Política de Seguridad TOC PERU SAC

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**

ÍNDICE

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 PERUcomo 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.

2 RESPONSABILIDADES

TOC PERU 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 TOC SA.

Asimismo, TOC PERU 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 PERU son recibidas directamente por TOC PERU como prestador de Servicios Digitales o a través de nuestra Entidad de

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 de registro descritos en la Declaración de Prácticas de Registro.

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:

a) Señalización de zonas seguras
b) Provisión de extinguidores contra incendios
c) No debe existir cableado eléctrico expuesto
d) Uso de estabilizadores y supresores de picos

5.3 PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas de archivo de documentos en papel y archivos electrónicos, deben estar protegidas constantemente contra acceso no autorizado:

a) Deben estar en ambientes separados de las áreas públicas de registro.
b) Solo debe ingresar personal autorizado
c) El ingreso y salida del personal debe ser registrado

d) 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
e) El ingreso y salida de documentos debe ser registrada
f) Debe estar cerrada bajo llave cuando no esté siendo usada
g) 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 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.

5.5 PROTECCIÓN CONTRA INCENDIOS

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

a) Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de TOC PERU
b) Se debe contar con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.
c) 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

5.6 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.

5.7 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.

5.8 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
- Responsable de Seguridad
- Responsable de Privacidad
- Operadores de Registro
- 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.

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.

7.2 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro, incluyendo:

- Verificación de antecedentes criminales

- Verificación de antecedentes crediticios

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

7.3 REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de registro deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.

- Los aspectos de la RPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.

- Requisitos legislativos en relación a sus funciones.

- Sus roles en relación al Plan de Contingencias.

7.4 FRECUENCIA DE LAS CAPACITACIONES

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

7.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores.

7.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

Dichas sanciones deben estar establecidas en los contratos de cada empleado y/o contratista.

7.7 REQUERIMIENTOS DE CONTRATISTAS

El personal contratado para fines específicos dentro de las operaciones de TOC PERU en calidad Entidad de Registro, será evaluado respecto de sus antecedentes criminales, conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC de TOC PERU.

8 PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

8.1 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 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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 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.

8.8 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 ARCHIVO

9.1 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.

9.2 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.

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

9.3 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.

9.4 PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Mensualmente, la integridad del archivo debe ser verificada.

10 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

10.1 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.

10.2 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.

10.3 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.

11 CONFIDENCIALIDAD DE INFORMACIÓN

11.1 INFORMACIÓN CONSIDERADA CONFIDENCIAL

La ER de TOC PERU 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.

11.2 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.

12 RESPONSABILIDADES

El Responsable de Seguridad de TOC PERU 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.

13 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.