Política de Seguridad TOC PERU SAC

OID 1.3.6.1.4.1.53748.1.1.008

Información del documento

Nombre	POLÍTICA DE SEGURIDAD
Realizado por	TOC PERU S.A.C.
Dirigido a	INDECOPI
Versión	1.0
Fecha	03/10/2018

Historial de versiones

Versión	Fecha	Descripción
1.0	03/10/2018	Elaboración de documento inicial.
1.0	02/10/2019	REVISION DE DOCUMENTO
1.0	01/09/2020	Revisión de documento
1.0	09/08/2021	Revisión de documento
1.0	30/09/2022	Revisión de documento

ÍNDICE **3**

1 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, re-emisión, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC de PERU SECUE y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

1.1 PKI PARTICIPANTES

1.1.1 ENTIDAD DE CERTIFICACIÓN TOC PERU (EC TOC PERU)

TOC PERU, 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.

A TOC PERU como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la AAC a fin de poder ingresar a la IOFE.

1.1.2 ENTIDAD DE REGISTRO TOC PERU (ER TOC PERU)

TOC PERU, brinda los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

1.1.3 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 PERU, 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 ofrece TOC PERU son provistos, en un contrato de tercerización, por **TOC S.A.** en Chile.

1.1.4 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 Declaración de Prácticas de Certificación de TOC PERU.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por TOC PERU conforme a lo establecido en la Política de Certificación.

1.1.5 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 de 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 corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

1.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la Declaración de Prácticas de Certificación de TOC PERU.

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

1.1.7 TERCERO QUE CONFÍA

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

1.1.8 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.

Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone TOC PERU es permanente.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por TOC SA de acuerdo a su documento Declaración de Prácticas de Certificación, publicado en:

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

3. ALCANCE

La presente política es de cumplimiento obligatorio para el personal contratado por TOC PERU que participan de las operaciones críticas de los servicios descritos en la Declaración de Prácticas de Registro y Declaración de Prácticas de Certificación.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TOC PERU, en calidad de Entidad de Registro, tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de sellado de tiempo, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la ER en los ámbitos legales, regulatorios y contractuales.

5. SEGURIDAD FÍSICA

5.1. UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la ER de TOC PERU debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

5.2. SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de TOC PERU, los medios que garanticen la seguridad física de los equipos y del personal, deben implementar los siguientes controles:

5.2.1. Señalización de zonas seguras
5.2.2. Provisión de extinguidores contra incendios
5.2.3. No debe existir cableado eléctrico expuesto
5.2.4. Uso de estabilizadores y supresores de picos

5.3. 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:

5.3.1. Deben estar en ambientes separados de las áreas públicas de registro.
5.3.2. Solo debe ingresar personal autorizado
5.3.3. El ingreso y salida del personal debe ser registrado

5.3.4. 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
5.3.5. El ingreso y salida de documentos debe ser registrada
5.3.6. Debe estar cerrada bajo llave cuando no esté siendo usada
5.3.7. Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de TOC PERU 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.

5.4. 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".

5.4.1. 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

5.4.2. 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.

5.4.3. 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.

5.4.4. 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.

5.4.5. 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.

5.4.6. Control de conexión de las redes

- La capacidad de descarga de cada usuario final será de 10 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.

5.4.7. 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.

5.5. PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA

Las instalaciones deben estar protegidas contra exposición al agua, en particular, las áreas de archivo deben estar distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

5.6. PROTECCIÓN CONTRA INCENDIOS

Las instalaciones deben poseer las siguientes medidas para la prevención y protección contra incendios:

5.6.1. Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de TOC PERU

5.6.2. Se debe contar con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.

5.6.3. Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado

5.7. ARCHIVO DE MATERIAL

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), deben estar protegidos en las áreas de archivo, en contenedores de protección contra fuegos y deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos contenedores debe estar restringido a personal autorizado.

5.8. GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

5.9. COPIA DE SEGURIDAD EXTERNA

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado.

6. GESTIÓN DE ROLES

6.1. ROLES DE CONFIANZA

Los roles de confianza deben ser definidos de la siguiente manera:

- Responsable de la ER: Son aquellos responsables de dar de alta a los operadores en las plataformas de la ER.
- Responsable de la EC: Son aquellos que están autorizados para hacer instalaciones, configuraciones y al mismo tiempo, mantener los sistemas para la administración de los servicios.
- Responsable de Seguridad: Es aquel responsable de la administración e implementación de las políticas, planes y procedimientos de seguridad y privacidad de la información
- Operadores de Registro: Es aquel responsable de comprobar la autenticidad de la información entregada por el solicitante para la emisión, re-emisión, revocación, suspensión o modificación de certificados digitales.
- Auditores:

Estos roles deben ser asignados formalmente por el Responsable de TOC PERU en calidad Entidad de Registro.

La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.

6.2. NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los cambios en los documentos normativos requieren de la autorización de los Responsables de la ER, el Responsable de Seguridad y el de Privacidad, dichos roles no son incompatibles y pueden ser asumidos por un mismo cargo.

6.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza se deben emplear controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a los sistemas de Registro dependen de la configuración de los sistemas de la EC de TOC PERU.

6.4. AUDITORÍA

El auditor asignado por el INDECOPI deberá ser siempre una persona independiente de las operaciones de registro.

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.

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

7. GESTIÓN DEL PERSONAL

7.1. CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de registro digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos.

Asimismo, deben tener experiencia relacionada a los temas de certificación digital.

8. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

8.1. 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

8.2. TIPOS DE EVENTOS REGISTRADOS

Los sistemas de información sensible son provistos por la EC de TOC PERU ya que es esta quien administra y define los logs de auditoría.

Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.

La ER de TOC PERU genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.

- Cambios en el personal.

- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores software/hardware.

8.2.1. 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.

8.3. FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

8.4. PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro deben conservarse por un periodo de diez (10) años.

8.5. PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

8.6. COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA

Todas las solicitudes y contratos físicos serán generados con copia y los documentos electrónicos tendrán una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el Responsable de TOC PERU en calidad Entidad de Registro.

8.7. AUDITORÍA

Las auditorías internas se llevarán a cabo al menos una vez al año en TOC PERU en calidad Entidad de Registro.

Las evaluaciones técnicas de INDECOPI se llevarán a cabo una vez al año y cada vez que INDECOPI lo requiera.

8.7.1. AUDITORÍA DE REGISTRO

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

8.7.2. AUDITORÍA DEL ARCHIVO

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

8.7.3. 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.

8.8. NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO

Las notificaciones automáticas dependen de los sistemas de la EC de TOC PERU, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

8.9. VALORACIÓN DE VULNERABILIDAD

Los sistemas de registro son administrados por la EC de TOC PERU, por lo que la protección perimetral de redes corresponde a la infraestructura de TOC SAC.

9. TARIFAS, VALORES Y REEMBOLSO DE SERVICIOS

9.1. Tarifas

Las tarifas correspondientes a los servicios brindados por TOC SAC, serán informadas por el área de ventas, quienes pondrán a disposición de los clientes la información detallada de los valores .

- Cargo por emisión de certificado.
- Cargos de re- emisión de certificado.
- Tarifas de acceso al certificado.
- Revocación o tarifas de acceso a la información de estado.
- Honorarios por otros servicios tales como el acceso a la correspondiente CP o CPS.
- Política de reembolso.

9.2. Reembolso de Servicios

TOC SAC incluye políticas de Reembolso en los contratos del suscriptor la cual aplica para los siguientes casos:

- En el caso que un certificado no pueda ser instalado correctamente.
- En el caso que se proporcione un certificado de propósito o características tecnológicas diferentes.

10. ARCHIVO

10.1. TIPOS DE EVENTOS REGISTRADOS

Se mantiene: los datos de los suscriptores y titulares, los contratos y documentos que dan constancia de cada solicitud realizada en la ER, las claves públicas de dicha entidad y el registro de auditorías.

10.2. PERIODO DE CONSERVACIÓN DEL ARCHIVO

El periodo mínimo que se conservarán los archivos es por un periodo de diez (10) años, el cual es el periodo máximo requerido por la legislación vigente. Transcurrido este tiempo, los archivos de auditorías serán debidamente destruidos unicamente con la autorización de INDECOPI

De ser necesario, las aplicaciones requeridas para tener acceso a un archivo también deberán ser archivadas.

10.3. PROTECCIÓN DEL ARCHIVO

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos deben estar firmados de manera manuscrita y digital respectivamente para prevenir cualquier modificación.

El ingreso y salida de documentos físicos y digitales debe ser registrado para impedir la pérdida o destrucción no autorizada.

Debe tomarse en consideración la posibilidad de re-firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

10.4. PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Mensualmente, la integridad del archivo debe ser verificada.

11. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

11.1. PLAN DE CONTINGENCIAS

La ER de TOC PERU mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones de registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

El plan asegura que los servicios de registro para los procesos de emisión y revocación, puedan ser reasumidos dentro de un plazo máximo de veinticuatro (24) horas.

Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, conjuntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

La recuperación de los sistemas administrados por la EC, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC. En esos casos, TOC PERU en calidad Entidad de Registro informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

11.2. COMPROMISO DE LA CLAVE PRIVADA

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

11.3. 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.

12. CONFIDENCIALIDAD DE INFORMACIÓN

12.1. INFORMACIÓN CONSIDERADA CONFIDENCIAL

La ER de TOC PERÚ mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares y terceros en quien confían.
- Se asegura la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.
- Se permite la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

12.2. INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

La siguiente información será considerada no confidencial:

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

13. DERECHOS DE PROPIEDAD INTELECTUAL

Propiedad de la Declaración de Prácticas de Certificación:

"La propiedad intelectual de esta Política de Seguridad, Declaración de Prácticas de Certificación y de las Políticas de Certificación asociadas pertenece a TOC SAC."

Propiedad de los certificados :

"TOC SAC será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita si no se acuerda explícitamente lo contrario".

Normas y políticas:

"Regular las normas y políticas de conocimiento público, resguardando la propiedad intelectual y velar por la No utilización de esto sin previo aviso o autorización por TOC".

14. CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la ER de TOC PERU, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.