



## La Declaración de Prácticas y Política (VAPS) de la TSA de la TOC PERU SAC

### Control de cambios y versiones

<b>Versión</b>	<b>Fecha</b>	<b>Descripción</b>	<b>Responsable</b>	<b>Estado</b>
1.0	28/03/2018	Elaboración	Gerencia de Informática y Tecnología	Culminada
1.0	27/03/2019	Revisión anual	Gerencia Seguridad y QA	Culminada
1.0	01/09/2020	Revisión anual	Gerencia Seguridad y QA	Culminada
1.0	09/08/2021	Revisión anual	Gerencia Seguridad y QA	Culminada



## CONTENIDO

1. Introducción
2. Alcance
3. Definiciones, Acrónimos Y Abreviaturas
  - 3.1 Definiciones
  - 3.2 Acrónimos Y Abreviaturas
4. Conceptos Generales
  - 4.1 Servicios De Sellado De Tiempo
  - 4.2 Autoridad
  - 4.3 Solicitante, Suscriptor Y Usuario
  - 4.4 Política De Sellado De Tiempo Y Declaración De Prácticas De TSA
    - 4.4.1 Propósito
      - 4.4.1.2 Organigrama de la TSA
    - 4.4.2 Nivel de especificad
    - 4.4.3 Enfoque
5. Políticas De Sellado De Tiempo
  - 5.1 Visión General
  - 5.2 Identificación
  - 5.3 Comunidad De Usuarios Y Aplicabilidad
  - 5.4 Conformidad
6. Obligaciones Y Responsables
  - 6.1 Obligaciones De La TSA
    - 6.1.1 Generalidades
    - 6.1.2 Obligaciones De La TSA Con Los Suscriptores
  - 6.2 Obligaciones De Los Solicitantes Y Suscriptores
  - 6.3 Obligaciones De Los Terceros Que Confían
  - 6.4 Responsabilidades
    - 6.4.1 Responsabilidades De La TSA
    - 6.4.2 Responsabilidades Del Suscriptor
    - 6.4.3 Responsabilidades Del Usuario
7. Limitaciones De Responsabilidad, Políticas De Reembolso E Indemnizaciones
8. Requisitos Sobre Las Prácticas De La TSA
  - 8.1 Declaración De Las Prácticas De La TSA Y Declaración De Libre Divulgación
    - 8.1.1 Declaración De Las Prácticas De La TSA
    - 8.1.2 Declaración De Libre Divulgación De Las Prácticas De La TSA
  - 8.2 Ciclo de vida de la gestión de las claves
    - 8.2.1 Generación de las claves de la TSA
    - 8.2.2 Protección De Las Claves Privadas De La TSU
    - 8.2.3 Distribución De Las Claves De La TSU
    - 8.2.4. Regeneración De Las Claves De La TSU
    - 8.2.5 Fin Del Ciclo De Vida De Las Claves De La TSU
    - 8.2.6 Gestión Del Ciclo De Vida Del Módulo Criptográfico Usado Para La Firma De Sellado De Tiempo.
  - 8.3 Sellado De Tiempo
    - 8.3.1 Sellado Digital De Tiempo
    - 8.3.2 Sincronización De Relojes
  - 8.4 Gestión Y Operación De La TSA
    - 8.4.1 Gestión De La Seguridad
    - 8.4.2 Información Confidencial Y/O Privada



- 8.4.3 Gestión Y Clasificación De Activos
- 8.4.4 Seguridad Del Personal
- 8.4.5 Seguridad Física Y Del Entorno
- 8.4.6 Gestión De Operaciones
- 8.4.7 Gestión De Acceso A Los Sistemas
- 8.4.8 Mantenimiento Y Despliegue De Sistemas Confiables
- 8.4.9 Compromiso De Los Servicios De La TSA
- 8.4.10 Extinción De La TSA
- 8.4.11 Cumplimiento De Los Requisitos Legales
- 8.4.12 Registro De Información Concerniente A La Operación De Los Servicios De Sellado De Tiempo
- 8.5 Aspectos Organizacionales
- 9. Consideraciones De Seguridad
- 10. Auditorias
- 11. Publicación De La Declaración De Practicas
- 12. Bibliografías.



## 1. INTRODUCCIÓN

La Declaración de Prácticas y Política (VAPS) de la TSA de la TOC PERU SAC, ha sido elaborada respetando los lineamientos establecidos por la normativa sobre certificación digital aprobada por el Estado Peruano y tiene un ámbito de aplicación para todos los participantes que figuran detallados en el numeral 5.3 del presente documento denominado Comunidad de usuarios y aplicabilidad.

La acreditación de la TOC PERU SAC como Prestador de Servicios de Valor Añadido, en la modalidad de Autoridad de Sellado de Tiempo, se encuentra a cargo de la Autoridad Administrativa Competente, quien se encargará de la publicación de dicha condición de acreditación, para efectos de información a terceros.

## 2. ALCANCE

El presente documento constituye la Declaración de Prácticas de Sellado de Tiempo de TOC PERU SAC, en su calidad de Autoridad de Sellado de Tiempo (TSA), en donde se definen los mecanismos relacionados con la Política de Sellado de Tiempo y la manera en la que la política es implementada.

Este documento describe, según la legislación aplicable, las obligaciones y proporciona información a todas las partes que requieren, utilizan y validan Sellos Digitales de Tiempo (TST).

También incorpora las recomendaciones de las normas internacionales RFC 3628 - "Policy Requirements for Time-Stamping Authorities (TSAs)" y ETSI TS 102 023 - "Electronic Signatures and Infrastructures (ESI) - Policy requirements for time-stamping authorities".

El Sellado de Tiempo (TS), es un servicio mediante el cual la TOC PERU SAC suministra de manera electrónica y a solicitud del suscriptor, un Sello Digital de Tiempo (TST) firmado electrónicamente por la TSA, que permite verificar la existencia de un mensaje de datos desde la fecha y la hora del día en que el suscriptor hizo la solicitud de Sellado de Tiempo. Este servicio es útil cuando se requiere crear evidencia digital confiable y manejable para asociar información de fecha y hora a transacciones, de tal forma que estas puedan ser comparadas una contra otra posteriormente.

La presente Declaración de Prácticas y Políticas de Valor Añadido (VAPS) para la Autoridad de Sellado de Tiempo de TOC PERU SAC ha sido redactada conforme lo establece la "Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", Versión 3.3.

### 3. DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS

#### 3.1. Definiciones

- **Acuerdo de Prestación de Servicios de Sellado de Tiempo:** convenio o documento similar que tiene por objeto regular los derechos y obligaciones derivados de la prestación de los Servicios de Sellado de Tiempo (TS), entre TOC PERU SACy el suscriptor. No es necesario contar con dicho acuerdo en el caso que el suscriptor sea la TOC PERU SAC.
- **Autoridad de Sellado de Tiempo (TSA):** Es la entidad de confianza, que emite Sellos Digitales de Tiempo (TST), en el contexto de este documento se refiere a la Oficina Nacional de Procesos Electorales.
- **Certificado Digital de la Autoridad de Sellado de Tiempo:** Es el Certificado Digital de la TSA que permite firmar los Sellos digitales de Tiempo.
- **Declaración de Prácticas y Políticas de Sellado de Tiempo:** Documento que reúne las reglas que la TSA utiliza para la aplicabilidad del Servicio de Sellado de Tiempo (TS) a una comunidad. Se describen los papeles, responsabilidades y relaciones entre el solicitante, suscriptor y usuario final y la TSA. Además, las reglas de solicitud, adquisición, gestión y uso de los Sellos digitales de Tiempo (TST); y, las reglas del proceso de emisión de los Sellos digitales de Tiempo.
- **Firma Digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que se refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica.
- **Lista de Certificados Digitales Cancelados:** Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.
- **Mensaje de datos:** Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.
- **PKI:** En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital y el no repudio de transacciones electrónicas.
- **Protocolo NTP:** Comúnmente referido solamente por sus siglas, NTP, se deriva de la frase inglesa "Network Time Protocol". Es un protocolo de Internet utilizado para transferir

información del tiempo (fecha y hora) a través de una red. NTP es utilizado para sincronizar el tiempo en clientes de red a una hora precisa.

- **Sello Digital de Tiempo (TST):** Es el conjunto de datos firmado que vincula un documento digital a un tiempo específico, evidenciando que este documento digital existió antes del tiempo indicado.
- **Servicio de Sellado de Tiempo (TS):** Es la generación de los Sellos Digitales de Tiempo (TST) y la administración de este servicio.

### 3.2. Acrónimos y abreviaturas

- **CRL** Lista de Certificados Digitales Cancelados
- **EC** Entidad de Certificación.
- **ETSI:** European Telecommunications Standards Institute - Instituto Europeo de Normas de Telecomunicaciones.
- **ETSI TS 101 861:** Time Stamping Profile. Perfil de Sellado de Tiempo.
- **ETSI TS 102 023:** Policy Requirements for Time-Stamping Authorities. Equivalente al IETF RFC 3628.
- **FIPS:** Federal Information Processing Standard - Estándares del Gobierno Norteamericano para el procesamiento de la información.
- **HASH:** Se refiere a una función o algoritmo para generar claves que representen de manera casi unívoca a un documento, registro, archivo o mensaje de datos, en forma de un Resumen Hash.
- **HSM:** Hardware Security Module - Módulo de seguridad de hardware.
- **IETF:** Internet Engineering Task Force. Organización Internacional de normalización de ingeniería de Internet, mediante estándares conocidos como RFC.
- **IETF RFC 3161:** Public Key Infrastructure Time-Stamp Protocol (TSP). Protocolo de Sellado de Tiempo (TSP) basado en PKI.
- **IETF RFC 3628:** Policy Requirements for Time Stamping Authorities. Requerimientos de Políticas para Autoridades de Sellado de Tiempo (TSA).
- **INDECOPI** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- **OCSP:** Online Certificate Status Protocol. Este protocolo permite comprobar en línea la validez de un certificado digital.
- **OID:** Object identifier - Identificador de objeto único.
- **TOC PERU SAC** Oficina Nacional de Procesos Electorales.
- **PKCS:** Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
- **PKI:** Public Key Infrastructure - Infraestructura de Clave Pública.
- **PKIX:** Grupo de trabajo del IETF (Public Key Infrastructure X509 IETF Working Group) constituido con el objeto de desarrollar las especificaciones relacionadas a PKI e Internet.
- **RFC:** Request For Comments (estándares y recomendaciones emitidos por la IETF).
- **RUC** Registro Único de Contribuyentes.
- **SVA** Prestador de Servicios de Valor Añadido.
- **TSA:** Time Stamping Authority. Autoridad de Sellado de Tiempo de la TOC PERU SAC.
- **TS:** Time Stamping Service. Servicio de Sellado de Tiempo.
- **TSQ:** Time Stamping Query. Solicitud de Sellado de Tiempo.



- **TSR:** Time Stamping Response. Respuesta de Sellado de Tiempo.
- **TSU:** Time Stamping Unit. Unidad de Sellado de Tiempo, comprendida por hardware y software que es gestionado como una unidad y tiene una única clave de firma de Sellos Digitales de Tiempo activa a la vez.
- **TST:** Time Stamping Token. Sello Digital de Tiempo.
- **UTC:** Coordinated Universal Time. Escala de tiempo basada en el segundo, recomendada por la ITU Radiocommunication Sector (ITU-R).

#### 4. CONCEPTOS GENERALES

##### 4.1. Servicios de sellado de tiempo

El Servicio de Sellado de Tiempo de la TSA-TOC PERU SAC, se basa en los siguientes componentes:

- Generación de Sellos Digitales de Tiempo (TST), en base a una Fuente Confiable y Redundante de Tiempo stratum 1 a través del protocolo de comunicaciones NTP, utilizando para el efecto la firma correspondiente a un certificado digital de la TSA.
- Gestión del Servicio de Sellado de tiempo (TS), encargado de ofrecer este servicio vía Intranet o Internet (de ser aplicable) a sus suscriptores y usuarios, que confían en estos Sellos Digitales de Tiempo.

##### 4.2. Autoridad de sellado de tiempo

La empresa TOC PERU SAC, como Autoridad de Sellado de Tiempo (TSA-TOC PERU SAC), es el tercero de confianza para los suscriptores y usuarios, quienes utilizan el servicio de Sellado de Tiempo (TS), de conformidad con los términos del presente documento.

La TSA realiza la emisión de Sellos Digitales de Tiempo (TST), solicitados por los suscriptores de ese servicio; además, realiza la administración y control de la infraestructura de los servicios de sellado de tiempo, que se describen en el presente documento.

Los TST son firmados digitalmente por la TSA-TOC PERU SAC, utilizando un certificado digital y su correspondiente clave privada, que se encuentran custodiados por la TSA-TOC PERU SAC en un entorno físico seguro.

##### 4.3. Solicitante, Suscriptor y usuario

A los efectos del presente documento, se entenderá por solicitante a la entidad que solicita convertirse en suscriptor del Servicio del Sellado de Tiempo (TS) por parte de la TSA-TOC PERU SAC.

El suscriptor será la entidad que solicita la emisión de Sellos Digitales de Tiempo (TST) para determinadas transacciones. Los suscriptores deberán ajustarse a lo señalado en el presente documento y al Acuerdo de Prestación de Servicios de Sellado de Tiempo suscrito con la TSA-TOC PERU SAC, cuando sea aplicable. Los suscriptores deberán ajustarse a los procedimientos



establecidos para la petición de cada Sello Digital de Tiempo (TST), y cumplir los requisitos que se establezcan en el presente documento.

El usuario, también conocido como la parte que confía, es a la persona natural, jurídica, funcionario público, entidad, equipo, servicio o cualquier otro ente que voluntariamente confía y hace uso de los Sellos Digitales de Tiempo (TST) previamente emitidos por la TSA a solicitud de un determinado suscriptor. Cuando el usuario decida voluntariamente confiar y hacer uso de los Sellos Digitales de Tiempo le será de aplicación el presente documento.

#### 4.4. Política de Sellado de Tiempo y Declaración de Prácticas de la TSA

##### 4.4.1. Propósito

La Política de Sellado de Tiempo y la Declaración de Prácticas de la TSA-TOC PERU SAC (VAPS), quedan definidas de la siguiente manera:

- La Política de Sellado de Tiempo determina a qué se adhiere la TSA-TOC PERU SAC. Se incluye aquí las reglas y procesos aplicados por la TSA-TOC PERU SAC para generar un sello de tiempo y mantener la precisión de su reloj.
- La Declaración de Prácticas de la TSA-TOC PERU SAC es una declaración de cómo se implementa el servicio de sellado de tiempo para cumplir con los requisitos de la Política de Sellado de Tiempo.

##### 4.4.1.2 Organigrama de la TSA

## 70E ORGANIGRAMA TSA



##### 4.4.2. Nivel de especificidad





El presente documento especifica los procesos usados para brindar los servicios de sellado de tiempo.

La TSA-TOC PERU SAC se apoya en algunos procesos desarrollados por la TOC PERU SAC. Debido a ello el presente documento referencia documentos normativos de dichos procesos.

La Política de la TSA-TOC PERU SAC especifica los lineamientos usados para brindar los servicios de sellado de tiempo, mientras que la Declaración de Prácticas de la TSA-TOC PERU SAC implementa las reglas establecidas por la Política de sellado de tiempo. Las políticas y declaraciones se encuentran integradas en el presente documento.

#### 4.4.3. Enfoque

El presente documento muestra por un lado la Política de Sellado de Tiempo a la que se adhiere la TSA-TOC PERU SAC enfocándose en procesos generales en conformidad con el RFC 3628, “Policy Requirements for Time-Stamping Authorities (TSAs)” de la IETF. Asimismo, presenta la Declaración de Prácticas de la TSA denotando la forma en que dicha política se implementa. Forman parte de dicha declaración detalles técnicos propios de la TSA-TOC PERU SAC tales como los referidos a aspectos organizacionales, procedimientos operativos, instalaciones físicas y entorno de tecnologías de la información.

Determinados detalles técnicos pueden encontrarse en documentos internos que no se encuentran disponibles al público.

## 5. POLÍTICAS DE SELLADO DE TIEMPO

### 5.1. Visión general

La información que se almacena en los Sellos Digitales de Tiempo se encuentra firmada digitalmente, utilizando un certificado digital de la TSA-TOC PERU SAC y su respectiva clave privada, los cual se encuentra bajo las condiciones de seguridad provistas por un módulo de seguridad de hardware (HSM).

El certificado digital de la TSA-TOC PERU SAC, así como su correspondiente autoridad certificadora raíz, serán publicados a través del portal de la TOC PERU SAC, para que sean descargados y utilizados por los suscriptores y usuarios del servicio para validar los TST.

Las claves de la TSA-TOC PERU SAC se mantienen depositadas y custodiadas en un entorno de hardware seguro (HSM). El acceso a esas claves sólo se permite a personas debidamente autorizadas por la TSA-TOC PERU SAC.

El Certificado Digital de la TSA-TOC PERU SAC asignado para el Servicio de Sellado de Tiempo en la firma de Sellos Digitales de Tiempo se encuentra en concordancia con las recomendaciones en ETSI TS 101 861 y ETSI TS 102 176-1.

El Certificado Digital de Sellado de Tiempo sirve para firmar digitalmente estampas o sellos de tiempo de acuerdo a los límites de uso impuestos, permite identificar a la TSA-TOC PERU SAC,

quien será responsable de lo que firme dentro del ámbito de su actividad y límites de uso que correspondan.

El perfil del certificado digital de la TSA se ajusta a lo especificado en RFC 3161, ETSI TS 101 861 y ETSI TS 102 176-1, y se define con los campos detallados en la Tabla 1.

Tabla 1. Perfil del certificado de la TSA

Nombre del campo	Contenido
Versión	v3
Número de Serie	4454963382380791558
Algoritmo de Firma	SHA-256 con cifrado RSA
Emisor DN	CN: TOC PERU RAIZ G1
	O: TOC PERU SAC
	SerialNumber: 20547367112
	L: Lima ST: Lima C: PE
Validez	Válido desde: 12 de Julio 2018
	Válido hasta: 12 de Julio 2038
Sujeto (DN)	CN: TOC PERU TSA G1
	O: TOC PERU SAC
	L: Lima ST: Lima C: Peru
	SerialNumber: 20547367112
Longitud de la clave	2048 bits
Uso de la clave	Key Cert Sign, CRL Sign
CRL Distribution Points	<a href="http://firma.toc.pe/root_toc_pe.crl">http://firma.toc.pe/root_toc_pe.crl</a>

Tabla 2. Perfil del certificado de la TSU

Nombre del campo	Contenido
Versión	v3
Número de Serie	2039004160783142080
Algoritmo de Firma	SHA-256 con cifrado RSA
Emisor DN	CN: TOC PERU TSA G1

	O: TOC PERU SAC L: Lima ST: Lima C: Peru
Validez	Válido desde: 23 de Octubre 2018
	Válido hasta: 22 de Octubre 2028
Sujeto (DN)	CN=Unidad de Sellado de Tiempo TOC PERU SAC - TSU_4
	c=PE st=Lima l=Lima o=TOC PERU SAC ou=PSC DE SELLADO DE TIEMPO serialNumber=20547367112 email=soportepki@toc.pe
	SerialNumber: 20547367112
Longitud de la clave	2048 bits
Uso de la clave	Firma Digital
Uso extendido de la clave	Sello de Tiempo (id-kp-timeStamping) 1.3.6.1.5.5.7.3.8 Critico
CRL Distribution Points	<a href="http://firma.toc.pe/TSA_peru_toc_g1.crl">http://firma.toc.pe/TSA_peru_toc_g1.crl</a>

## 5.2. Identificación

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)

El identificador de la Política de Sellado de Tiempo, que forma parte del presente documento, es incluido en cada sello de tiempo emitido por la TSA-TOC PERU SAC.

## 5.3. Comunidad de usuarios y aplicabilidad



La comunidad de usuarios está conformada por personas naturales, jurídicas, funcionarios públicos, entidades, equipos, servicios o cualquier otro ente que voluntariamente confía y hace uso de los Sellos Digitales de Tiempo (TST) previamente emitidos por la TSA-TOC PERU SAC a solicitud de un determinado suscriptor.

El Sello Digital de Tiempo es multipropósito, así tenemos, como ejemplos: todo tipo de transacciones electrónicas, documentos electrónicos, mensajes de datos, sistemas de registro de entrada o salida de datos, complemento a la firma digital, etc.

#### 5.4. Conformidad

El identificador de la Política de Sellado de Tiempo, que forma parte del presente documento, es incluido en cada sello de tiempo emitido por la TSA-TOC PERU SAC.

La TSA-TOC PERU SAC, para su acreditación en el marco de la IOFE, se somete a la evaluación de la Autoridad Administrativa Competente. En dicha evaluación la TSA-TOC PERU SAC demuestra el cumplimiento de sus obligaciones descritas en la sección 6.1 del presente documento y que ha implementado controles que cumplen con los requisitos especificados en su sección 7.

## 6. OBLIGACIONES Y RESPONSABILIDADES

### 6.1. Obligaciones de la TSA

#### 6.1.1. Generalidades

La TSA-TOC PERU SAC, como Autoridad de Sellado de Tiempo, está obligada a:

- Aprobar o negar las solicitudes de Servicio de Sellado de Tiempo, de acuerdo con lo establecido en el presente documento.
- Custodiar por medios seguros la información y documentación relativa a la Declaración de Prácticas vigente, al menos durante 10 años contados desde el momento de su expedición. A estos efectos, la TSA almacena en formato digital las versiones de la Declaración de Prácticas publicada y copia del Acuerdo de Prestación de Servicios de Sellado de Tiempo entre la TOC PERU SAC y el suscriptor, cuando este aplique.
- Emitir Sellos Digitales de Tiempo cuyo contenido mínimo sea el definido en el presente documento y, cuando aplique, en los Acuerdos de Prestación de Servicios de Sellado de Tiempo entre la TOC PERU SAC.
- Emitir Sellos Digitales de Tiempo según la información que obra en su poder y libres de errores en el TSR.
- Facilitar el acceso a la versión vigente del presente documento.
- Brindar el acceso a la cadena de confianza del certificado digital raíz de la TSA que sirvió para emitir los Sellos Digitales de Tiempo.
- Brindar la exactitud del tiempo mediante la sincronización con una Fuente Confiable y Redundante de Tiempo de acuerdo a la escala "Coordinated Universal Time (UTC)", excluyendo



incidentes o eventos que sean atribuibles a fallas generalizadas por parte de la fuente de tiempo.

- Brindar los Sellos Digitales de Tiempo durante la validez del certificado digital de la TSA utilizado en el momento de su generación.
- Emitir Sellos Digitales de Tiempo cuyas horas y fechas se mantengan dentro del margen de precisión de un segundo, o de lo contrario dentro de los márgenes de precisión establecidos en el Acuerdo de Prestación de Servicios de Sellado de Tiempo, cuando aplique el uso de este documento.
- Generar y emitir Sellos Digitales de Tiempo (TST) conforme a esta Declaración de Prácticas, y a los estándares internacionales de aplicación.
- Implementar y mantener los requerimientos de seguridad impuestos a la clave privada de la TSA, de acuerdo a lo indicado en el presente documento.
- Informar sobre las modificaciones del presente documento.
- Mantener sus propias claves privadas bajo su exclusivo control empleando sistemas y componentes fiables para almacenarlas de guardando su confidencialidad y que éstas sean inaccesibles a personas no autorizadas, evitando su pérdida o divulgación.
- Ofrecer y mantener la infraestructura tecnológica necesaria para los servicios de Sellado de Tiempo, así como los controles de seguridad física, de procedimiento y personal necesarios para la práctica de la actividad de emisión de Sellos Digitales de Tiempo.
- Proporcionar al solicitante del Servicio de Sellado de Tiempo (TS) la información mínima necesaria para el uso de los Sellos Digitales de Tiempo (TST).

#### 6.1.2. Obligaciones de la TSA con los suscriptores

La TSA-TOC PERU SAC garantiza que Sellos Digitales de Tiempo son emitidos en concordancia con lo siguiente:

- Cumplir con las obligaciones establecidas por la normativa vigente, la Ley de Firmas y Certificados Digitales (Ley 27269) y su modificatoria (Ley 27310), el Reglamento de la Ley de Firmas y Certificados Digitales, D.S. Nº 052-2008-PCM, la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, Versión 3.3, INDECOPI.
- Proteger su información contra pérdidas, destrucción y falsificaciones.
- La exactitud de la fecha y hora incorporada en los sellos de tiempo basados en el sistema UTC.
- La TSA-TOC PERU SAC, para su acreditación en el marco de la IOFE, se somete a la evaluación y auditorías periódicas de la Autoridad Administrativa Competente.
- La TSA – TOC PERU SAC brinda disponibilidad del Servicio de Sellado de Tiempo, excluyendo el tiempo que haya sido notificado a los suscriptores y usuarios para realizar tareas de mantenimiento preventivo o actualizaciones del sistema y los tiempos de no disponibilidad que sean atribuibles a casos fortuitos o de fuerza mayor.

#### 6.2. Obligaciones de los solicitantes y suscriptores

Los solicitantes del Servicio del Sellado de Tiempo (TS) están obligados a lo siguiente:

- Abonar las tasas o brindar las contraprestaciones que correspondan en virtud de los servicios de Sellado de Tiempo (TS), cuando esto sea de aplicación.
- Señalar la dirección IP desde la cual solicitará la generación de sellos digitales de tiempo por parte del servicio de Sellado de Tiempo.
- Presentar credenciales de autenticación apropiadas y legítimas cuando sean requeridas para consumir el servicio de Sellado de Tiempo.



- Solicitar el Servicio de Sellado de Tiempo (TS) según se estipula en los términos y condiciones que se establezcan en el presente documento y, si aplica, en el Acuerdo de Prestación de Servicios de Sellado de Tiempo suscrito con la TOC PERU SAC.

Los suscriptores del Servicio del Sellado de Tiempo (TS) están obligados a lo siguiente:

- Aceptar como válidos los datos incorporados en el Sello Digital de Tiempo (TST).
- Cumplir en todo momento con las normas y regulaciones indicadas en el presente documento.
- Verificar, a través de la conexión OCSP o de la Lista de Certificados Revocados (CRL), que la TOC PERU SAC ponga a disposición, el estado del Certificado de la TSA, en el momento de firmar los Sellos Digitales de Tiempo, es decir, verificar que los Sellos Digitales de Tiempo (TST) se encuentren firmados correctamente y que la clave privada usada para la firma del TST no se encuentre revocada o comprometida. En el supuesto de que los Suscriptores no verificaran las firmas a través del OCSP o la CRL, la TSA no se hace responsable del uso y confianza depositada por parte de los Suscriptores en estos Sellos Digitales de Tiempo (TST).
- Verificar, que los Sellos Digitales de Tiempo (TST) han sido correctamente emitidos por la TSA.

### 6.3. Obligaciones de los terceros que confían

Los usuarios o terceros que confían están obligados a verificar, a través de la conexión OCSP o de la Lista de Certificados Revocados (CRL) que ponga a disposición la TOC PERU SAC, el estado del Certificado de la TSA, en el momento de verificar los Sellos Digitales de Tiempo, es decir, verificar que los Sellos Digitales de Tiempo (TST) se encuentren firmados correctamente y que la clave privada usada para la firma del Sello Digital de Tiempo (TST) no se encuentre revocada o expirada. En el supuesto de que los usuarios no verificaran el certificado de la TSA a través del OCSP o la CRL, la TSA no se hace responsable del uso y confianza que los usuarios hagan de estos Sellos Digitales de Tiempo (TST).

### 6.4. Responsabilidades

#### 6.4.1. Responsabilidades de la TSA

Las responsabilidades de la TSA-TOC PERU SAC son las siguientes:

- Velar por el cumplimiento de las responsabilidades y obligaciones descritas en el presente documento así como en la normativa vigente.
- La TSA, única y exclusivamente, responderá por los daños y perjuicios causados, por incumplimiento de sus obligaciones legales derivadas de la legislación vigente.
- La TSA no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente Declaración de Prácticas si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la TSA no pueda tener un control razonable.
- La TSA no será responsable de la utilización negligente o dolosa de los Sellos Digitales de Tiempo (TST).
- La TSA no será responsable de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del solicitante, suscriptor y/o usuario.

- La TSA no será responsable de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los Sellos Digitales de Tiempo (TST) emitidos en favor de un determinado suscriptor.
- La TSA no será responsable del contenido de aquellos documentos electrónicos (mensaje de datos) para los cuales se hayan solicitado Sellos Digitales de Tiempo (TST). La TSA no será responsable en ningún caso por los daños causados por el empleo de sus servicios de Sellado de Tiempo (TS).

#### 6.4.2. Responsabilidades del Suscriptor

Las responsabilidades del Suscriptor son las siguientes:

- El Suscriptor deberá tomar todas las precauciones y medidas conducentes para efectuar el requerimiento del Servicio de Sellado de Tiempo (TS), en particular pero no exclusivamente, deberá solicitar el Sellado de Tiempo de un mensaje de datos considerando que el término de fijación de cada Sellado de Tiempo a un mensaje de datos determinado, dependerá de las condiciones de calidad, agilidad y seguridad de los medios y servicios de telecomunicación dispuestos por el suscriptor para efectuar el requerimiento del Servicio de Sellado de Tiempo a la TSA-TOC PERU SAC y recibir la respuesta correspondiente.
- La TSA-TOC PERU SAC advierte que dependiendo de las anteriores condiciones, podrá existir un término de diferencia entre el momento en que es realizada la Solicitud de Sellado de Tiempo (TSQ) y la realización efectiva del mismo. El suscriptor deberá considerar esta posible diferencia de tiempo, para efectos de la utilización del servicio. La TSA-TOC PERU SAC no será responsable por cualquier consecuencia que se derive de la diferencia de tiempo entre el momento de la Solicitud de Sellado de Tiempo (TSQ) y el momento efectivo de la realización del Sellado de Tiempo.
- El suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en el presente documento.
- El suscriptor será responsable del cumplimiento de todas aquellas obligaciones impuestas en el presente documento, y por la normativa vigente en materia de prestación de servicios de Sellado de Tiempo (TS).
- El suscriptor se compromete a indemnizar a la TOC PERU SAC los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposa o dolosa por su parte, asumiendo igualmente los costos procesales en los que la TSA-TOC PERU SAC pudiera incurrir por esta causa.
- El suscriptor indemnizará y mantendrá indemne a la TOC PERU SAC por cualquier daño que esta pudiera sufrir por el cumplimiento total, parcial o defectuoso de las obligaciones asumidas y en base a toda reclamación dirigida contra ella por cualquier tercero con el que el suscriptor hubiera contratado.

#### 6.4.3. Responsabilidades del Usuario

Las responsabilidades del Usuario son las siguientes:

- El usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en el presente documento.
- El usuario será responsable del cumplimiento de todas aquellas obligaciones impuestas en el presente documento, y por la normativa vigente en materia de prestación de servicios de Sellado de Tiempo.
- En todo caso, el usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Sello Digital de Tiempo (TST), sin haber observado las obligaciones recogidas



en el presente documento, garantizando la plena indemnidad de la TSA-TOC PERU SAC por dicho concepto.

#### 6.4.4. **Responsabilidades de los terceros que confían**

- Verificar que el sello de tiempo ha sido correctamente firmado, y que la clave privada utilizada para firmar el sello de tiempo no debe haber sido comprometida hasta el momento de la verificación.
- Tomar en cuenta cualquier limitación en el uso de los sellos de tiempo considerados en la Política de Sellado de Tiempo o en la DPSVA
- Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte

### 7. **LIMITACIONES DE RESPONSABILIDAD, POLITICAS DE REEMBOLSO E INDEMNIZACIONES**

- TOC PERU SAC no se hace responsable de la veracidad ni del contenido de los datos sellados por la TSA-TOC PERU SAC.
- Bajo ninguna circunstancia, TOC PERU SAC será responsable por cualquier pérdida, daños indirectos o consecuentes, o por pérdida de datos por la utilización de un software no confiable
- Límite de responsabilidad en caso de pérdida por transacciones y responsabilidad financiera, a TSA no se responsabilizará en caso de las pérdidas por transacciones ni asume ningún tipo de responsabilidad financiera.
- Políticas de reembolso por los servicios los servicios serán definidas en los contratos de titulares.
- Respecto a las indemnizaciones, sin estipular. Podrán establecerse acuerdos particulares que se negociarán individualmente en el contrato en relación a errores u omisiones referentes a la TSA.

### 8. **REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA**

La TSA-TOC PERU SAC brinda sus servicios de sellado de tiempo en concordancia con las reglas establecidas en el presente documento, y en documentos adicionales de carácter interno que definen requisitos técnicos, operativos y procedimentales que sean aplicables a dichos servicios.

#### 8.1. **Declaración de Prácticas y Declaración de Libre Divulgación de la TSA**

##### 8.1.1. **Declaración de Prácticas de la TSA**

Los procedimientos definidos y su correcta implementación por la TSA-TOC PERU SAC son evaluados bajo un proceso de acreditación seguido ante la AAC en el marco de la IOFE conforme a su rol definido en el Reglamento.

Esta Declaración de Prácticas de TSA y cualquier otra información relevante será publicada en <https://firma.toc.pe>.

La Declaración de Libre Divulgación de la TSA (en inglés TSA Disclosure Statement) se incluye en el ítem 7.1.2 del presente documento. Los documentos de tipo interno no serán publicados.





La TSA-TOC PERU SAC brinda la confiabilidad necesaria en la provisión de servicios de sellado de tiempo conforme a lo siguiente:

- a) La TSA-TOC PERU SAC ha desarrollado un análisis de riesgos por el cual se identifican sus activos y las amenazas a dichos activos determinando los controles de seguridad necesarios para mitigar dichos riesgos y los procedimientos operativos correspondientes.
- b) El presente documento contiene la política de sellado de tiempo y el desarrollo de la implementación de sus requisitos mediante la declaración de las prácticas de sellado de tiempo y otros procedimientos relacionados.
- c) Los servicios de la TSA-TOC PERU SAC serán soportados internamente por el propio TOC PERU SAC. En caso de que se recurra a terceros para la prestación de los mismos en el futuro, ello se divulgará a suscriptores y terceros que confían. Esto significa:
  - i. Controlar obligaciones y cumplimiento del proveedor servicios de TSU (empresa AGILE)
  - ii. Controlar obligaciones y cumplimiento de proveedores servicios de TOC.
- d) La TSA-TOC PERU SAC pone a disponibilidad de los suscriptores y partes que confían su Declaración de Prácticas y Política de Sellado de Tiempo, y otra documentación relevante en su repositorio, disponible en <https://firma.toc.pe>
- e) La TSA-TOC PERU SAC divulgará a todos los suscriptores y potenciales terceros que confían los términos y condiciones de uso de sus servicios de sellado de tiempo según se encuentran especificados en la sección 7.1.2.
- f) La TSA-TOC PERU SAC vela porque las prácticas de TSA declaradas se encuentren adecuadamente implementadas.
- g) La TSA-TOC PERU SAC tiene definido un proceso de revisión para sus prácticas incluyéndose responsabilidades definidas para el mantenimiento de la Declaración de Prácticas de la TSA, encontrándose el mismo especificado en la sección 6.4.

#### 8.1.2. Declaración de Libre Divulgación de la TSA

La TSA-TOC PERU SAC divulga a todos sus suscriptores y potenciales terceros que confían los términos y condiciones de uso en relación a los servicios de sellado de tiempo prestados bajo la política de sellado de tiempo especificada en el presente documento y particularmente bajo su presente sección como su Declaración de Libre Divulgación de la TSA.

En particular se refiere:

- a) Las consultas relacionadas con la presente VAPS podrán ser dirigidas al correo electrónico [contacto@toc.pe](mailto:contacto@toc.pe), o a los datos de contactos indicados en la sección 7.5 Aspectos organizacionales.
- b) La política de sellado de tiempo aplicable a los servicios de la TSA-TOC PERU SAC es la especificada en el presente documento.



- c) El algoritmo de hash utilizado para representar los datos a los que se aplica el sello de tiempo es SHA-256.
- d) La precisión del tiempo en los tokens de sellado de tiempo emitidos por la TSA-TOC PERU SAC guarda conformidad con los estándares establecidos de precisión mínima respecto al UTC de  $\pm 1$  segundo.
- e) El uso del servicio de sellado de tiempo puede limitarse a los suscriptores de un certificado digital válido en la IOFE.
- f) Las obligaciones del suscriptor están definidas en la sección 6.2 del presente documento.
- g) Las obligaciones del tercero que confía se encuentran definidas en la sección 6.3 del presente documento.
- h) La información sobre cómo verificar el sellado de tiempo de tal manera que el tercero que confía pueda considerarse que “confía razonablemente” en el mismo, se detalla en la sección 6.3 del presente documento.
- i) El periodo de tiempo durante el cual se guarda registro de los eventos de la TSA es de 10 años.
- j) La TSA-TOC PERU SAC como SVA puede obligar a los suscriptores y terceros que confían a cumplir con acuerdos de uso adicionales siempre que los mismos se encuentren bajo el marco de lo previsto en la Ley de Firmas y Certificados Digitales, su Reglamento y normas complementarias y modificatorias.
- k) El servicio de sellado de tiempo de la TSA-TOC PERU SAC se prestará bajo el marco de las leyes del Perú.
- l) El cumplimiento de la TSA-TOC PERU SAC respecto de la normatividad y regulaciones que le son aplicables es verificada por la AAC de la IOFE en conformidad con el Reglamento y la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA.

## 8.2. Ciclo de vida de la gestión de las claves

### 8.2.1. Generación de las claves de la TSA

Los datos de creación de las claves privadas de firma digital de la TSA se generan en un ambiente de seguridad, directamente controlado por el personal especializado de la TOC PERU SAC.

### 8.2.2. Protección de las claves privadas de la TSU

Las claves privadas de firma de la TSA se encuentran con un adecuado nivel de protección y seguridad para de esta manera garantizar la integridad de los Sellos Digitales de Tiempo (TST) generados; es por ello, que el servidor de Sellado de Tiempo tiene incorporado un módulo de seguridad de hardware (HSM) que cumple con el estándar FIPS 140-2 nivel 3 y es utilizado para generar, almacenar y usar las claves privadas de la TSA.

### 8.2.3. Distribución de las claves públicas de la TSU



Los certificados digitales de la TSA con su clave pública son de acceso público, sin restricción alguna. Y serán publicados en <https://firma.toc.cl/indexpki.php>

#### 8.2.4. **Regeneración de claves de la TSU**

Cada clave privada de la TSA será reemplazada por una nueva antes que finalice el periodo de validez de su correspondiente certificado digital, cuando se encuentre próximo a concluir dicho periodo, en caso de un compromiso de la misma, o por debilidades descubiertas en su algoritmo o longitud.

#### 8.2.5. **Fin del ciclo de vida de las claves de la TSU**

El Sello Digital de Tiempo firmado por la TSA, se realizará en plena vigencia del certificado digital de la TSA. El sistema de generación de los sellos de tiempo rechazará cualquier intento de emitir el sello si la clave privada de firma de la TSA ha expirado, ha sido revocada o se encuentra comprometida. Para la destrucción de las claves antiguas y la generación de otras nuevas se seguirán las instrucciones propias del módulo de seguridad de hardware (HSM).

#### 8.2.6. **Gestión del ciclo de vida del módulo criptográfico usado para la firma de sellos de tiempo**

Los HSM se operan por personal interno de la TOC PERU SAC con roles autorizados para su inicialización y puesta en marcha dentro de las dependencias internas seguras, con los controles de seguridad física adecuados, siendo desde este momento todas las manipulaciones registradas y auditadas.

En caso de cambio de HSM por cualquier motivo, las claves son borradas y destruidas, de acuerdo a los procedimientos técnicos indicados por el fabricante.

### 8.3. **Sellado de tiempo**

#### 8.3.1. **Sello digital de Tiempo (TST)**

Los TST emitidos por la TSA-TOC PERU SAC tienen la siguiente estructura básica:

<b>ESTRUCTURA BÁSICA DEL SELLO DIGITAL DE TIEMPO</b>
Identidad de la TOC PERU SAC - Autoridad de Sellado de Tiempo (TSA)
Resumen HASH
OID de Política de Sellado de Tiempo: OID: 1.3.6.1.4.1.47911.1.1.1
Fecha y Hora (UTC)
Número de serie
Firma digital de la TSA



Todos los TST emitidos por la TSA-TOC PERU SAC incluyen un identificador único y un identificador OID correspondiente a esta Declaración de Prácticas a la que se someten.

Cada TST incluye el certificado del TSU que lo generó, permitiendo determinar la identificación o ID de la máquina selladora o TSU.

Cada TST incorpora la fecha y hora UTC, momento en que el servidor de Sellado de Tiempo lo generó, en base a una fuente confiable de tiempo, mediante acceso a Internet a través del protocolo NTP.

### 8.3.2. Sincronización del reloj

La administración del Servicio de Sellado de Tiempo vela para el reloj usado para el Sello Digital de Tiempo se encuentre correctamente sincronizado con UTC. En caso de que el reloj usado presente imprecisiones no se realizará la emisión del Sello Digital de Tiempo.

Como Fuente Confiable de Tiempo, se toma como referencia de tiempo la hora facilitada por el SHOA de Chile, el mismo que distribuye el tiempo a través del protocolo NTP.

El Perú se encuentra en la zona horaria UTC-5 y los sellos de tiempo se emiten teniendo en cuenta este parámetro.

Los valores de la fecha y hora no tienen en cuenta ni aplican en ningún caso los valores que el sistema informático del suscriptor del Servicio de Sellado de Tiempo señale. Tampoco el suscriptor, ni terceras personas, pueden cambiar o solicitar la aplicación de información distinta de fecha y hora.

Al contar con una fuente confiable de tiempo, el Sello Digital de Tiempo (TST), constituye prueba inequívoca del instante de tiempo en que un documento electrónico (mensaje de datos) es creado, enviado o recibido.

La TSA no reconoce la localización geográfica ni la zona de tiempo en que se encuentre el suscriptor al momento de solicitar el Servicio de Sellado de Tiempo, en todos los casos se registrarán la fecha y hora bajo UTC, de acuerdo a lo declarado en el presente documento.

## 8.4. Gestión y operación de la TSA

### 8.4.1. Gestión de la seguridad

Los elementos relacionados a la seguridad de la información en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.



#### **8.4.2 Información confidencial y/o privada**

Es de obligatorio cumplimiento para todos los empleados y proveedores de TOC PERU S.A.C que tienen relación con los servicios de sellado de tiempo dar cumplimiento a las POLÍTICA DE PRIVACIDAD TOC PERU S.A.C, o sus proveedores, no recogen información personal de los usuarios (personas naturales) de los servicios de sellado de tiempo, ya que estas transacciones no implican firma digital del usuario final.

TOC PERU SAC como Autoridad emisora de sellos de tiempo, cumple los requerimientos establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales -Ley27269 y exige a CAMERFIRMA el cumplimiento de la certificación ISO 27001.

#### **8.4.3 Gestión y clasificación de activos**

Los elementos relacionados a la gestión y clasificación de activos en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.

#### **8.4.4 Seguridad del personal**

Los elementos relacionados a la seguridad relacionada a los recursos humanos en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.

La TSA-TOC PERU SAC asigna roles de confianza a su personal para el manejo de su información sensible.

#### **8.4.5 Seguridad física y del entorno**

Los elementos relacionados a la seguridad física y ambiental de las instalaciones en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.

#### **8.4.6 Gestión de operaciones**

Los elementos relacionados a la seguridad de operaciones en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.

Para la operación de equipos de seguridad de manejo de claves privadas y de información sensible se cuenta con los procedimientos respectivos.

#### **8.4.7 Gestión de acceso a los sistemas**

Los elementos relacionados a la gestión de accesos en la TOC PERU SAC se encuentran en la "Política de Seguridad de la Información" de la TOC PERU SAC, los cuales se extienden al servicio de sellado de tiempo.

El acceso a los sistemas está limitado solo al personal autorizado, de acuerdo a los roles asignados.

#### **8.4.8 Mantenimiento y despliegue de sistemas confiables**

Tal como se indica en el numeral 7.2 "Ciclo de vida de la gestión de las claves", se realiza el control de la gestión del ciclo de vida de las claves privadas de la TSA.

Adicionalmente, las modificaciones y actualizaciones de los sistemas confiables son realizadas en entornos seguros, por personal autorizado, generándose la documentación que permite realizar el control de los cambios.

#### **8.4.9 Compromiso de los servicios de la TSA**

En el caso de los acontecimientos que afecten a la seguridad de los servicios de la TSA, incluyendo el compromiso de las claves de firma privada de TSU o la pérdida detectada de calibración, la TSA-TOC PERU SAC facilitará información relevante a los suscriptores y a las partes que confían. La información incluirá la naturaleza del compromiso, y las herramientas o sistemas necesarios para la comprobación de sus sellos de tiempo, garantizando la identificación de los elementos comprometidos. (Referirse al Procedimiento Compromiso de clave privada firma TSU). Respecto a eventos de contingencias o interrupción de servicios existen procedimientos establecidos que entregan las directrices para enfrentar este tipo de situaciones (refiérase a DRP y BCP).

Respecto a estas situaciones, la TSA de TOC PERU SAC ha:

Desarrollado un Plan de continuidad operacional, el cual incluye los escenarios de compromiso de llave, pérdida de la precisión declarada del reloj de la TSA o falla de componentes que afecten directamente la operación del sitio principal de la TSA. Para estos escenarios TOC ha definido un plan que permite la recuperación de servicios frente a estos eventos. Dichos escenarios son probados periódicamente a fin de probar la eficacia y eficiencia del plan e incorporar mejoras producto de la misma ejecución de estos escenarios.

Ante los eventos antes mencionados, la TSA de TOC no emitirá nuevos TST hasta superar el compromiso declarado. Ante pérdida de la precisión, compromiso del mismo o sospecha de compromiso en el tiempo de la TSA; TOC dejará esta información a los suscriptores y terceros que confían indicando la descripción del evento. Esta comunicación será directa o a través de su sitio web. En caso de comprometerse ya sea la llave o la precisión declarada, se informará a los suscriptores y terceros que confían de aquella información que permite detectar los sellos de tiempo afectados, a menos que esta información vulnere su política de privacidad de datos

personales - disponible en su sitio web - de sus usuarios o la seguridad del servicio de la TSA de TOC.

Ver Doc.: Plan de Recuperación de Desastres (DRP-BCP)

Ver Doc.: Plan de Continuidad Operacional.

#### **8.4.10 Extinción de la TSA**

A fin de causar el menor impacto posible, tanto a los suscriptores como a los usuarios del sistema de Sellado de Tiempo, ante un hipotético cese de actividad de la TSA de la TOC PERU SAC, ésta realizará las gestiones necesarias para transferir, con el consentimiento expreso de los suscriptores (cuando se requiera), la gestión del Sellado de Tiempo a otro prestador de servicios de Sellado de Tiempo, que los asuma o, en caso contrario, extinguir la validez de todos los sellos de tiempo emitidos. Para la consecución de este objetivo se establecen las siguientes medidas:

Establecer, cuando ello fuera posible, un acuerdo con otro prestador del Servicio de Sellado de Tiempo con el propósito de transmitir todas las obligaciones y derechos a este último con la intención de continuar proveyendo el servicio. Si se produce la subrogación, esta Declaración de Prácticas seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito. Además, ante este evento se comunicará con una antelación mínima de tres meses el cese de la actividad, informando al mismo tiempo sobre las características del prestador de Servicios de Sellado de Tiempo al que se propone la transferencia de la gestión del servicio.

Recabar el consentimiento expreso de los suscriptores (cuando se requiera) que tengan en ese momento sellos de tiempo aún vigentes para proceder a la transferencia de la gestión del Servicio de Sellado de Tiempo (TS).

Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, a la revocación del certificado digital de la TSA una vez transcurrido el plazo de dos meses desde la comunicación.

Informar a los órganos internos competentes, con la antelación indicada, el cese de la actividad y el destino que se vaya a dar a los sellos de tiempo aún válidos, especificando en su caso si se va a transferir la gestión y a quien.

Con carácter previo al cese definitivo de la actividad, se comunicará a los órganos competentes la información relativa a los sellos de tiempo emitidos cuya vigencia será extinguida.

Cumplir con las obligaciones que estén impuestas por la ley.

#### **8.4.11 Cumplimiento de requisitos legales**



La TSA-TOC PERU SAC cumple con las obligaciones establecidas por la normativa vigente, la Ley de Firmas y Certificados Digitales (Ley 27269) y su modificatoria (Ley 27310), el Reglamento de la Ley de Firmas y Certificados Digitales, D.S. N° 052-2008-PCM, la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, Versión 3.3, INDECOPI.

La TSA-TOC PERU SAC cumple con las obligaciones establecidas por la normativa vigente en cuanto a la protección de datos personales, de conformidad con lo dispuesto por la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento.

Respecto a Seguridad en los Procesos de Desarrollo y Soporte de los Sistemas de Información debe asegurarse, que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

#### Derechos de propiedad intelectual

La TSA es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación.

Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la TSA sin la autorización expresa por su parte. No obstante, no necesitará autorización de la TSA para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Certificación.

#### **8.4.12 Registro de información concerniente a la operación de los servicios de sellado de tiempo**

La TSA-TOC PERU SAC, realiza el registro y control de eventos relevantes de su operación. Estos incluyen los registros de auditorías de operaciones de la gestión del ciclo de vida de las claves privadas de la TSA y la operación de sus sistemas.

#### **8.5 Aspectos organizacionales**

La TSA-TOC PERU SAC forma parte de la TOC SA, siendo sus datos de contacto los siguientes:

<b>TOC PERU SAC- Autoridad de Sellado de Tiempo</b>	
Correo electrónico	contacto@toc.pe
Número de teléfono	+51 975 165 669
Sitio web	<a href="http://www.toc.pe">http://www.toc.pe</a>

### **9. CONSIDERACIONES DE SEGURIDAD**





Para verificar los Sellos Digitales de Tiempo (TST) se debe verificar que el certificado de la TSU se confiable y no se encuentre revocado o cancelado. Esta operación debe realizarse cada vez que se requiera verificar el TST.

Adicionalmente, para la aplicación de los sellos de tiempo quien solicita el sello de tiempo debe asegurarse el valor del hash que se remite a la TSA concuerda con el hash de los datos que se desean firmar.

## **10. AUDITORIAS**

### **10.1 Frecuencia.**

Las auditorías internas se llevarán a cabo al menos una vez al año en TOC PERU SAC S.A.C. Las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y cada vez que esta entidad lo requiera.

### **10.2 Auditores**

La selección de los auditores depende del INDECOPI.

### **10.3 Relación de los auditores con la TSA**

Los auditores, evaluadores o asesores serán independientes de TOC PERU S.A.C., o cualquiera en calidad de proveedor de TOC Perú SAC

## **11. Publicación De La Declaración De Practicas**

La DPSAV de TOC PERÚ S.A.C., y otros documentos relevantes asociados, son publicados en [www.toc.pe](http://www.toc.pe) . Toda modificación importante será comunicada a INDECOPI, las versiones nuevas reemplazarán las anteriores en el sitio web.

El presente documento será revisado y aprobado por los responsables de la SVA antes de ser publicado, y se controlan las versiones del mismo.



## 12. BIBLIOGRAFÍA.

En la redacción del presente documento se utilizó:

- Ley N° 27269, de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo N° 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105-2012-PCM.
- Ley N° 29733, de Protección de Datos Personales.
- ANEXO 1: Marco de la Política de Registro para la Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Registro ER, versión 3.3, expedido por la AAC.
- 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).
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16ª Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.

A handwritten signature in blue ink is positioned above a circular stamp. The stamp contains the text: ALEXANDER DE FELDUS, TOC PERU SAC, and GERENTE GENERAL.