI.

27.13. REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

TOC SA, como prestador de servicios de TOC PERÚ, publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año. La disponibilidad del servicio OCSP no es obligatorio para los certificados de garantía bajos, como el Certificado “FEA”.

La URL utilizada para acceder a este servicio está incluido en la "extensión AIA" en todos los certificados emitidos.

Para ciertos Certificados de la EC emisora se podría publicar en servicios online,

web- based u otros.

Estos servicios adicionales están estipulados en el “Contrato de suscriptor/titular”.

27.14. REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON- LINE

La comprobación de la revocación online se ofrece abiertamente sin restricción a todos los participantes en la PKI, para los tipos de certificados que incluyan la extensión AIA apropiado.

Se solicita a los terceros que confían verificar siempre la validez del certificado en la que se basan, según lo estipulado en el apartado *Requisitos de verificación de las revocaciones por los terceros que confían.*

27.15. OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No se estipula.

27.16. REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

Cualquier tercero que detecte un compromiso de la clave en cualquier nivel de la jerarquía TOC SA es requerido para comunicar inmediatamente esto a la Entidad de Registro o a la Entidad de Certificación.

27.17. CIRCUNSTANCIAS PARA LA SUSPENSIÓN

La suspensión sólo se admite para certificados personales.

Las personas autorizadas de acuerdo con la sección *Quién puede solicitar la suspensión*, pueden explícitamente solicitar la suspensión de sus certificados.

27.18. QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Ver el apartado *Quién puede solicitar una revocación.*

27.19. PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

Ver el apartado *Procedimiento de solicitud de revocación.*

27.20. LÍMITES DEL PERIODO DE SUSPENSIÓN

No se estipula.

28. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

28.1. CARACTERÍSTICAS OPERACIONALES

Los servicios de estado de certificados son accesibles a través de servidores HTTP pertenecientes a las EC de TOC SA. Se puede acceder a los servicios mediante la descarga de listas de revocación (CRL).

Las direcciones URL de servicios de información de revocación de certificados apropiados se incluyen en las extensiones estándar dentro de los certificados emitidos.

Otros servicios podrían estar disponibles, según lo estipulado en el "Contrato de suscriptor/titular" correspondiente.

28.2. DISPONIBILIDAD DEL SERVICIO

El servicio de consulta del estado de certificados digitales tiene una disponibilidad 7X24 durante todos los días del año.

28.3. CARACTERÍSTICAS OPCIONALES

No se estipula.

28.4. Finalización de la suscripción

Cada suscripción se verá finalizada inmediatamente luego de que el certificado haya cumplido con su vigencia.

28.5. FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO

La finalización de la vigencia de un certificado se produce después de la expiración o revocación de un certificado, y es solo en ese caso, que no afecta a las suscripciones adicionales (si las hay) que la entidad final puede llevar a cabo dentro de TOC SA.

29. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

TOC PERÚ establece en esta CP, la forma de cómo se realizan las notificaciones.

De forma general las notificaciones se realizarán a través de la pagina web https://www.toc.pe/

En los casos con problemas relacionados a seguridad de la información, que puedan afectar a una persona natural o física y/o jurídica, TOC PERÚ notificará a los participantes afectados.

En términos generales, los participantes se podrán comunicar con TOC PERÚ, según los datos mencionados en el punto 10 de esta CP.

30. CUSTODIA Y RECUPERACIÓN DE CLAVES

30.1. ALMACENAMIENTO DE LA CLAVE PRIVADA DEL TITULAR

Solo se permite el depósito de garantía de los certificados de suscriptor/titular. Para los certificados de infraestructura, como EC, ER o de otros, las políticas de copia de seguridad apropiadas deben ser implementadas, según la sección *Backup de la clave privada*.

30.2. PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

TOC SA, como prestador de servicios de TOC PERU, no estipula cómo las claves privadas de los usuarios finales pueden ser custodiados o recuperadas, ni ofrece este tipo de instalaciones en los servicios comerciales directas a los usuarios finales. Las ECs o ERs emisoras con el acceso a través de una interfaz de "Managed PKI", pueden aplicar diferentes procedimientos para el depósito de claves, siendo obligatoria en tal caso una comunicación explícita de tales características al suscriptor del certificado.

En particular, TOC SA no recomienda ningún tipo de depósito en garantía o respaldo de las claves privadas habilitadas para las firmas digitales, siempre y cuando el usuario final sea la única entidad que tiene acceso efectivo a esta información.

La recuperación de claves no se admite bajo ningún supuesto, por tanto no hay un procedimiento.

30.3. PRÁCTICAS Y POLÍTICAS

De acuerdo con las consideraciones anteriores, cualquier clave de sesión que permite el descifrado de una clave privada debe mantenerse bajo el control exclusivo del suscriptor del certificado o representante autorizado.

31. CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES.

31.1. CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE TOC SA COMO PRESTADOR DE SERVICIOS DE TOC PERÚ

31.1.1. UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Los sistemas de información TOC SA, como prestador de servicios de TOC PERÚ, se encuentran en el Centro de Datos Seguros que proporcionan niveles de seguridad adecuados y bajo vigilancia las 24 horas del día, los 7 días a la semana. Este Centro de Datos está construido de tal manera que los riesgos físicos críticos correspondientes estén controlados.

31.1.2. ACCESO FÍSICO

El Centro de Datos Seguros de TOC SA, como prestador de servicios de TOC PERÚ, implementa diversos perímetros de seguridad. El acceso desde un externo hacia un perímetro interno requiere diferentes controles de seguridad y autorización. Entre estos controles se implementan la puerta de acceso biométrico, sistemas de video vigilancia y detección de intrusos.

31.1.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones de TOC SA, como prestador de servicios de TOC PERÚ, están equipadas con sistemas de alimentación ininterrumpida (SAI) con capacidad suficiente para mantener de forma autónoma los sistemas TOC SA durante los cortes de energía eléctrica y proteger estos sistemas de los daños que puedan deberse a fluctuaciones de energía.

Los sistemas de aire acondicionado utilizados en TOC SA se componen de un equipo independiente que asegura los márgenes operativos de temperatura y humedad en el interior del Centro de Datos Seguros.

31.1.4. EXPOSICIÓN AL AGUA

Las instalaciones de TOC SA, como prestador de servicios de TOC PERÚ, están ubicadas en un lugar donde se controlan los riesgos de inundación naturales, además de encontrarse equipadas con sensores de inundación y alarmas.

31.1.5. PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las instalaciones de TOC SA, como prestador de servicios de TOC PERÚ, implementan controles de detección de incendios, prevención y protección

31.1.6. SISTEMA DE ALMACENAMIENTO

Los medios de información confidencial se almacenan de forma segura en contenedores a prueba de fuego y cajas fuertes de alta seguridad, en función del tipo de soporte y la clasificación de la información que contienen.

Estos contenedores y cajas fuertes se encuentran en ubicaciones redundantes, con el fin de eliminar los riesgos del uso en una sola ubicación (es decir, en caso de eliminación incendio o daño por agua).

El acceso a estos lugares de almacenamiento y los artículos está restringido a personas autorizadas y regulada por procedimientos de seguridad.

31.1.7. ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

La eliminación de desechos de papel y medios de comunicación ópticos o magnéticos que contienen cualquier información generada durante las operaciones TOC SA, se ejecuta siguiendo los procedimientos establecidos para tales fines, incluyendo los procesos de destrucción y/o de desmagnetización, dependiendo del tipo de medio a ser eliminado.

31.1.8. BACKUP FUERA DE LA INSTALACIÓN

Diariamente TOC SA, en calidad de prestador de servicios de TOC PERÚ, realiza una copia de seguridad de toda la información necesaria para promover un centro de datos secundario al estado operativo en el caso de un desastre.

De forma periódica, se hace una copia de seguridad remota y se almacena de manera tal que se requiere un control de acceso doble para restaurar las copias de seguridad.

31.2. CONTROLES DE PROCEDIMIENTO

31.2.1. ROLES DE CONFIANZA

TOC SA establece y hace cumplir una política de seguridad estricta para controlar todas las operaciones realizadas en cualquier nivel dentro de TOC SA. Esto incluye la identificación y el control de las personas que realicen estas operaciones. Estas personas se consideran "Roles de confianza" e incluyen, pero no se limitan a:

- Director de la Entidad de Certificación
- Administrador de la Entidad de Certificación
- Operador de la Entidad de Certificación
- Director de la Entidad de Registro
- Administrador de la Entidad de Registro
- Operador de la Entidad de Registro
- Oficial del Punto de Registro
- Director de Soporte, Capacitación y Comunicación
- Consejero legal
- Director de la documentación
- Administrador de sistemas
- Gerente de seguridad
- Administrador de Seguridad y del operador
- Autoridad de Aprobación de Políticas

Las personas que quieran obtener dichos Roles de confianza deben completar con éxito los requisitos de selección establecidos en la presente CPS, sección *Controles de personal.*

31.2.2. CUALIFICACIÓN DEL AUDITOR

El auditor debe estar autorizado por el INDECOPI para realizar sus funciones

El auditor debe ser independiente de la Entidad Certificadora, y, al mismo tiempo, no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.

El auditor debe contar con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas

31.2.3. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

TOC SA, como prestador de servicios de TOC PERÚ, establece la necesidad de segregar funciones en base a la responsabilidad del trabajo con el fin de garantizar el número adecuado de Roles de confianza para realizar tareas confidenciales.

Las funciones que requieren la separación de funciones se estipula en la sección *Roles que requieren segregación de funciones.*

31.2.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todas las personas que asuman un rol en los sistemas de TOC SA siguen un proceso de autorización que les da derecho a acceder a la información y los sistemas apropiados para su función.

El control de acceso físico para todas las personas autorizadas que acceden a los sistemas y servicios de sistemas de TOC SA típicamente se ve impuesto mediante la autenticación de dos factores que por lo general incluye la biometría.

31.2.5. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Los roles que requieren separación de funciones incluyen al menos los siguientes:

- La habilitación de una EC en un estado de producción (Ceremonia de procedimientos EC)
- La emisión o revocación de certificados de la EC
- Validación de la información y la emisión de certificados de alta seguridad del suscriptor

31.3. CONTROLES DE PERSONAL

31.3.1. REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Se requiere que el personal que actúa directa o indirectamente para la TOC SA posea la titulación requerida y/o experiencia demostrada en relación a la prestación de servicios de certificación. Además, se requiere que todo el personal involucrado actúe de acuerdo con la Política de Seguridad de TOC SA y poseer lo siguiente:

- El conocimiento y la formación (de acuerdo con el papel asignado a la persona) en Infraestructuras de Clave Pública.
- El conocimiento y la formación (de acuerdo con el papel) en Sistemas de Información de Seguridad.
- El conocimiento y la formación específica de las responsabilidades asignadas.

31.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

El Departamento de Recursos Humanos realiza las comprobaciones de verificación en el personal permanente en el momento de las solicitudes de empleo, y

se asegura de que todo el personal con acceso a información confidencial es digno de confianza y comprende sus responsabilidades; esto incluye, como mínimo, lo siguiente:

- Disponibilidad y verificación de referencias satisfactorias;
- La confirmación de las calificaciones académicas y profesionales reivindicadas;
- Los controles de identidad de pasaporte o documento similar.

31.3.3. REQUISITOS DE FORMACIÓN

El personal implicado en TOC SA, incluyendo las ECs emisoras operadas por terceros y las ER, seguirán un plan de formación interna adaptada a sus atribuciones asignadas. Esta formación será compatible con las normas de la industria, como el EC/Línea Base del Foro Internacional y/o requisitos de Validación extendida, según sea el caso.

31.3.4. REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se considera formación a través de cursos de certificación y capacitación en el SGSI y SGCN (ISO 27001 y 22301). Además, cursos específicos para el personal asociado a la EC, cuyo contenido, duración y fechas de realización se describen en el plan de capacitación anual de TOC. El mencionado plan, aplica a todo el personal del área Seguridad de la Información y Calidad y, personal asociado a la EC.

31.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No se estipula.

31.3.6. SANCIONES POR ACTUACIONES NO AUTORIZADAS

En caso TOC SA, como proveedor de servicios de TOC PERÚ, detecte una acción no autorizada, emprenderá las acciones disciplinarias necesarias. Cualquier acción que (intencionalmente o no) contraviene la Declaración de Prácticas de Certificación.

Tras la detección de una acción no autorizada, TOC SA iniciará un proceso de investigación. Durante este proceso se evitará que las personas involucradas obtengan acceso a los sistemas e información de TOC SA.

Las medidas disciplinarias serán tomadas después de la investigación determine la gravedad y la intención de la acción.

31.3.7. REQUISITOS DE CONTRATACIÓN DE TERCEROS

Se requiere que los contratistas externos estén de acuerdo con las Políticas de seguridad de la información de TOC SA, y el personal temporal no amparado por un acuerdo de confidencialidad existente también estará obligado a firmar el acuerdo de confidencialidad antes de concederse el acceso a los recursos de información.

El acuerdo se examina cuando existen cambios en las condiciones de empleo o contratos.

31.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

A todo el personal incorporado dentro de TOC SA se le proporciona el acceso a por lo menos la siguiente información:

- Declaración de Prácticas de Certificación
- Políticas de Certificación
- Política de Privacidad
- Política de Seguridad
- Organigrama y funciones y responsabilidades asignadas
- Procedimientos operacionales
- Procedimientos de respuesta a incidentes

31.3.9. FIN DEL CONTRATO Y PROCEDIMIENTO DE CAMBIO DE ROLES ASIGNADOS

En el caso de que un contrato finalice o se cambie el papel asignado a una persona, TOC SA se asegura de que se ejecute el procedimiento correspondiente. Este procedimiento incluye al menos los cambios necesarios en los privilegios concedidos a las instalaciones de acceso, sistemas de información y documentación.

El material asignado (tarjetas inteligentes, ordenadores, etc.) será devuelto o reasignado como sea necesario.

El cambio o terminación será notificado a todas las partes involucradas.

31.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

31.4.1. TIPOS DE EVENTOS REGISTRADOS

TOC SA, en calidad de prestador de servicios de TOC PERÚ, registra en sus servidores todos los eventos relacionados a:

- Eventos de administración en relación al ciclo de vida del par de claves de la EC, que incluyen:

a. La generación de claves, copia de seguridad, almacenamiento, recuperación, archivo y destrucción tal como se expone en la documentación de procedimiento

b. Eventos de administración de ciclo de vida del dispositivo criptográfico tal como se expone en la documentación de procedimiento

- Eventos de administración en relación al ciclo de vida del Certificado del Suscriptor, entre otros:

a. Las solicitudes de revocación de certificados tal como se expone en los registros de la EC

b. Las actividades de verificación

c. Fecha, hora, número de teléfono utilizado, personas con las que se habló, y los resultados finales de las llamadas telefónicas de verificación tal como lo exponen los oficiales de registro

d. La aceptación y el rechazo de las solicitudes de certificados tal como se expone en los registros de la EC

e. La emisión de certificados tal como se expone en los registros de la EC

f. Generación de listas de certificados revocados tal como se expone en los registros de la EC (NB CRL no se conservan, sólo el registro de su generación)

- Los eventos de seguridad, incluyendo:

a. Los intentos de acceso al sistema PKI exitosos y no exitosos, tal como se expone en los registros del sistema operativo

b. Las principales acciones de PKI y del sistema de seguridad llevadas a cabo, tal como se expone en los registros del sistema operativo

c. Cambios en el perfil de seguridad, tal como se expone en los registros del sistema operativo

d. Los fallos del sistema, fallos de hardware y otras anomalías en los registros del servidor

e. Actividades de firewalls y routers, tal como se expone en los registros del dispositivo

f. Las entradas y salidas de la instalación de la EC, tal como se expone en los registros de control de acceso.

g. Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo en los servidores.

h. Inicio y detención de la EC.

i. Intentos exitosos o fracasados de inicio y fin de sesión de administradores.

j. Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.

k. Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.

l. Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar

claves y certificados.

m. Intentos exitosos o fracasados de generar, firmar o emitir una CRL.

n. Intentos exitosos o fracasados de crear, modificar o borrar información de los suscriptores de certificados.

o. Intentos exitosos o fracasados de acceso a los sitios principal y secundario por parte de personal autorizado o no.

p. Backup, archivo y restauración.

q. Cambios en la configuración del sistema.

r. Actualizaciones de software y hardware.

s. Mantenimiento del sistema.

31.4.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

La revisión de los logs se realiza cuando se detecte una alerta de seguridad o existan indicios de un funcionamiento no usual de los sistemas.

Los registros son procesados y auditados de forma regular.

Para los sistemas que se mantienen fuera de línea, como la EC Raíz, los registros de auditoría se recogen solamente cuando se ejecuta una operación.

31.4.3. PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

TOC SA y las partes implicadas conservan todos los registros de auditoría como se especifica en la sección *Periodo de conservación*.

31.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Todos los registros de auditoría y los archivos se guardan en armarios a prueba de fuego, y sólo es accesible para personas autorizadas.

La destrucción de un registro de auditoría sólo puede ejecutarse después de constatarse:

c. La autorización firmada por el auditor de TOC SA y el Administrador de seguridad de la información de TOC SA.
d. la autorización de INDECOPI

Un rastro de los materiales destruidos se mantiene para pcs futuras referencias.

31.4.5. ARCHIVO DE REGISTROS Y EVENTOS

Los registros archivados y los registros de auditoría se mantienen durante el tiempo de validez de los certificados involucrados y se retienen por un

período no inferior a 10 años.
En el caso del Ciclo de vida de los Certificados y sus claves privadas, su registro será desde el momento en que éstos expiren.

TOC Perú SAC registra y guarda todos los logs de los eventos, correspondientes al sistema de seguridad de la CA y de la RA, de acuerdo a las siguientes especificaciones:

Registro de eventos del sistema de seguridad CA y RA:

Encendido del sistema.
Apagado del sistema.
Registro de inicio y fin de sesión.
Registro de Intentos de accesos no autorizados al sistema de la CA o las RA a través de la red.
Registro de Intentos de accesos no autorizados a la red interna de la CA.
Registro de Intentos de accesos no autorizados al sistema de archivos.
Registro de intentos de creación, modificación, borrado, establecimiento de contraseñas o cambio de privilegios.
Registro de generación de claves propias.
Registro de eventos relacionados al ciclo de vida de la clave privada de la CA
Acceso físico a los logs.
Registros de las aplicaciones de las CA y las RA.
Encendido y apagado de las aplicaciones de las CA y las RA.
Cambios en los detalles de las CA y/o sus claves.
Cambios en la creación de perfiles de certificados.
Cambios en la configuración y mantenimiento del sistema.
Eventos del ciclo de vida de los certificados.
Eventos asociados al uso del módulo criptográfico de la CA.
Registros de la destrucción de los medios que contienen las claves, datos de activación.

Registro de eventos tecnológicos:

Modificación y actualización en la política de seguridad de la información.
Fallas e intermitencias del sistema.
Fallas del funcionamiento del hardware.
Registro de actividades en firewall, enrutadores y otros equipos de comunicaciones..
Registro de la documentación presentada por el solicitante.
Registro de toda la información relacionada con el proceso de registro.

TOC SAC conserva toda la información de los sucesos relacionados con la preparación de los dispositivos DCCF.

TOC SAC, mantienen en formato físico o digital, la siguiente información:

Documentación de las ceremonias de creación de claves de las CA.
Registros de acceso físico a HSM.
BBDD de gestión de claves.
Mantenimiento, actualización y modificaciones en la configuración del sistema.
Actualización de información del personal técnico especializado que lleva a cabo labores de confianza en las CA y las RA.
Informes de compromisos y discrepancias.
Registros de la destrucción de información de claves, datos de activación.
Registro de información personal del Solicitante, y del Firmante o del Custodio de Claves,
Registro de posesión de datos de activación, para operaciones con la clave privada de las CA.

31.4.6. PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría están respaldados mediante procedimientos graduales y remotos.

Los respaldos de la información de auditoría se realizan acorde a un detallado programa de respaldos aplicable por igual al resto de los datos generados en las operaciones del PSC. Dicho programa contempla respaldos incrementales y respaldos completos.

En los respaldos completos se almacenan los datos en soporte físico en armarios a prueba de fuego, y sólo es accesible para personas autorizadas.

31.4.7. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de recogida de registros de auditoría en TOC SA es una combinación de procesos automáticos y manuales, y es ejecutado por los sistemas operativos adecuados, aplicaciones de software, y el personal de operación de estos sistemas.

31.4.8. NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

No se estipula.

31.4.9. AUDITORÍA DE LOS PROCEDIMIENTOS Y CONTROLES

Los procedimientos y controles implementados que forman parte del SGSI y declarados en el SoA deben ser auditados de forma anual. Además, de acuerdo a lo señalado en norma ISO 27001.

31.4.10. AUDITORÍA DEL ARCHIVO

El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.

31.4.11. AUDITORÍA DE REGISTRO

Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.

31.4.12. ANÁLISIS DE VULNERABILIDADES

TOC SA, como prestador de servicios de TOC PERÚ, realiza una evaluación periódica de la vulnerabilidad mediante el control de los registros de actividad. Las evaluaciones a profundidad y los controles se realizan sobre una base anual, incluyendo la conformidad con los planes de recuperación de desastres. En el caso de que una evaluación no logre realizarse o se retrase, TOC SA informará a las partes involucradas los registros de tal evento y su causa se mantendrá para futuras consultas.

Este análisis de la seguridad implica la identificación de las tareas necesarias para corregir las vulnerabilidades detectadas.

31.5. ARCHIVO DE REGISTROS

31.5.1. TIPOS DE EVENTOS ARCHIVADOS

La información y los eventos archivados son:

32. La información generada (en la EC y ER) durante el ciclo de vida de todos los certificados TOC SA,
33. Los contratos y acuerdos,
34. Los registros de auditoría estipulados en la sección Procedimientos de auditoría de seguridad de la presente CPS.

34.1.1. EVENTOS SIGNIFICATIVOS.

Todos los registros de auditoría contienen la fecha y hora del servidor de la PSC, sincronizado con la TSA de TOC SAC, quedando registrada la ocurrencia del evento pertinente.

Se deben registrar eventos relacionados al ciclo de vida de la clave privada de la EC

34.1.2. PERIODO DE CONSERVACIÓN

Los registros archivados y los registros de auditoría se mantienen registros y se conservarán durante el tiempo de validez de los certificados involucrados y se retienen por un período no inferior a 10 años.

34.1.3. PROTECCIÓN DE ARCHIVOS

El acceso a los materiales de archivo está restringido a personas autorizadas para garantizar la integridad del archivo.

34.1.4. PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Las copias de seguridad se ejecutan diariamente. La copia principal se mantiene

en el centro principal de TOC SA y se almacena dentro de una zona protegida. Las copias son encriptadas periódicamente y de forma remotamente almacenadas fuera del sitio.

34.1.5. REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Además de las estipulaciones mencionadas en el apartado *Protección de archivos*, el sellado de tiempo está incluido en los registros firmados digitalmente. El sellado de tiempo no tiene por qué ser de la naturaleza criptográfica.

34.1.6. Fuente de tiempo confiable

34.1.6.1. **Token de Sello de Tiempo**

La TSA de TOC garantiza que los token de sellado de tiempo son emitidos en forma segura e incluyen un identificador único de política (OID), valores de fecha y hora proveniente de una fuente confiable de tiempo UTC sincronizado en la precisión definida en esta política. Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el suscriptor para que sea sellado con el sello de tiempo.
- Un identificador para la política de marca de tiempo.
- Un número serial único que será usado para ordenar los TSTs así como para identificar un sello de tiempo específico.
- El Token de Sello de Tiempo tiempo calibrado a 1 segundo de la UTC, indicando la fuente de tiempo confiable.
- La firma electrónica que ha sido generada usando una llave que es sólo usada para la firma de los sellos de tiempo.
- La identificación de la TSA y de la TSU.
- La TSA de TOC establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

34.1.6.2. **Sincronización de los relojes con UTC**

La TSA de TOC declara utilizar una fuente fiable de tiempo, mediante un servidor basado en el Network Protocol (NTP) que sincronice con el tiempo UTC a través de una red de satélites GPS o en caso excepcional contra múltiples fuentes que incluyen el “National Measurement Institute”, el cual provee tiempo UTC; lo anterior con una desviación máxima de 1 segundo. Esta fuente de tiempo está basada en el NTP haciendo que la exactitud no disminuya por debajo de los requerimientos. De manera más específica:

- La calibración de la TSU es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la TSU se encuentra protegido contra amenazas ambientales que puedan afectar su precisión fuera del rango declarado.
- En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la TSA.

- En caso de detectarse una desviación más allá de la precisión declarada, la TSU no generará nuevos TST hasta que el tiempo correcto sea restaurado.
- TOC declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el TST.
- La administración del reloj de la TSU requiere de un quórum de 3 de 8.

34.1.7. SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de archivo es una tarea interna en TOC SA que no puede ser encargada a terceros.

Con la única excepción de puntos de Entidad de Registro autorizados, a los cuales se les permite archivar la información recogida durante el ciclo de vida de los certificados. En ese caso, esta información debe mantenerse de forma segura, accesible solo para personas autorizadas, y estará disponible para cualquier entidad de auditoría interna o externa exigida por TOC SA.

34.1.8. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Solo personal autorizado puede obtener acceso a los medios físicos que contienen archivos, copias de seguridad y otra información registrada.

Las comprobaciones de integridad se realizan automáticamente si el archivo incluye una firma digital.

34.1.9. PROCEDIMIENTO DE DESTRUCCIÓN DE MEDIOS

continuación, se presentan los diferentes procedimientos que debe seguir el personal responsable de TOC BIOMETRICS para velar por la eliminación y mantenimiento de manera segura, manteniendo la disponibilidad, integridad y confidencialidad de ésta.

- **Eliminación de lógica de discos duros**
  - **Reunir Dispositivos**: Se reunirán todos los dispositivos físicos que estén en desuso o en mal estado y que se encuentren ubicados en la bodega,
  - **Verificación de Información**: Se verificará si los dispositivos requieren de un respaldo para así proteger información sensible para TOC BIOMETRICS.
  - **Respaldar Información**: Se respaldará todo aquel dispositivo que contenga información valiosa para TOC BIOMETRICS.
  - **Eliminación de la información**: Luego de Respaldar la Información de los dispositivos que así lo requirieron, se dará comienzo a la eliminación segura de la información y al formateo del dispositivo.
  - **Verificación de los dispositivos**: Se verificará en qué condiciones físicas y estructurales se encontrarán los dispositivos y se separarán de 2 formas, las cuales se detallan a continuación:
  - **Dispositivos Dañados**: Todo aquel dispositivo dañado se separará de los demás para luego ser entregado a la empresa de destrucción de los dispositivos.
  - **Dispositivos en buen estado**: Todo aquel dispositivo que se encuentre en buenas condiciones será almacenado para una futura reutilización siempre que así sea considerado.
- **Eliminación de dispositivos físicos**
  - **Reunir Dispositivos**: Se agruparán todos los dispositivos físicos que estén en desuso o en mal estado y que se encuentren ubicados en la bodega,
  - **Verificación de los dispositivos**: Se verificará en qué condiciones físicas y estructurales se encontrarán los dispositivos y se separarán de 2 formas, que son:
  - **Dispositivos Dañados**: Todo aquel dispositivo dañado se separará de los demás para luego ser

entregado a la empresa de destrucción de los dispositivos.

- **Dispositivos en buen estado**: Todo aquel dispositivo que se encuentre en buenas condiciones será almacenado para una futura reutilización, siempre que así sea considerado.

34.1.10. REUTILIZACIÓN Y/O DESTRUCCIÓN DE MEDIOS DE RESPALDO.

A.Toda destrucción de documentación respaldada en papel, debe realizarse de manera controlada, previa autorización del dueño de la misma. Incorporando en el registro histórico: la fecha y método de destrucción, así como las partes que asistieron a la actividad en calidad de observadores del proceso.
B. El área de finanzas es la responsable de definir si los dispositivos desincorporados ya no contarán con vida útil para las actividades de TOC BIOMETRICS, por lo cual será el área encargada de solicitar la destrucción de los equipos desechados.
C. El área de soporte y seguridad de la información deberán definir, actualizar y ejecutar los procedimientos de destrucción de medios tecnológicos lógicos o físicos que llegasen a contener información sensible para TOC BIOMETRICS

34.2. CAMBIO DE CLAVES DE UNA EC

TOC SA, como prestador de servicios de TOC PERÚ, requiere cambio de claves para la EC que necesite renovar su certificado. Solo en casos excepcionales se puede TOC PERÚ repetir la ceremonia de creación de claves de la EC manteniendo las mismas claves creadas en un HSM para una ceremonia previa, en orden de enmendar cualquier error en el proceso.

Cuando se crea un nuevo certificado para una entidad, el periodo de validez aplicado a este certificado se verá limitado a la validez de las claves de las EC que lo emita.

34.3. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

34.3.1. PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Las ECs y/o ERs que operen bajo TOC SA están obligadas a hacer cumplir los controles necesarios para comprobar y demostrar que los procedimientos de gestión de incidentes y vulnerabilidades son eficaces. Las personas involucradas deben ser convenientemente entrenadas en sus roles y responsabilidades en el ejercicio de sus funciones.

34.3.2. ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

Si los recursos de hardware o de software se ven alterados o se sospecha que han sido alterados, TOC SA detendrá las operaciones normales hasta que se establezca un entorno seguro. De forma paralela, una auditoría se llevará a cabo con el fin de

identificar la causa y disponer las medidas necesarias para evitar futuras repeticiones.

En el caso de que los certificados digitales se emitan durante el periodo de incertidumbre y existe el riesgo de que estos certificados podrían verse comprometidas, a continuación, estos certificados serán revocados y los suscriptores serán notificados de la necesidad de volver a emitir sus certificados.

34.3.3. PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD

En el caso de que una clave privada se vea comprometida en la arquitectura de TOC SA y además de las estipulaciones en la sección Alteración de los recursos hardware, software y/o datos, las entidades subordinadas en función de la clave privada comprometida serán notificadas de este evento y se llevará a cabo las acciones necesarias.

Todos los certificados emitidos por entidades de subordinación a la clave comprometida desde el momento de compromiso de la clave y la revocación del certificado serán revocados, y los terceros que confían, así como los suscriptores, podrán identificar los certificados comprometidos a través de los servicios CRL u OCSP Además, se tomarán medidas para volver a emitir los certificados afectados.

34.3.4. CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

En el caso de un desastre (independientemente de su naturaleza) que afecte a las instalaciones principales de TOC SA, y cualquiera de los servicios que se proporcionan a partir de estos, el Plan de Continuidad de Negocio y Recuperación de Desastres de TOC SA se activará, asegurando que los servicios identificados como "críticos" están disponibles en menos de 72 horas después de la activación del plan. El resto de los servicios estaría disponible en los términos razonables, según se juzga adecuado para su importancia y nivel de criticidad. Para efectos del Sistema de Gestión de Continuidad de Negocio (SGCN), los escenarios declarados son los siguientes:

- Sin sistemas
- Sin agua potable
- Sin instalaciones
- Sin personas

34.4. CESE DE UNA EC O ER

34.4.1. ENTIDAD DE CERTIFICACIÓN

En el caso de que una EC bajo TOC SA se vea obligada a poner fin a sus actividades, las acciones mínimas que deben ejecutarse son:

- Notificar a todos los suscriptores de certificados y revocar todos los certificados en el marco de la EC.

- Informar a todas las partes de confianza que tienen una relación directa registrada con esa EC sobre la terminación de la prestación del servicio certificado. Esto también terminará la acreditación otorgada a la EC para operar bajo TOC SA.
- Realizar un aviso público de la terminación dentro de la sección de repositorio del sitio web de la EC afectada, y llevar a cabo otras comunicaciones públicas que se consideren necesarias para informar a la comunidad del tercero que confía.

En el caso de cese de una EC Raíz de TOC SA, esto implicará la terminación de toda la jerarquía que depende de esa CA raíz.

35. CONTROLES TÉCNICOS DE SEGURIDAD

35.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

35.1.1. GENERACIÓN DEL PAR DE CLAVES

Los pares de claves de las EC que operan en TOC SA, se generan y se instalan por personal que pertenezca a la EC TOC PERÚ bajo al menos el control de dos personas y separación de accesos en un procedimiento que cumple con las regulaciones aplicables. Los detalles de este procedimiento son:

- La generación del par de claves de la EC Raíz es auditado por un evaluador externo calificado.
- Las ECs Subordinadas se generan bajo la supervisión directa de los auditores internos de TOC SA.
- Las ceremonias de las ECs son ejecutados por personal de confianza designados.
- Hay una secuencia de comandos de ejecución pre-definido que se debe seguir durante la ceremonia.
- Durante la ceremonia, la auditoría es grabada lo suficiente en orden de probar que la ceremonia se realizó sin ningún riesgo de seguridad.
- Después de la ceremonia, un informe de la ceremonia se genera y debidamente archivada para referencia futura

El par de claves de la EC Raíz de la TOC SA se generan en los módulos de seguridad de hardware (HSM) acreditada en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos.*

El par de claves para la Política de las ECs emisoras en TOC SA pueden ser generados en los módulos de seguridad de hardware (HSM) acreditada en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos*.

El par de claves para la Política de las ECs emisoras en TOC SA pueden ser generados en forma “escrowable” y protegidos, importado y operado dentro de los módulos de seguridad de hardware (HSM) en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos*.

Otro par de claves distinto de los asignados a las Entidades de certificación pueden ser generados por componentes de software, excepto el "FEA" y los certificados de plataforma de enrolamiento, que deben generarse en dispositivos seguros de firma (FIPS 140-1 Nivel 2 y equivalentes, o más altos).

35.1.2. ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

En el Modelo de confianza de TOC SA, los perfiles específicos de certificados de entidad final permiten la generación de la clave privada de la ER o por el Suscriptor usuario final. Si las claves son generadas por la ER, se deben usar contenedores asegurando una distribución segura de estas que cumplan con el estandar FIPS 140-1 Nivel 3, o superior. En particular, se acepta el uso de archivos protegidos con contraseñas cifradas o software, tarjetas inteligentes u otros cripto-tokens válidos.

35.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Las claves públicas generadas por, o para, las entidades finales se envían a la EC por medio de canales seguros a través de las ERs de TOC SA, como parte de una solicitud de certificado en formatos TOC PERÚ bles, tales como PKCS # 10 u otros estándares de RSC.

35.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS TOC PERÚ

Las claves públicas de todas las ECs que operan bajo el Modelo de confianza de TOC SA se publican y se pueden descargar libremente desde su repositorio que se encuentra en

https://firma.toc.cl/indexpki.php

Los certificados raíz de confianza se pueden obtener directamente de los repositorios apropiados en la mayoría de navegadores y sistemas operativos.

35.1.5. TAMAÑO DE LAS CLAVES

TOC SA, como prestador de servicios de TOC PERÚ, impone el uso de un mínimo de longitud de 2048 bits RSA y ECC NIST P-256, P-384, o P- 521 pares de claves en todos los niveles de la jerarquía. Teniendo un ciclo de vida de máximo (3) años.

Los algoritmos hash soportados son SHA-1 y SHA-2, dependiendo de la jerarquía a la que pertenece el certificado de entidad final. En particular, no hay emisión de nuevos certificados SHA-1 después del 31 de diciembre del 2015.

35.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

El algoritmo utilizado en TOC SA para la generación de claves es RSA o ECC.

35.1.7. USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

Todos los certificados emitidos en TOC SA contienen los atributos "uso de la clave" y "uso extendido de la clave", como se define en el estándar X.509v3. Más información disponible en la sección Extensiones del certificado.-

35.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

TOC SA, como prestador de servicios de TOC PERÚ, ha establecido controles para asegurar que los riesgos derivados de un compromiso de la clave privada, se gestionan y se mantienen en niveles razonables. Estos controles son diferentes para los componentes principales (ECs) y las claves de usuario final.

35.2.1. CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Se requiere que las ECs de TOC SA utilicen módulos de seguridad de hardware, por lo menos compatible con FIPS 140-2 Nivel 2 para los componentes de PKI.

Los requisitos para los dispositivos criptográficos de usuario final (si los hay) pueden variar en términos del nivel de seguridad esperado.

Para el hardware (HSM) se cumple con el estándar FIPS 140-2 nivel 3 y es utilizado para generar, almacenar y usar las claves privadas de la TSA.

Criptografía en PKI

-El hardware criptográfico cumple el estándar FIPS PUB 140-2 nivel 3.

- El HSM es un SafeNet HSM Luna SA 5.1.

35.2.2. CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Las claves privadas de las ECs siempre están bajo el control multipersona. Los datos de activación necesarios para permitir a una Entidad de certificación, serán compartidos de tal manera que se necesiten al menos dos personas autorizadas para realizar cualquier operación delicada en una EC, excepto cuando se activa el reinicio de funcionamiento sin supervisión de ECs emisoras.

Las claves privadas para entidades finales están bajo el control exclusivo del suscriptor o del representante autorizado

35.2.3. CUSTODIA DE LA CLAVE PRIVADA

La clave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del titular. Bajo ninguna circunstancia TOC SA como prestador de servicios de TOC PERÚ guarda copia de la clave privada del titular ya que esta es generada por el mismo titular y no es posible tener acceso a ella por TOC SA o por TOC PERÚ.

35.2.4. BACKUP DE LA CLAVE PRIVADA

No aplica

35.2.5. ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas no se archivan para cualquier participante PKI.

35.2.6. TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO

El proceso de descarga de las claves privadas se realiza según procedimiento del dispositivo criptográfico y se almacenan de forma segura protegidas por claves criptográficas con control dual.

Para la EC que opere bajo el Modelo de confianza de TOC SA, es obligatorio que los pares de claves se operen en los Módulos de seguridad de hardware como se define en la sección *Controles y estándares para los módulos criptográficos*. Las claves privadas se pueden transferir a los módulos de seguridad de hardware adecuados para las operaciones de copia de seguridad y recuperación.

No hay ninguna estipulación para las llaves pertenecientes a otros participantes de PKI.

35.2.7. ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de la EC o ER mantenidas en los módulos criptográficos de hardware se almacenan en un formato cifrado apoyado por el proveedor de HSM.

Las claves privadas de entidad final deben utilizar contenedores cifrados que cumplen al menos con FIPS 140-1 Nivel 1.

35.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la EC en TOC SA se activa al iniciar el software de PKI y activando el HSM donde se almacena la clave. Este proceso requiere al menos un control dual-persona, a excepción de una EC emisora donde se permite la activación automática de claves en caso de fallo del sistema o reinicio.

La activación de la clave privada del suscriptor se estipula en la sección *Datos de Activación.*

35.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En las EC, la clave privada se desactiva por el apagado del servidor asociado o por terminar el software PKI o mediante la extracción o la puesta fuera de servicio el HSM que contiene la clave. Esta tarea puede ser realizada por un administrador del sistema y, previamente, tiene que ser notificado y autorizado a/por la EC responsable.

Por otro lado, la desactivación de las claves privadas de las ER o de los usuarios finales basados en hardware, se realiza mediante la extracción del dispositivo de seguridad (tarjeta inteligente u otros cripto-tokens TOC PERÚ dos) de la estación de trabajo donde es utilizada.

La desactivación de otras claves privadas del usuario final, mientras que no se encuentran basadas en el hardware, se lleva a cabo mediante el apagado del dispositivo en el que se almacena la clave privada. El suscriptor debe tomar todas las medidas razonables para evitar el uso no autorizado del dispositivo.

35.2.10. MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

El procedimiento para destruir una clave privada se realiza en los siguientes casos:

- La clave privada ya no se utiliza.
- El token o HSM contiene la clave que se ha deteriorado hasta el punto que impide el uso normal.
- El token se encuentra perdido o ha sido robado, y se sospecha que las teclas que contenía se ven comprometidas.

Asimismo, una clave privada puede ser destruida por el propietario de la clave o un representante legal. En tales casos, el certificado correspondiente será revocado y se le notificará a la comunidad. El procedimiento utilizado para destruir la clave privada depende del contenedor en cuestión, siendo responsabilidad del individuo

la ejecución de la destrucción, haciéndolo de una manera apropiada. En particular, para las claves privadas asociadas a las ECs, esta tarea debe ejecutarse bajo control dual y debe ser registrado un seguimiento apropiado de la información.

35.2.11. GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

El módulo criptográfico respecto de su tratamiento de seguridad:

- El CISO autoriza cambios y/o actualizaciones, sujeto al procedimiento respectivo.
- El módulo criptográfico respecto de su tratamiento de seguridad:
- Es evaluado periódicamente para comprobar su estado.
- Está registrado en el inventario de activos.
- Mantiene un espacio independiente separado del resto de dispositivos.
- No se manipula durante su transporte.
- Para uso en la firma de certificados se aplica al menos control dual.
- Previamente a retirarse del uso el dispositivo criptográfico, las claves privadas de las CA almacenadas son eliminadas.
- Requiere al menos control dual para acceder a su configuración y operación.
- Se mantiene un contrato de soporte y mantenimiento con el proveedor del dispositivo.
- Su configuración, incluyendo modificaciones y actualización, son documentadas y controladas.

35.2.12. EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

Sin estipulación adicional a la sección *Controles y estándares para los módulos criptográficos.*

35.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

35.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas en el Modelo de confianza TOC SA son archivados por un período de siete (7) años después de la expiración o revocación del certificado digital correspondiente.

35.3.2. PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo en plenamente operativo de un certificado comienza en la emisión y termina con la expiración o revocación del certificado.

El periodo de validez para los pares de claves se establece en la siguiente tabla:

Se debe entender que el periodo de validez de un certificado puede estar limitado por la propia validez de la EC emisora, ya que no se permite que una entidad subordinada extienda su validez más allá del emisor.

Los certificados son operativos para la validación de la firma y el descifrado desde la emisión hasta el final del periodo de archivo, tal como se indica en el apartado *Archivo de la clave pública.*

35.4. DATOS DE ACTIVACIÓN

35.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación para las ECs se generan y almacenan en tokens criptográficos y/o tarjetas inteligentes y son utilizados por personas autorizadas. Además, estos tokens requieren una contraseña o PIN con el fin de permitir el proceso de activación.

Las activaciones que requieran el control multi-perona, serán impuestas por la división de los datos de activación de varios tokens.

Los datos de activación de la entidad final, solo se establecen para claves privadas basadas en hardware. En particular:

- Claves privadas para la ER y Certificados reconocidos, requerirán el uso de un código PIN o contraseña de ocho o más caracteres con el fin de activar el dispositivo de hardware en el que se almacena la clave.
- Claves privadas para Certificados “FEA” se pueden generar e instalar sin el uso de una contraseña, aunque no es recomendable.
- Claves privadas para otros tipos de certificados deben ser generadas después de que el suscriptor es autenticado correctamente en el sistema en el que se crean las claves. Un método TOC PERÚ do es el uso de contraseñas razonablemente seguras para acceder a la interfaz de usuario de la ER.

35.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo las personas autorizadas deben conocer la contraseña o PIN para activar las claves privadas. En el caso de entidades finales, solo el suscriptor del certificado tiene derecho a conocer esta información.

En todos los casos, se requiere que el propietario sea el encargado de salvaguardar los datos de activación para la confidencialidad de esta información.

35.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

35.5. Distribución de la clave pública

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, estas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

Cada uno de los certificados de la EC Intermedia son firmados por los certificados raíz.

35.6. CONTROLES DE SEGURIDAD INFORMÁTICA

Los detalles de esta información se clasifican y por lo tanto no se hacen públicos. Los documentos que describen los Controles de seguridad informática solo están disponibles para las personas involucradas en TOC SA y solo son revelados a partes externas acreditadas para fines de auditoría.

Se requiere que las ECs y ERs que operen bajo el Modelo de confianza de TOC SA, cumplan con estos controles de seguridad. El cumplimiento se aplica periódicamente por un procedimiento de auditoría.

35.6.1. Responsable de la seguridad de la información

El Responsable de Seguridad de TOC PERÚ gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

Oficial de Seguridad de la información (OSI): Representa a TOC SAC en la definición y aplicación de los criterios de seguridad de la información tanto dentro de la organización como en la relación entre esta con sus clientes y proveedores. Analiza permanentemente el nivel de riesgo proponiendo soluciones efectivas. Mantener actualizadas las políticas, planes y procedimientos, además de difundirlas entre los colaboradores. Monitorear el cumplimiento de las políticas establecidas y es responsable además de gestionar el sistema de Gestión de seguridad de la información (SGSI) y el Sistema de Gestión de continuidad de Negocio (SGCN).

35.6.2. REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

TOC SA, en calidad de prestador de servicios de TOC PERÚ, exige el uso de adecuados procedimientos, además de medidas y sistemas técnicos con el fin de controlar eficazmente los riesgos de seguridad. Estos incluyen, pero no se limitan a:

- Políticas de contraseñas fuertes
- La mejora continua de los procedimientos administrativos y operativos
- El aislamiento físico de los sistemas confidenciales y
- Protección antivirus y sistemas de detección de antivirus
- Revisiones periódicas de seguridad interna

En particular, se garantiza el cumplimiento de la Línea de base y los requisitos de Validación extendida por el Foro Internacional de la EC, si es el caso.

35.6.3. EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

TOC SA, como prestador de servicios de TOC PERÚ, establece que las evaluaciones del ordenador cumplan con las ECs y ERs que operen bajo el Modelo de confianza. El cumplimiento de estas clasificaciones se garantiza mediante periódicas auditorías internas.

35.6.4. PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Acorde al objetivo de control A9 Control de acceso de la norma ISO 27001:2013, se definen las reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad; en el Sistema de Gestión de Seguridad de la Información (SGSI) de TOC.
Detalles del anterior propósito y finalidad, se encuentran en el documento PR-03-00 Control de Acceso, donde se especifican los protocolos relacionados con gestión de privilegios, equipos, software, entre otros.

Con respecto a las áreas de archivo de documentos en papel y archivos electrónicos, estas deben estar protegidas constantemente contra acceso no autorizado:

35.6.4.1. Deben estar en ambientes separados de las áreas públicas de registro.

35.6.4.2. Solo debe ingresar personal autorizado.

35.6.4.3. El ingreso y salida del personal debe ser registrado

35.6.4.4. Los terceros y el personal de limpieza pueden ingresar con autorización del Responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área

35.6.4.5. El ingreso y salida de documentos debe ser registrada

35.6.4.6. Debe estar cerrada bajo llave cuando no esté siendo usada

35.6.4.7. Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de TOC PERÚ o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del Operador de Registro, el cual será responsable de proteger la información proporcionada por el cliente.

35.7. CONTROLES TÉCNICOS DEL CICLO DE VIDA

35.7.1. Controles de desarrollo y mantenimiento de sistemas confiables

Los sistemas de TOC SA se han desarrollado utilizando una tecnología que garantiza la seguridad y la calidad mediante el establecimiento de una serie de políticas y procedimientos operativos y técnicos que controlan la construcción de los componentes PKI durante todas las fases del proyecto.

La autenticidad e integridad de los componentes de software críticos deben ser comprobadas antes de que estén activadas en un entorno de producción, mediante el

uso de firma de código u otros métodos TOC PERÚ.

Se debe realizar un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas de la EC, para asegurar que dichos requerimientos son considerados en los sistemas críticos

La EC debe mantener controles para proveer garantías razonables que las actividades de desarrollo de sistemas y mantenimiento son documentadas, testeadas, autorizadas, e implementadas apropiadamente para mantener la integridad de los sistemas de la EC.

35.7.2. CONTROLES DE GESTIÓN DE SEGURIDAD

TOC SA, como prestador de servicios de TOC PERÚ, recomienda seguir el enfoque de gestión de seguridad del certificado ISO 27000. En particular TOC SA, como operador principal del Modelo de confianza sigue una adopción no oficial de tales normas de seguridad.

35.7.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Los controles de seguridad del ciclo de vida y cambios relacionados están garantizados por la Metodología de TOC SA.

35.8. CONTROLES DE SEGURIDAD DE LA RED

TOC SA, como prestador de servicios de TOC PERÚ, impone la adopción de controles efectivos para minimizar cualquier riesgo relacionado con la seguridad de la red.

La información detallada acerca de estos controles se clasifica y solo se pone a disposición de los auditores externos después del proceso de autorización correspondiente.

En particular, el servidor utilizado para la EC Raíz de TOC SA son sistemas off-line, desconectados físicamente de cualquier red de ordenadores, y toda comunicación de información sensible está protegida mediante técnicas de firma digital y cifrado.

35.9. Control de acceso a la red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa " todo está restringido, a menos que esté expresamente permitido".

35.9.1.Política de utilización de los servicios de red

Para la activación y desactivación de derechos de acceso a las redes, se debe: 1

● Controlar el acceso a los servicios de red tanto internos como externos.

● Identificar las redes y servicios de red a los cuales se permite el acceso.

● Realizar procedimientos de autorización de acceso entre redes.

● Establecer controles y procedimientos de administración para proteger el acceso y servicios de red

35.9.2.Autenticación de usuarios para conexiones externas

TOC contempla servicios de conexiones externas SSL, VPN y primarios para usuarios que requieran conexión remota a la red de datos. La autenticación a los servicios VPN para usuarios con conexiones externas, está documentada mediante el procedimiento PROC Acceso Remoto VPN.

35.9.3.Identificación de equipos en la red

TOC controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.

35.9.4.Protección de los puertos de configuración y diagnóstico remoto

- Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estará restringido a los administradores de red o servidores.
- Los usuarios finales deberán permitir tomar el control remoto de sus equipos para el Área de Soporte, teniendo en cuenta no tener archivos con información sensible a la vista, no desatender el equipo mientras que se tenga el control del equipo por un tercero.
- Se deben implementar controles de acceso a nivel de puertos según los estándares tanto en las oficinas centralizadas, como en los sitios de teletrabajo.

35.9.5.Separación de redes

● TOC utilizará dispositivos de seguridad "firewalls", para controlar el acceso de una red a otra.

● La segmentación se realizará en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLANs en los equipos de comunicaciones.

● Las redes inalámbricas no podrán conectarse a redes alámbricas.

35.9.6.Control de conexión de las redes

● La capacidad de descarga de cada usuario final será de 1O Mb.

● La seguridad para las conexiones WiFi será WPA2 o superior.

● Se restringirá el acceso a mensajería instantánea, telefonía a través de interne!, correo electrónico comercial no autorizado, descarga de archivos de sitio peer to peer, conexiones a sitios de streaming no autorizado, acceso a sitios de pornografía., servicios de escritorio remoto a través de interne!, cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeíjo de la misma.

35.9.7.Control de enrutamiento de red

TOC proveerá a través del Proveedor de Servicio de Internet, el servicio de internet! institucional, el cual será administrado por el Oficial de Seguridad de Información y será el único servicio de internet! autorizado.

35.10. Reporte y respuesta a incidentes.

Tanto la identificación, registro, atención y comunicación de incidentes, se encuentra regulado en la Política de Gestión de Incidentes.

35.11. Interrupción de operaciones

En el caso de compromiso de las operaciones de la EC, de su clave privada, no deberán emitirse certificados hasta que se supere el incidente. El certificado comprometido de la EC deberá ser revocado. Los certificados firmados por ésta en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente dejarán de ser válidos. Se deberá comunicar inmediatamente a la AAC del INDECOPI el motivo

del compromiso, así como las acciones realizadas. Sus titulares deberán solicitar a la EC la re-emisión de nuevos certificados, debiendo ésta emitirlos, conforme al procedimiento establecido.

35.12. Gestión Documental

Para definir y establecer un marco de acción, directrices y responsabilidades para la gestión documental del Sistema Normativo (documentos) a los cuales estarán sujetas las distintas unidades de negocio y que puedan ser generados, modificados y manipulados por cada una de ellas, se referencia el documento “Política de Gestión documental”.

35.13. SELLADO DE TIEMPO

TOC SA, como prestador de servicios de TOC PERU, proporciona una Política de sellado de tiempo que regula el funcionamiento de las Entidades de sellado de tiempo según RFC3161. Este servicio está disponible por TOC SA como operador principal y otras entidades autorizadas que se adhieren a la TSP. Más información sobre los servicios y normas de sellado de tiempo se publica en:

https://firma.toc.cl/indexpki.php

Para otros datos que requieren tiempo e información de datos, como certificados y CRL, no es obligatorio estar basados en criptografía.

36. PERFILES DE CERTIFICADOS, CRL Y OCSP

36.1. PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo el Modelo de confianza de TOC SA cumplen con:

- Recomendación UIT-T X.509 (1997): Tecnología de la Información - Interconexión de sistemas abiertos - El directorio: Marco de autenticación, junio de 1997

- RFC 5280: Internet certificado de infraestructura de clave pública X.509 y CRL Perfil, abril de 2002 ("RFC 5280").

Esta sección de la CPS se proporciona para estipulación general y como una referencia a la Política de certificación específica para cada tipo de certificado, disponible en el anexo B: Políticas y perfiles de certificados aprobados.

36.1.1. NÚMERO DE VERSIÓN

Los certificados emitidos por la Entidad de Certificación TOC SA cumplen con el estándar X.509 Versión 3.

36.1.2. EXTENSIONES DEL CERTIFICADO

Las extensiones de certificado se describen en las tablas disponibles en el anexo A.

36.1.3. KEY USAGE

El “key usage” se describe en las tablas disponibles en el anexo A.

36.1.4. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Los certificados emitidos bajo TOC S.A pueden utilizar alternativamente SHA-1 o SHA-2. Los identificadores de objeto de los algoritmos son:

- Sha256withRSAEncryption: identificador de objeto :: = {iso(1) member-body(2) us(840) RSADSI (113549) PKCS (1) pkcs-1 (1) 11}
- Sha-1WithRSAEncryption: OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) RSADSI (113549) PKCS (1) pkcs-1 (1) 5}
- En su caso, se aplicarán algoritmos de identificación relacionados con ECC.

Y para TOC PERU SAC:

Nombre del documento	Declaración de Prácticas y Política de Autoridad de Sellado De Tiempo (TSA) de TOC PERU SAC (TOC PERU SAC)
OID	1.3.6.1.4.1.47911.1.1.1
Versión del documento	1.0
Autor	TOC PERU SAC (TOC PERU SAC)
OID (Object identifier)	1.3.6.1.4.1.47911.1.1.1 iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TOC PERU SAC(47911) pki(1) policyIds(1) ts-policy(1)

Cualquier cambio en el OID de cualquiera de los certificados y políticas o declaraciones de prácticas será aprobado previamente por la AAC.

36.1.5. FORMATOS DE NOMBRES

Los certificados emitidos bajo TOC PERÚ SAC y TOC SA contienen el "nombre completo", en formato X.500, para el emisor y el suscriptor, situado en los campos "Nombre del emisor" y "Nombre de sujeto", respectivamente, y se forman como se define en la sección Tipos de nombre.

36.1.6. RESTRICCIONES DE LOS NOMBRES

Las Entidades de Certificación no operadas por TOC SA se verán limitadas en cuanto a la emisión de certificados bajo un conjunto de nombres predefinidos y acordados (nombres de dominio, los sufijos de correo electrónico u otro componente del nombre). Para los casos excepcionales en los que no se aplican estas restricciones, estas ECs se incluirán en la auditoría externa para la garantía del cumplimiento en contra de cualquier requisito aplicable (incluyendo la Línea base y los Requerimientos de validación extendida de la EC / Foro internacional).

Las restricciones de nombres de dominio pueden ser también aplicadas al utilizar la Interfaz de RA MPK de solicitudes de certificados para las empresas que tienen acceso a una dedicada ER.

IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

La CPS de TOC PERU SAC tiene asignado el identificador (OID) 1.3.6.1.4.1.47911.1.2.2 el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a TOC PERÚ en un contexto global.

36.1.7. USO DE LA EXTENSIÓN POLICY CONSTRAINS

Las Entidades de Certificación emisoras no operadas por TOC SA se ven propiamente limitadas a cumplir con los Requerimientos de validación extendida de la EC / Foro internacional. Estas ECs tendrán dificultades por no permitir la emisión de sus propias ECs subordinadas y mediante el control de los usos de la clave permitidos en los certificados de usuario final. La exactitud de esta información está garantizada por las tareas de auditoría ejecutadas durante la ceremonia de Creación de clave de la EC.

36.1.8. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Esta información está disponible en el anexo A.

36.1.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

La extensión "Política de Certificación" identifica la Política de TOC SA asignada explícitamente con una Política de certificados. Las aplicaciones de software que requieren un modelo de certificado específico para procesar una firma digital debe comprobar esta extensión con el fin de verificar la idoneidad del certificado para el fin previsto.

36.2. PERFIL DE CRL

Las CRLs emitidas por la Entidad de Certificación TOC SA cumplen con el RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril 2002) y contienen los siguientes elementos básicos:

36.2.1. NÚMERO DE VERSIÓN

Las CRLs emitidas por TOC SA como prestador de servicios de TOC PERÚ cumplen con el estándar X.509 versión 1 y 2.

36.2.2. CRL Y EXTENSIONES CRL

El perfil genérico CRL se especifica en la siguiente tabla:

Si hay alguna consideración específica debe ser estipulada en la Política de certificación.

36.3. PERFIL OCSP

No aplica

36.3.1. NÚMERO DE VERSIÓN

TOC SA proporciona soporte para la versión 1 del RFC 2560 y RFC 5019.

36.3.2. EXTENSIONES OCSP

No aplica

37. AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

TOC SA monitorea y asegura el cumplimiento de los requisitos legales, de seguridad y de la industria, en todos los niveles del Modelo de confianza, a través de auditorías internas y externas.

Esas auditorías de conformidad externa e interna se ejecutan según lo definido por la EC / Foro Internacional en su Línea de base y los Requerimientos de validación extendida. Si se da el caso, otros requerimientos de evaluaciones nacionales y/o industriales pueden ser cumplidos.

Las evaluaciones y auditorías técnicas del INDECOPI deberán llevarse a cabo una

vez al año y cada vez que el INDECOPI lo requiera.

37.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Todas las ECs y ERs dependientes deben seguir el Programa de evaluación adecuado (como se estipula en la sección *Aspectos cubiertos por los controles*) en una frecuencia anual.

Las evaluaciones y auditorías técnicas del INDECOPI deberán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

37.2. IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

El evaluador se seleccionará cuando se requiera una auditoría o evaluación. A cualquier empresa o profesional cuyos servicios son contratados como auditor o asesor, debe de cumplir los siguientes requisitos:

- Capacidad y experiencia suficiente y acreditada para realizar los servicios requeridos (PKI de auditoría, evaluación de seguridad, etc.).
- En el caso de las auditorías externas, debe ser independiente de TOC SA a un nivel de organización.

37.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

La política de auditoría de TOC SA no permite ningún tipo de relación jurídica, organizativa o de otro tipo con el auditor externo que daría lugar a un conflicto de intereses.

37.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

TOC SA establece dos niveles de auditoría y acreditación.

- La EC raíz, la Política de las ECs y ECs emisoras pertenecientes u operados por TOC SA.

Entidades emisoras gestionadas por terceros que no hacen cumplir las restricciones de nombres deben ser incluidas en esta evaluación.

- Las ECs emisoras pertenecientes y / o gestionados por terceros hacen cumplir las restricciones de nombres. Estos servicios deben cumplir con las prácticas estipuladas en la presente CPS y las CP que tienen derecho a emitir, y son auditados y acreditados por TOC SA por medio de una auditoría interna realizada por TOC SA u otro auditor autorizado.

37.5. ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

En el caso de identificar una deficiencia, TOC SA adoptará y será responsable de todas las medidas correctivas necesarias.

En el caso de una deficiencia grave que afecte al funcionamiento fiable de una EC o ER, TOC SA podría decidir suspender temporalmente las actividades de los sistemas o servicios afectados hasta que se resuelva la deficiencia.

37.6. COMUNICACIÓN DE RESULTADOS

Todos los resultados de la evaluación estarán conformados por:

- Reporte detallado. Este documento incluye todos los temas que componen el programa de evaluación ejecutado en detalle. El informe detallado se considera privado y solo se encuentra disponible para el propietario de la Entidad de Certificación y la Entidad Aprobadora de la Política de TOC SA.
- Declaración del informe de auditoría. Este documento solo incluye una declaración formal por parte del auditor y refleja el resultado de la evaluación, una lista de los temas tratados y el resultado global. El informe resumido se considera público y solo se publica en el repositorio TOC SA.

38. OTROS ASUNTOS LEGALES Y COMERCIALES

38.1. TARIFAS

38.1.1. TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

La emisión de certificados en TOC PERÚ se considera un servicio comercial y por lo tanto está sujeto a tarifas. Los honorarios dependen del certificado y del proyecto y se acordarán antes de ponerla a disposición de los suscriptores.

TOC SA, como prestador de servicios de certificación de TOC PERÚ, no admite la renovación o re-emisión de clave de los certificados después de una revocación. El suscriptor debe solicitar un nuevo certificado digital mediante el uso de los procedimientos para su emisión.

38.1.2. TARIFAS DE ACCESO A LOS CERTIFICADOS

En general, TOC PERÚ no aplica tasa para el acceso a la información del certificado hecho público en los diferentes repositorios.

38.1.3. TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

En general, TOC PERÚ no aplica tasa para el acceso a la información del certificado hecho público en los diferentes repositorios.

38.1.4. TARIFAS DE OTROS SERVICIOS

TOC PERÚ, como operador de la TOC puede fijar tarifas para los diferentes servicios comerciales prestados a las partes que deseen participar en el Modelo de confianza.

38.1.5. POLÍTICA DE REEMBOLSO

La política de reembolso aplicable a los servicios comerciales prestados por TOC PERÚ está incluida en el "Acuerdo del suscriptor" comunicado al usuario final al prestar el servicio. Otras políticas de devolución pueden ser establecidas y en estos casos se deben comunicar de manera efectiva a todas las partes afectadas.

38.2. RESPONSABILIDAD

La EC dispondrá de garantías bancarias disponibles para satisfacer los requerimientos de los solicitantes de los certificados, de los Firmante/Titulares y de los terceros que confíen en los certificados, en caso se verifique responsabilidad de la EC.

Las responsabilidades de la EC incluyen las establecidas por la presente CPS, así como las que resulten de aplicación como consecuencia de la normativa colombiana, peruana e internacional.

La EC será responsable del daño causado ante el Titular o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Titular, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

38.3. EXONERACIÓN DE RESPONSABILIDAD

La EC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente CPS y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Entidad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Titular o Terceros

que confían en la normativa vigente, la presente CPS y sus Anexos.

- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.
- Fraude en la documentación presentada por el solicitante.

38.4. RESPONSABILIDADES FINANCIERAS

TOC PERÚ establece los controles adecuados para garantizar que los diferentes niveles de responsabilidad financiera son recibidos por los diferentes participantes, de acuerdo con su impacto en el Modelo de confianza.

38.4.1. COBERTURA DEL SEGURO

Para la EC Raíz, ECs emisoras y los servicios de certificación prestados directamente por TOC SA, se mantiene un contrato de seguro que cubre la responsabilidad expresada en la sección *Obligaciones*.

Para los afiliados y clientes corporativos que actúan como ECs o ERs, las condiciones contractuales acordadas entre las partes garantizan las responsabilidades asumidas por cada parte y transfieren los requisitos a favor del correspondiente seguro para las obligaciones transferidas.

38.4.2. Conformidad legal

Los controles que garantizan las prácticas de TOC son conformes con los requerimientos legales, regulatorios y contractuales. Estos se encuentran declarados en el SOA y regulados en la Política de Control de Acceso.

38.4.3. OTROS BIENES

Sin estipulación.

38.5. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

En general, una EC bajo TOC SA no puede revelar la información confidencial de un suscriptor, o utilizar dicha información para cualquier propósito, excepto:

- Para el personal que requiera la información para los fines de la presente CPS o para la prestación de los servicios.
- Con el consentimiento explícito del suscriptor.
- Si es necesario hacerlo por cualquier ley o un acuerdo aplicable.

38.5.1. ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

La información revelada al suscriptor o al tercero que confía mediante la EC emisora puede ser considerada confidencial.

Toda EC bajo TOC SA mantendrá los siguientes tipos de información confidencial y mantendrá controles razonables para evitar la exposición de dichos registros para personal no confiable.

- Todas las claves privadas
- Los datos de activación utilizados para acceder a las claves privadas o lograr acceso al sistema de la EC
- Cualquier plan de continuidad de negocio, de respuesta a incidentes, de contingencia y recuperación de desastres
- Cualquier otra práctica de seguridad, medidas, mecanismos, planes o procedimientos utilizados para proteger la confidencialidad, integridad o disponibilidad de la información
- Cualquier información en poder de la EC emisora de conformidad con la sección *Protección de la información personal*
- Cualquier transaccional, registro de auditoría y registro de archivo identificado en la sección *Procedimientos de auditoría de seguridad* o *Archivo de registros*, incluidos los registros de solicitud de certificado y la documentación presentada en apoyo de la solicitud de certificado ya sea TOC PERÚ da o rechazada.
- Los registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externa o interna y los informes de auditoría (con la excepción de la carta de un auditor que confirma la eficacia de los controles establecidos en la presente CPS)
- Toda la información clasificada explícitamente como "PRIVADA", "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL" cuando se genera o intercambia entre las partes involucradas.

38.5.2. INFORMACIÓN NO CONFIDENCIAL

La siguiente información se considerará como no confidencial:

- Toda la información contenida en los certificados emitidos y listas de revocación de certificados (CRL), incluyendo toda la información que se pueda obtener de este tipo.
- Toda la información clasificada expresamente como "PÚBLICA".

38.5.3. DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Las ECs emisoras de TOC SA son responsables de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las partes delegadas, como las entidades que gestionan las ECs subordinadas, emisoras o ERs, son responsables de proteger la información confidencial que se ha generado o almacenado por sus propios medios.

Para las entidades finales, los suscriptores de certificados son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesarios para acceder o utilizar la clave privada.

38.6. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

La política de privacidad de TOC SA se publica en el URL: https://firma.toc.cl/indexpki.php

Esta política cumple con los requisitos aplicables a los servicios comerciales internacionales, y específicamente con los requisitos aplicables de la EC / Foro Internacional.

38.6.1. POLÍTICA DE PRIVACIDAD

La información personal comunicada a TOC PERÚ por los suscriptores de certificados se almacena en una base de datos propia del operador de la EC o ER. Esta base de datos está convenientemente protegida para evitar cualquier acceso o modificación no autorizada.

Los suscriptores tendrán derecho a acceder a su información y solicitar su modificación o cancelación.

Estos derechos pueden hacerse efectivos mediante solicitud por escrito a la dirección de correo electrónico publicado en la sección *Persona de contacto* de este documento.

En el curso de sus funciones, las ECs emisoras de TOC SA operados por TOC necesitan almacenar y procesar los datos personales electrónicamente. Todas estas acciones deben llevarse a cabo de conformidad con las leyes suizas relacionadas con la seguridad de los datos y la privacidad y Firma Electrónica. Por otra parte, se aplican todas las disposiciones del apartado *Confidencialidad de la información comercial*.

38.6.2. INFORMACIÓN TRATADA COMO PRIVADA

La información personal acerca de un individuo que no está disponible públicamente en el contenido de un certificado o del CRL se considera privada.

38.6.3. INFORMACIÓN NO CALIFICADA COMO PRIVADA

Para mayor información personal, las disposiciones de la sección *Información no confidencial* se aplican respectivamente.

38.6.4. RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

TOC SA garantiza el cumplimiento de las obligaciones legales para las ECs, ERs y

otras entidades que operen bajo el Modelo de confianza de TOC SA. Cada uno de estos participantes es responsable de proteger la información privada que ha sido proporcionada por los suscriptores u otros participantes en la emisión y mantenimiento de certificados digitales.

38.6.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

Para llevar a cabo el servicio de proveer certificación, se requiere que TOC PERU SAC obtenga el consentimiento para utilizar la información personal del suscriptor.

Este consentimiento se entiende por la aceptación de las "Condiciones Generales" y / o "Contrato de usuario final" por el suscriptor. Esta TOC PERÚ es reconocida por la aceptación del suscriptor para obtener e instalar el certificado.

38.6.6. REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL

Los participantes en TOC PERU SAC divulgarán información personal de los participantes si es requerido por un proceso judicial o administrativo, previa presentación de las órdenes apropiadas de conformidad con las leyes aplicables del país en el que opera la EC.

38.6.7. OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN

No se estipula.

38.7. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual, incluidos los certificados digitales y las CRL emitidas bajo TOC SA y TOC PERU SAC, identificadores de objetos, los CPS y los diferentes CP son propiedad de los mismos.

Las claves privadas y públicas son propiedad de sus respectivos dueños.

Cualquier marca comercial o respaldada incluida en el Nombre Distintivo de un certificado está bajo la responsabilidad del suscriptor del certificado.

38.8. OBLIGACIONES

En esta sección se incluyen estipulaciones generales, términos específicos pueden ser establecidos en la Política de certificación apropiada para una comunidad de usuarios y tipo de certificado dado. Si tal es el caso, el suscriptor específico, el tercero que confía y otros acuerdos serán distribuidos entre las partes.

38.8.1. OBLIGACIONES DE LA EC

La EC Raíz de TOC SA, y TOC PERU SAC hará lo siguiente:

- Establecer una cadena de confianza mediante la emisión de un certificado, que es un certificado autofirmado.
- Asegurarse de que la Raíz firma cualquier EC subordinada emitida bajo la jerarquía de TOC SA
- Llevar a cabo correctamente el proceso de verificación se describe en la sección *Validación inicial de la identidad*
- Asegurar la exactitud e integridad de cualquier parte de la información del certificado que se genera o recopila por TOC PERÚ SAC, de acuerdo con la Política de certificación aplicable
- Asegurarse de que toda la información pertinente relativa a un certificado se registra (por medios electrónicos o de otro tipo) por un periodo de tiempo adecuado, y en particular, con el fin de proporcionar pruebas de los efectos de los procedimientos legales
- Utilizar sistemas fiables, procedimientos y recursos humanos en el desempeño de sus servicios
- Cumplir con cualesquiera otras disposiciones pertinentes de la CP o CPS pertinente, y otros documentos aprobados.

TOC PERÚ SAC como EC debe:

- Operar de acuerdo con los requisitos de esta CPS y cualquier nivel de servicio aplicable.
- Asegurarse que en el momento de emitir un certificado, este contenga todos los elementos requeridos por la CP o el PDS.
- Administrar sus claves de acuerdo con la sección *Protección de la clave privada y controles de ingeniería de los módulos criptográficos.*
- Asegurar la disponibilidad de un directorio de certificados y CRL
- Revocar inmediatamente un certificado si es necesario
- En particular, sea el caso, la EC respetará las garantías y obligaciones establecidas por la EC / Línea Base del Foro Internacional.

38.8.2. OBLIGACIONES DE LA ER

Las ERs que operan bajo la orden de TOC SA, como es el caso de TOC PERÚ deberán velar por:

- Funcionar de acuerdo con los requisitos de esta CPS.
- Sus certificados cumplan con todos los requisitos materiales de la presente CPS.
- No haya errores introducidos en la información del certificado por las entidades que aprueban la Solicitud de Certificado como resultado de un fallo en la gestión de la Solicitud de Certificado.
- No haya declaraciones falsas de hechos en el Certificado en las entidades que

aprueban la Solicitud de Certificado o expide el certificado.

- La disponibilidad de los servicios de revocación (en su caso) y el uso de un depósito conforme con el CPS aplicable en todos los aspectos materiales.

Los contratos y acuerdos comerciales de la ER podrían incluir garantías adicionales.

38.8.3. OBLIGACIONES DEL TITULAR Y DEL SUSCRIPTOR

Los suscriptores de los certificados emitidos bajo TOC PERÚ deben garantizar que:

- Toda la información suministrada por el suscriptor y contenida en el Certificado es verdadera y válida.
- Todas las representaciones hechas por el Suscriptor en la Solicitud de Certificado presentados son verdaderos y válidos.
- Su clave privada está protegida y que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del suscriptor.
- La obligación y garantía de no instalar y utilizar el certificado o los certificados hasta que se haya revisado y verificado la exactitud de los datos de cada certificado.
- La obligación y garantía de instalar el certificado sólo en el servidor accesible en el nombre de dominio que aparece en el certificado, y para utilizar el certificado únicamente en cumplimiento con todas las leyes aplicables, exclusivamente para el negocio autorizado de la empresa, y únicamente de conformidad con el "Acuerdo del suscriptor".
- El certificado se utiliza exclusivamente para los fines autorizados y legales, de conformidad con la presente CPS.
- Cada firma digital creada utilizando la clave privada correspondiente a la clave pública contenida en el certificado, es la firma digital del Suscriptor y el Certificado ha sido aceptado y es operativo (no caducado o revocado) en el momento de crear la firma digital.
- El Suscriptor es un Suscriptor usuario final y no una EC, y no está utilizando la clave privada correspondiente a cualquier clave pública contenida en el certificado a efectos de firmar digitalmente cualquier Certificado (o cualquier otro formato de clave pública certificada) o CRL, como una EC o de otra manera.
- La obligación y la garantía de que cesen de inmediato el uso de un certificado y su clave privada asociada, y la solicitud de inmediato que la entidad emisora de certificados revoca el certificado, en caso de que: (a) toda la información en el certificado es o se vuelve incorrecta o inexacta, o (b) existe cualquier mal uso o sospecha del compromiso de la clave privada del suscriptor asociado a la clave pública contenida en el certificado.
- La obligación y garantía de que cesen de inmediato todo el uso de la clave privada correspondiente a la clave pública contenida en un certificado al vencimiento o revocación de dicho certificado.

El "Acuerdo del suscriptor" podría incluir garantías adicionales.

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.
En particular los suscriptores y titulares tienen la responsabilidad de solicitar la Revocación de sus certificados en casos de compromiso de su clave privada.

garantías

38.8.4. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

Antes de confiar en un certificado o una firma digital, el tercero que confía debe:

- Validar el certificado y la firma digital (en particular comprobando si es que no se ha revocado, caducado o suspendido)
- Determinar y cumplir con los fines para los cuales se expidió el certificado y cualesquiera otras limitaciones de la dependencia o el uso del certificado que se especifican en la presente CPS.

  Si el tercero que confía se basa en una firma digital o certificado, en circunstancias en que no ha sido validado, asume todos los riesgos con respecto a ella (a excepción de aquellas que hubieran surgido si la parte que confía valida el certificado), y no tiene derecho a cualquier presunción de que la firma digital es efectiva a partir de la firma del suscriptor o que el certificado es válido.

  El tercero que confía también debe cumplir con las demás obligaciones pertinentes especificadas en la presente CPS incluyendo las impuestas a la entidad cuando se está actuando como suscriptor.

  Además, el tercero que confía debe considerar el tipo de certificado. La decisión final sobre si confía o no en una firma digital verificada, es exclusivamente del tercero que confía.

  El "Acuerdo del tercero que confía" podría incluir garantías adicionales.

38.8.5. OBLIGACIONES DE LA ENTIDAD

Conforme lo establecido en las Políticas de Certificación anexadas a este documento, en el caso de los certificados donde se acredite la vinculación del Titular con la misma será obligación de la Entidad solicitar a la ER la suspensión/revocación del certificado cuando cese o se modifique dicha vinculación.

38.8.6. OBLIGACIONES DE OTROS PARTICIPANTES.

La ER de TOC PERU no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes son especificados en este documento.

No se estipula.

39. Indemnización

El SUSCRIPTOR/TITULAR liberará de toda responsabilidad y en su caso indemnizará, a la EC y/o ER del uso indebido que haga del Certificado otorgado, es decir que no sea el uso indicado en el contrato del titular y

en los documentos brindados por la EC y/o ER (Políticas de certificación, CPS, RPS).

Para mayor detalle respecto a las disposiciones por las cuales una de las partes hace un conjunto de pagos por pérdidas o daños que afectan a la segunda parte, refiérase al contrato con el suscriptor.

40. Notificaciones

Los medios de notificación serán definidos en los contratos de titulares y suscriptores.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por TOC PERÚ S.A.C., mediante un comunicado publicado en la siguiente dirección: http://www.toc.pe

41. Enmendaduras y cambios

En el caso de que TOC realice una nueva versión de su CP o DCP, debidamente aprobada por la AAC, se comunicará con antelación a todos los colaboradores, INDECOPI y participantes de la IOFE los respectivos cambios o modificaciones que se lleven a cabo en el servicio de prestación de servicios que ofrece.

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio publicado para acceso público a través del sitio web de TOC Perú cumpliendo con cada uno de los requisitos para una emisión validada por la AAC. Además, será notificado a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

42. Resolución de disputas

El procedimiento de resolución de disputas será definido en los contratos de los titulares.

Ante cualquier disputa o conflicto que pueda surgir relativa a la interpretación y/o cumplimiento de acuerdos, ambas partes se someterán a un juzgado con árbitro, el cual tendrá la facultad de entregar un fallo objetivo imparcial para los involucrados. (agregar más información verídica de cómo se lleva a cabo el proceso).

43. Fuerza mayor

Las cláusulas de fuerza mayor serán definidas en los contratos de los titulares.

44. Limitaciones de responsabilidad

- La EC y la ER limitan su responsabilidad a la emisión y gestión de Certificados Digitales y, en su caso, de pares de claves de suscriptores y dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por la EC.
- La EC y la ER limitan su responsabilidad a la emisión y gestión de Certificados Digitales y, en su caso, de pares de claves, y limitan su responsabilidad mediante la inclusión de límites de uso del Certificado Digital, y límites de valor de las transacciones para las que puede emplearse el Certificado, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación.
- Todas las responsabilidades legales, contractuales o extracontractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del SUSCRIPTOR/TITULAR. En

ningún caso podrá el SUSCRIPTOR/TITULAR ni los terceros perjudicados reclamar a la EC y/o ER compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados digitales para fines de cifrado.

- Los derechos y los deberes asociados a la condición de EC y ER no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de dichas entidades. En caso de que la ER disponga de Agencias delegadas debidamente comunicadas a INDECOPI, seguirá siendo responsable de sus derechos y deberes de cara al SUSCRIPTOR/TITULAR o terceros perjudicados.

45. Derechos de propiedad intelectual

La ER de TOC PERÚ tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

46. Cláusulas Misceláneas, Acuerdo Íntegro y Cláusulas de Ejecución

46.1. Cláusula de divisibilidad: Cada una de las cláusulas es independiente. En ese sentido, una cláusula no podrá invalidar a otra en caso de adición, omisión o modificaciones, excepto previo acuerdo con el SUSCRIPTOR/TITULAR.

46.2. Cláusulas Misceláneas.

Toda cláusula miscelánea que se aplique a las operaciones que realiza TOC PERU SAC bajo la IOFE, serán establecidas o referenciadas en los contratos de suscriptores o terceros que confían

46.3. Acuerdo Integro

TOC PERU SAC establece en sus contratos de suscriptor y terceros que confían, cláusulas de acuerdo íntegro. En virtud de la cual se entenderá que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

46.4. Cláusulas de Ejecución

Toda cláusula de ejecución, tarifas de abogados y cláusulas de derechos que se aplique a las operaciones que realiza TOC PERU SAC estarán establecidas o referenciadas en los contratos de suscriptor y tercero que confía.

47. Otras Provisiones

No aplica

48. CONFORMIDAD CON LA LEY APLICABLE

TOC PERÚ es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades de Certificación, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

49. FINALIZACIÓN DE LA PSC TOC PERÚ

Antes de su finalización, TOC PERÚ informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con un periodo de anticipación de al menos treinta (30) días calendario. Además, TOC PERÚ tiene la obligación de comunicar a la AAC - INDECOPI y titular del certificado con (60) días de anticipación y declarar los procedimientos para la protección de los registros de auditoría ante la respectiva finalización. A no ser que la finalización de la ER no sea voluntaria, se comunicará de manera inmediata a los titulares. En caso contrario, TOC tiene que solicitar la cancelación como PSC en el registro público de Perú, detallando quién será el encargado de mantener los registros y certificados vigentes.

Además, las claves privadas de la EC incluyendo las copias de respaldo deberán ser destruidas de tal manera que la clave privada no pueda ser recuperada.

En el caso que el titular se oponga a la transferencia de su certificado, éste quedará sin efecto alguno resguardandolo por al menos (6años desde la emisión.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro PSC designado por éste, cumpliendo con el periodo de (10) años establecido por la AAC.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por la EC de TOC PERÚ que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección: https://www.toc.pe/.

49.1. Transferencia de las operaciones de registro para las solicitudes de revocación y reemisión

TOC se encargará de transferir las solicitudes de revocación y reemisión en caso del término de sus operaciones ya sea de manera voluntaria o por fuerza mayor. Teniendo un plazo de 15 días para recibir la objeción del titular del certificado, en caso contrario se da por hecha la transferencia hacia otra PSC.

50. Obligaciones financieras

- El SUSCRIPTOR/TITULAR deberá abonar las tarifas acordadas con la EC o la ER.
- El SUSCRIPTOR/TITULAR liberará de toda responsabilidad y en su caso indemnizará, a la EC y/o ER del uso indebido que haga del Certificado otorgado, es decir que no sea el uso indicado en el presente contrato y en los documentos brindados por la EC y/o ER (Políticas de certificación, CPS, RPS).

51. Vigencia y Conclusión

La vigencia del documento “Política de Certificación EC TOC PERÚ” entrará en vigencia una vez que la AAC de la IOFE lo aprueba. Una vez aprobado, estará vigente por (5) años, siendo este el máximo plazo de vigencia establecido por la AAC.

52. BIBLIOGRAFÍA

a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012
f) Decreto Supremo 026-2016
g) Declaración de Prácticas de TOC SA v1
h) Ley N° 27269, de Firmas y Certificados Digitales.
i) Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105-2012-PCM.
j) Ley N° 29733, de Protección de Datos Personales

k) RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” del Internet Engineering Task Force (IETF) (que sustituye a la RFC 2527).
l) Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16º Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.

País (C)	<Código del país del suscriptor> m/e
Información del asunto de la Clave pública	2048 bit RSA f

Extensiones x.509

Autoridad del Key Identifier	Extensión marcada como NO-crítica
Key Identifier	<KeyID>
Asunto del Key Identifier	Extensión marcada como NO-crítica
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
Capacidades del SMIME (opcional)	[1] Capacidades del SMIME Object ID=1.2.840.113549.3.2 Parámetros=02 02 00 80 [2] Capacidades del SMIME Object ID=1.2.840.113549.3.4 Parámetros=02 02 00 80 [3] Capacidades del SMIME Object ID=1.3.14.3.2.7 [4] Capacidades del SMIME Object ID=1.2.840.113549.3.7

Punto de distribución del CRL	Extensión marcada como NO-crítica
Nombre completo	[1]CRL Distribución Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Authority Information Access	Extension marked non-critical.
Extensiones	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL-TO-ISSUER-CERT>

Key Usage	Extension marked critical.
Key Usages Permitidas	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

53. ANEXO A: PERFIL DE CERTIFICADO DIGITAL

Agregar tabla del certificado digital que se van a emitir

Versión 2	(i.e. X.509 versión 3)
Único número de serie	Los números de serie son asignados por la EC
Algoritmo de firma	Sha1RSA o Sha2RSA
Nombre Distintivo del emisor	
Nombre Común (CN)	<Nombre de la EC emisora>
Unidad Organizativa (OU)	<Opcional>
Unidad Organizativa (OU)	<Opcional>
Organización (O)	<Organización que emite>
País (C)	<País que emite>
Validez	
No antes de	Hora de emisión
No después de	1 – 3 años f
Asunto	
Email (E)	<Email del suscriptor> m/e
Nombre Común (CN)	<Nombre Común del suscriptor, persona jurídica autorizada> m/e
Localidad (L)	<Localidad del suscriptor> o/e
Nombre del Estado o Provincia (ST)	<Estado del suscriptor> o/e

Unidad Organizativa (OU)	<Opcional> “Usuario de CertifyID Advanced” o/f
Unidad Organizativa (OU)	<Opcional> o/e
Unidad Organizativa (OU)	<Opcional> Validado por [Appointed ER] – CertifyID ER o/f vía de emisión [Nombre del suscriptor cliente MPKI]
Unidad Organizativa (OU)	<Opcional, Unidad Organizativa del suscriptor> o/e
Organización (O)	<Opcional, Organización del suscriptor> o/e