ACEPTA

Empresas
a velocidad
digital

PO01

Políticas de Sello de Tiempo

Marzo de 2015

OID: 1.3.6.1.4.1.6891.200

MANUEL ENRIQUE GODOY RAMIREZ

Digitally signed by MANUEL ENRIQUE GODOY RAMIREZ
Date: 2025.02.14 10:39:02 -03'00'

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y Seguridad	- Gerente de Certificación y Seguridad - Oficina técnica.	Gerente General

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Políticas de Sello de Tiempo	1.0	Primera versión	18-03-2015
Políticas de Sello de Tiempo	4.0	Revisión anual	01-10-2016
Políticas de Sello de Tiempo	4.1	Ampliación Perú	03-01-2017
Políticas de Sello de Tiempo	5.0	Revisión anual	01-10-2017
Políticas de Sello de Tiempo	5.1	Ajustes auditoría Acreditación	06-04-2018
Políticas de Sello de Tiempo	5.2	Ajustes contacto, acrónicos y calificación asesores	25-04-2018
Políticas de Sello de Tiempo	6.0	Revisión anual	11-03-2019
Políticas de Sello de Tiempo	6.1	Ajustes a capítulo 6, producto de seguimiento 2019	15-04-2019
Políticas de Sello de Tiempo	6.2	Actualización producto de nuevas guías de acreditación INDECOPI	30-09-2019
Políticas de Sello de Tiempo	7.0	Revisión anual	01-10-2019
Políticas de Sello de Tiempo	8.0	Revisión anual	01-10-2020
Políticas de Sello de Tiempo	9.0	Revisión anual	15-03-2022
Políticas de Sello de Tiempo	10.0	Revisión anual	15-03-2023
Políticas de Sello de Tiempo	10.1	Ajustes producto de Renovación de Acreditación	17-05-2023
Políticas de Sello de Tiempo	11.0	Revisión anual	30-04-2024

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: **Baja** **NIVEL DE CONFIDENCIALIDAD:** **Pública**
NOTA DE CONFIDENCIALIDAD: Se encuentra disponible ante su solicitud.

CONTROL DE DIFUSIÓN

AUTOR/ES: Gerencia de Certificación y Seguridad
DISTRIBUCIÓN: • Sitio web • INDECOPI

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	
Ley N° 27269 (Perú) RFC 3628 "Policy Requirements for Time-Stamping Authorities" RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)". ETSI TS 102 023 "Electronic Signatures and infrastructures (ESI) Policy Requirements for Time-Stamping Authorities" ISO 27001 ISO27002	

ÍNDICE

RESPONSABLES 2
HISTORIAL DE CAMBIOS 2
CLASIFICACIÓN DEL DOCUMENTO 3
CONTROL DE DIFUSIÓN 3
REFERENCIAS 4
ÍNDICE 5
1 Introducción 9
1.1 Presentación 9
1.1.1 Sobre las Políticas de Sello de Tiempo 9
1.1.2 Alcance 9
1.1.3 Referencias 9
1.2 Identificación 10
1.3 Comunidad de usuarios y aplicabilidad 10
1.3.1 Comunidad de usuarios 11
1.3.2 Aplicabilidad de los certificados de sellos de tiempo 12
1.3.2.1 Uso 12
1.3.2.2 Usos prohibidos 12
1.3.2.3 Estructura de los sellos de tiempo 12
1.4 Cumplimiento 12
1.5 Detalle de los contactos y administración de la TSA 12
1.6 Definiciones y Acrónimos 12
1.6.1 ACRÓNIMOS 13
2 Obligaciones y responsabilidades 14
2.1 Obligaciones de la TSA 14
2.1.1 GENERAL 14
2.1.2 OBLIGACIONES de la TSA hacia sus suscriptores 14
2.2 Obligaciones del suscriptor 14
2.3 Obligaciones de partes que confían 14
2.4 Responsabilidades 15
2.4.1 Responsabilidades Legales 15
2.4.2 Responsabilidades Generales 15
2.4.3 Fuerza Mayor 15

2.4.4 Resolución de Conflictos 15
3 Requerimientos en prácticas de la TSA 16
3.1 Prácticas y declaraciones de divulgación 16
3.1.1 Declaración de PRÁCTICAS de TSA 16
3.1.2 Declaración de DIVULGACIÓN de TSA 16
3.2 Gestión del ciclo de vida de las llaves 16
3.2.1 Generación de LA llave de la TSU 16
3.2.2 Protección de la llave privada de la TSU 17
3.2.3 Distribución de la LLAVE pública 17
3.2.4 Reemisión de LLAVES de la TSU 17
3.2.5 Termino del ciclo de VIDA de la llave del TSU 18
3.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo. 18
3.2.6.1 Hardware no es intervenido durante su viaje o almacenamiento 18
3.2.6.2 Administración del HW Criptográfico 18
3.3 Sello de tiempo 18
3.3.1 Token de sello de tiempo 18
3.3.2 Sincronización de LOS relojes con UTC 19
3.4 Gestión de la TSA y operaciones 19
3.4.1 Gestión de la SEGURIDAD 19
3.4.2 Gestión y clasificación de activos 20
3.4.3 SEGURIDAD del personal 20
3.4.3.1 Requerimientos de antecedentes y experiencia 20
3.4.3.2 Comprobación de antecedentes 20
3.4.3.3 Roles de confianza 20
3.4.3.4 Requerimientos de formación y reentrenamiento 20
3.4.3.5 Frecuencia de rotación de tareas 20
3.4.3.6 Sanciones 20
3.4.3.7 Requerimientos de contratación 21
3.4.3.8 Documentación entregada al personal 21
3.4.3.9 Control de cumplimiento 21
3.4.3.10 Finalización de contratos 21
3.4.4 Seguridad física y ambiental 21
3.4.4.1 Emisión de sellos de tiempo, así como su administración 21

3.4.4.2 Control de los módulos criptográficos 21
3.4.4.3 Controles físicos y ambientales 21
3.4.5 Gestión de las operaciones 23
3.4.6 Gestión de acceso a los SISTEMAS 23
3.4.7 Mantenimiento e IMPLEMENTACIÓN de sistemas de confianza 23
3.4.8 Compromiso DE los servicios de TSA 24
3.4.9 Cese DE una TSA 24
3.4.10 Cumplimiento de REQUERIMIENTOS legales 24
3.4.11 Registro de información concierne a las operaciones del servicio de sello de tiempo 24
3.5 Organización 25
4 Consideraciones de seguridad 26
5 Procedimientos de auditoría de seguridad 27
5.1 Tipos de eventos registrados 27
5.2 Frecuencia de procesamiento del log 27
5.3 Periodo de Retención para el log de auditoría 27
5.4 Protección del log de auditoría 27
5.5 Procedimientos de respaldo del log de auditoría y registros 27
5.6 Evaluaciones de vulnerabilidad 27
5.7 Identidad/calificaciones de asesores 27
5.8 Política para archivo de registros 27
5.9 Cumplimiento de auditoría y otras evaluaciones 27
6 Otros negocios y materias legales 28
6.1 Tarifas 28
6.1.1 Tarifas para la emisión de sellos 28
6.1.2 Tarifas de acceso a INFORMACIÓN de sellos 28
6.1.3 Tarifas para INFORMACIÓN sobre cancelación o estado 28
6.1.4 Tarifas para OTROS servicios 28
6.1.5 Políticas de REEMBOLSO 28
6.2 Responsabilidad Financiera 28
6.3 Confidencialidad de información del negocio 28
6.4 Privacidad 28
6.5 Propiedad Intelectual 28
6.6 Representación y Garantía 28
6.7 Exención de Garantías 28

6.8 Limitaciones de responsabilidad 28
6.9 Indemnizaciones 29
6.10 Duración y terminación 29
6.11 Noticias individuales y comunicaciones con participantes 29
6.12 Enmiendas 29
6.12.1 PROCEDIMIENTO para enmendaduras 29
6.12.2 Mecanismos y PERIODOS de notificación 29
6.12.3 Circunstancias bajo las CUALES debe ser cambiado el OID 29
6.13 Resolución de disputas 29
6.14 Leyes gubernamentales 29
6.15 Cumplimiento con la ley aplicable 30
6.16 Misceláneas 30
6.17 Otras provisiones 30
7 Revisión y aprobación del documento 31
7.1 Revisión 31
7.2 Control de cambio 31
7.3 Aprobación 31

1 Introducción

1.1 Presentación

En este documento se presenta la Política de sello de tiempo asociada a la emisión de sello de tiempo de Acepta, la cual se encuentra publicada en la página web de Acepta. Estas son una definición de las reglas a las que se ajustan los procedimientos o prácticas que Acepta declara convenir en la prestación de sus servicios de sello de tiempo. Lo anterior tanto al momento de emitir o gestionar la información usada en la solicitud del sello, durante la verificación de los token de *time-stamping*, al momento de la confirmación de vigencia de la llave privada de la TSA - a través de la CRL o servicio OCSP - así como ante el evento de que la llave de la TSA haya sido comprometida; todo lo cual se encuentra definido en esta política. Se define además los roles, responsabilidades y relaciones entre el usuario final y Acepta, siendo la Declaración de Prácticas de Sello de Tiempo de nuestra empresa un complemento a este documento.

Esta Política de sello de tiempo constituye el marco general de normas aplicables a toda la autoridad certificadora de Acepta, cuando ella actúa como Autoridad de sello de tiempo (TSA).Sin embargo, el detalle aplicable a cada sello que se emita se establece en. Este documento se encuentra disponible, en forma pública, en https://sovos.com/es/politicas-y-practicas/.

Cabe indicar que la presente Política de sello de tiempo, se ha generado siguiendo las especificaciones del documento RFC 3628 "*Policy Requirements for Time-Stamping Authorities*" así como también de las especificaciones técnicas definidas en el documento ETSI TS 102 023 *"Electonic Signatures and infraestructures (ESI) Policy Requirements for Time-Stamping Authorities"* y el documento RFC 3161 *"Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)".*

1.1.1 Sobre las Políticas de Sello de Tiempo

Las políticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los sellos de tiempo que provee Acepta, desde la gestión de la solicitud de un sello de tiempo, la obtención de un tiempo confiable, hasta la emisión del sello de tiempo requerido. Es decir son aquellas políticas a nivel de sistemas como de personal, que en base a sus buenas prácticas dan seguridad y confianza a los sellos de tiempo y servicios de certificación provistos por Acepta.

1.1.2 Alcance

El alcance de la Política de Sello de Tiempo define las normas y condiciones de los servicios que presta Acepta para la emisión de los mismos en su actuar como TSA.

1.1.3 Referencias

La presente Política de Sello de Tiempo se ha generado en base a las especificaciones del documento RFC 3628 "*PolicyRequirements for Time-Stamping Authorities*" así como también de las especificaciones técnicas definidas en el documento ETSI TS 102 023 *"Electronic Signatures and infraestructures (ESI) Policy Requirementsfor Time-Stamping Authorities"* y el documento RFC 3161 *"Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)".*

De manera complementaria a los documentos indicados, se ha utilizado el documento de las guías de acreditación de los servicios de SVA, entregadas por Indecopi en Perú.

1.2 Identificación

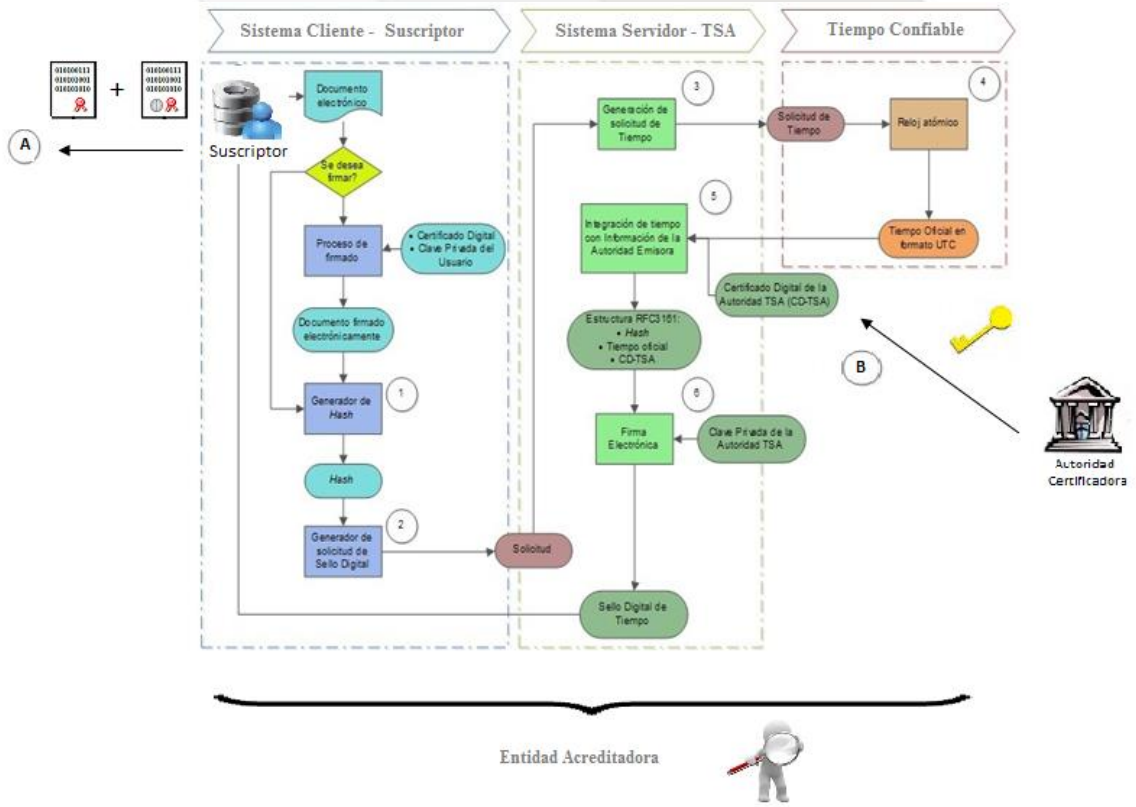
El presente documento se denomina “Políticas de Sello de Tiempo” de Acepta, las que internamente se citan como Políticas de Sello de Tiempo y están registradas con el número único internacional (OID) 1.3.6.1.4.1.689.200.Este número identifica únicamente a Acepta en un contexto global, el cual está registrado en la internet Assigned Number Authority (IANA).

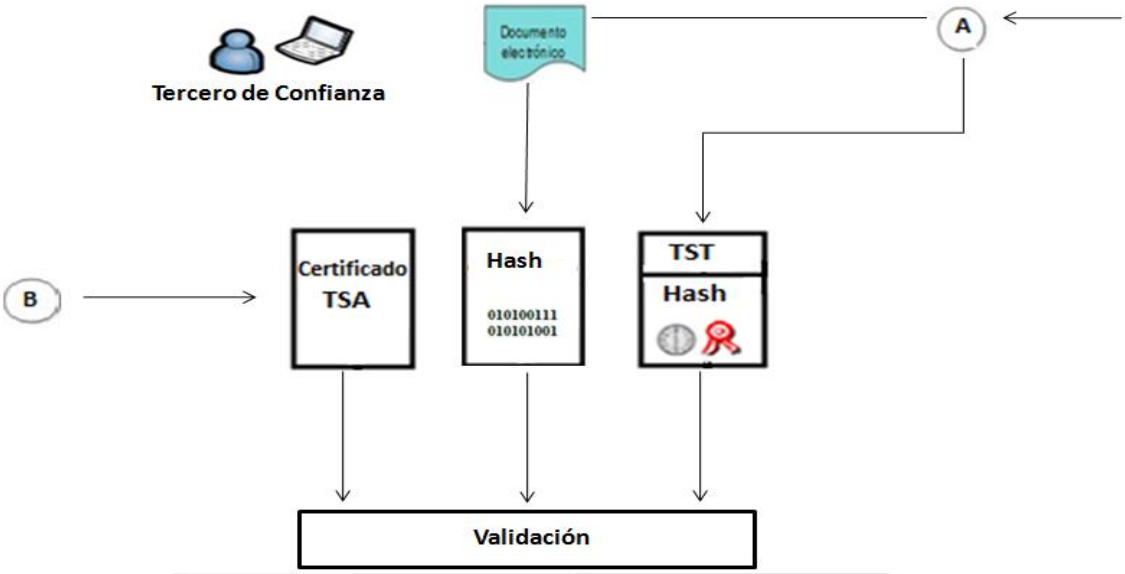
En la Declaración de prácticas de Sello de Tiempo de Acepta, sección 1.2 Identificación, se presenta la lista completa de OIDs administrados por Acepta.

1.3 Comunidad de usuarios y aplicabilidad

Los servicios de sellos de tiempo emitidos por la Autoridad de Sellado de Acepta, están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 5 tipos: Autoridad Certificadora (CA), Autoridad sello de tiempo (TSA), titulares, terceras partes que confían en los certificados y entidades acreditadoras.

La siguiente figura muestra dicha relación:





1.3.1 Comunidad de usuarios

- **Autoridad de Certificación:** Para el servicio de sello de tiempo (TSS), los certificados de las unidades de sello de tiempo (TSU) son entregados por la Autoridad de Certificación (CA). Estos certificados permiten a las terceras partes confinantes, el identificar a la Autoridad de sello de tiempo(TSA)

- **Autoridad de Sello de Tiempo:** Es la organización que opera y controla el funcionamiento de la sincronización del tiempo, emisión y otros procesos específicos de sellado de tiempo de un documento o dato, es decir la TSA tiene como obligación la provisión de los servicios de sellado de tiempo.

- **Suscriptores**: Son entidades que pueden ser individuos, empresas, sistemas y otro tipo, que solicitan la emisión de sellos de tiempo de la TSA y están de acuerdo con sus términos de uso descritos en las políticas y declaración de prácticas de sello de tiempo de la TSA.

- **Tercera parte que confía**: Son entidades que pueden ser individuos, empresas, sistemas y otro tipo, que son receptores de un sello de tiempo, generado por una TSA bajo las políticas y prácticas que ella ha definido, y actúan de acuerdo al resultado de la verificación obtenida para el sello de tiempo recibido . Una tercera parte que confía no necesariamente es un suscriptor de la TSA. Para realizar la verificación de los sellos de tiempo emitidos por la TSA, la parte que confía debe contar con mecanismos que le permitan validar si se trata de un sello de tiempo auténtico.

- **Entidad Acreditadora**: La comunidad de usuarios requiere de un organismo independiente y de confianza que acredite que las políticas y prácticas de la TSA, son coherentes con las necesidades del sello de tiempo y que la TSA cumple cabalmente con dichas políticas y prácticas. Por ejemplo para los sellos de tiempo, la entidad acreditadora es el INDECOPI; para los certificados válidos en el ámbito tributario la entidad acreditadora es SUNAT y para los certificados de sitio Web Acepta trabaja sin una entidad acreditadora.

1.3.2 Aplicabilidad de los certificados de sellos de tiempo

Los sellos de tiempo emitidos por Acepta se utilizarán únicamente conforme a la función y finalidad que tengan establecida en éstas Políticas de Sello de Tiempo y la Declaración de Prácticas de Sello de Tiempo, en concordancia con la normativa vigente para garantizar el no repudio.

1.3.2.1 Uso

El uso de los sellos de tiempo aquí descrito está acotado a demostrar que una serie de datos han existido y no han sido alterados desde un instante de tiempo específico y confiable.

El conjunto de normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denomina "Política de Sello de Tiempo".

1.3.2.2 Usos prohibidos

Los sellos de tiempo emitidos por Acepta, se utilizarán únicamente conforme a la función y finalidad que se tenga establecida en la presente Política de Sello de tiempo y la declaración de prácticas de sellos de tiempo y de acuerdo a la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

1.3.2.3 Estructura de los sellos de tiempo

La estructura de los sellos de tiempo generados por Acepta, se ajustan al documento RFC 3161 "*Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)".*

1.4 Cumplimiento

La TSA referencia el OID de las políticas de sello de tiempo, definidas por Acepta, en cada uno de los sellos de tiempo emitidos como en su página web. Declarando así la correcta implantación de éstas, a fin de asegurar el cumplimiento de las obligaciones descritas en este documento para cada una de las partes. Es por ello que realiza la implementación de los controles y procedimientos identificados en esta política y en las prácticas para garantizar la confianza en los sellos de tiempo que emite, ya que es periódicamente inspeccionada por la Entidad Acreditadora de INDECOPI.

1.5 Detalle de los contactos y administración de la TSA

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada en la siguiente dirección:

- **PERÚ:**
    - **Nombre**: ACEPTA PERU S.A.C.
    - **Dirección de e-mail**: contacto_cys@acepta.com
    - **Dirección**: Calle Amador Merino Reyna 465, Piso 6, Oficina 602, San Isidro, Lima, Perú
    - **Código Postal:** 15046
    - **Número telefónico**: (+511) 7307820

1.6 Definiciones y Acrónimos

El alcance de las definiciones del documento de Políticas de sello de tiempo, se entenderá como:

- **Parte que confía:** Receptor del *token* de sellado de tiempo que confía en este sello de tiempo, o cualquier entidad que quiera comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Puede ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.

- **Subscriptor:** Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sello de Tiempo y el cual implícita o explícitamente acepta las políticas de uso de este servicio. En un proceso de sellado de tiempo, es el solicitante que posee la información a la que quiere incluir un sello de tiempo para probar que los datos existían en un determinado instante.
- **Token de sellado de tiempo:** Dispositivo de datos empleado a un proceso de creación de firma electrónica, que está asociado a una representación de un dato para un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los *token* de sellado de tiempo deben emitirse de acuerdo al RFC 3161 "*Internet X.509 Public Key Infrastructure Time StampProtocol (TSP)*".
- **Autoridad de Sellado de Tiempo** (TSA por sus siglas en inglés *Time Stamping Authority*): Sistema de emisión y gestión de sello de tiempo basado en una firma digital acreditada dentro de la jerarquía nacional de certificadores registrados, encargada de proveer uno o más servicios de sellado de tiempo a través de unidades de sellado de tiempo (TSU).
- **Sistema de TSA:** Conjunto de elementos organizados para soportar los servicios de sellado de tiempo.
- **Política de sellado de tiempo:** Conjunto de reglas que indican la aplicabilidad de un *token* de sellado de tiempo para una comunidad particular y/o la clase de aplicación con requerimientos de seguridad comunes.
- **Unidad de sellado de tiempo** (TSU por sus siglas en inglés, "*time-stamping unit*") es el conjunto de hardware y software que es gestionado como una unidad y que tiene un *token* de sellado de tiempo firmado por una llave privada de la TSA.
- **Tiempo Universal Coordinado** (UTC por sus siglas en inglés *Universal Time Coordinated*): También conocido como tiempo civil, el cual es determinado por la referencia a una zona horaria. El tiempo coordinado UTC está basado en relojes atómicos que se sincronizan para obtener una alta precisión y es el sistema de tiempo utilizado como estándar por la *World Wide Web*.
- **Declaración de Prácticas de sellado de tiempo:** Declaración de las Prácticas que una autoridad de sellado de tiempo emplea en la emisión de los *token* de sellado de tiempo.

1.6.1 ACRÓNIMOS

- AC: Autoridad Certificadora
- AR: Autoridad de Registro
- CA: Certification Authority
- RA: Registration Authority
- TSA: Autoridad de sellado de tiempo
- TSS: Servicio de sellado de tiempo
- TST: *Token* de sello de tiempo
- UTC: Tiempo universal coordinado
- TSU: unidad de sello de tiempo

2 Obligaciones y responsabilidades

2.1 Obligaciones de la TSA

2.1.1 General

Acepta, en su calidad de Autoridad de Sello de Tiempo se obliga a:

- Realizar sus operaciones y proveer todo los servicios de *Time-Stamping* de acuerdo a lo dispuesto en ésta política, así como en la Declaración de Prácticas de sello de tiempo.
- En caso de subcontratar en el futuro alguno de los servicios, asegurará que los contratistas mantienen un fiel cumplimiento de estas políticas así como de las prácticas de *Time Stamp*.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sello de tiempo a los que sirven de soporte.

Las obligaciones específicas, pertinentes al sello de tiempo emitido detalladas en estas Políticas de sello de tiempo se encuentran disponible de manera pública en el sitio https://sovos.com/es/politicas-y-practicas/.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.1.2 Obligaciones de la TSA hacia sus suscriptores

La TSA de Acepta garantiza el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC, que está incluido en los sellos, se asegura con una desviación máxima 1 segundo.

Además garantiza que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo y se garantiza un nivel de servicio superior al 95% que permite dar el cumplimiento a las normas técnicas.

Para un mayor detalle respecto a la disponibilidad del sistema, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.2 Obligaciones del suscriptor

El suscriptor debe verificar que el *token* de *time-stamping* se ha firmado de manera correcta y comprobar en la CRL el estado del certificado de la TSA, esta comprobación de validez se puede hacer también, utilizando el servicio OCSP.

Además debe conocer las normas estipuladas en las políticas y prácticas de sello de tiempo de Acepta, así como el propósito y alcance de un sello de tiempo obtenido en Acepta o en algún Prestador de Servicios de Sellos de Tiempo acreditado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.3 Obligaciones de partes que confían

Las partes que confían deben tener conocimiento del alcance y uso del sello de tiempo recibido, como de las normas legales que sigue el Proveedor de Servicios de Certificación, además será responsable de verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Adicionalmente deberán dar aviso a la TSA de cualquier situación anómala ya sea en el servicio o en los sellos de tiempo emitidos por la TSA.

Para un mayor detalle sobre la verificación de sello de tiempo, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.4 Responsabilidades

2.4.1 Responsabilidades Legales

Acepta no será responsable de cualquier perjuicio que derive de una utilización negligente o no acorde a las políticas y/o declaración de prácticas de sello de tiempo, por parte de los suscriptores o terceras partes que confían.

Las responsabilidades asumidas por Acepta como TSA, se encuentran declaradas en sus prácticas de sello de tiempo y en los contratos o acuerdos de suscripción. Para asumir éstas, Acepta cuenta con un seguro de responsabilidad civil en conformidad al DS 052-2008.

Para un mayor detalle de las responsabilidades legales, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.4.2 Responsabilidades Generales

Acepta garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley N° 27269 y en virtud de esto, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, así como por el incumplimiento de las prescripciones contenidas en la Ley N° 29733 relativas a la protección de datos personales. En ningún caso será responsable de cualquier perjuicio que derive de una utilización negligente, por parte de los suscriptores o terceras partes interesadas, o no acorde con las políticas y prácticas establecidas por la TSA de Acepta.

Acepta, como proveedor de servicios de Sello de Tiempo, adhiere a los estándares internacionales que rigen esta actividad, siendo ellos los documentos RFC 3628, RFC 3161 y su equivalente ETSI 102 023.

Para un mayor detalle del cumplimiento de las responsabilidades generales, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.4.3 Fuerza Mayor

Acepta queda exenta de responsabilidad en caso de pérdida o perjuicio, siendo esto el resultado de un evento de fuerza mayor que le impida proveer los servicios de *Time-Stamp*.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

2.4.4 Resolución de Conflictos

Remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3 Requerimientos en prácticas de la TSA

3.1 Prácticas y declaraciones de divulgación

3.1.1 Declaración de PRÁCTICAS de TSA

La información establecida en este documento se completa con el documento de prácticas de sello de tiempo que detalla la implementación de los controles que son necesarios para cumplir con esta política de sellado de tiempo, así como políticas, normativas, procedimientos, ya sean estos operacionales y/o técnicos para uso interno de Acepta, que garantizan la fiabilidad y la confianza del servicio de sellos de tiempo.

En particular Acepta, como TSA establece que ha trabajado en:

- Una determinación de activos y riesgo asociado a c/u de los activos relevantes que participan en los servicios de la TSA.
- Un SGSI para mitigar los riesgos detectados, el cual es controlado por un comité de seguridad, el que define los cursos de acción y aprueba las mejoras a los controles implantados.
- Una política y práctica que permita proveer los servicios de su TSA, así como las modificaciones a estos documentos que han sido formalmente aprobadas.
- La publicación hacia la comunidad de la información relevante asociada a este servicio tales como las condiciones bajo las que se provee los servicios de la TSA.

Además se detallan los mecanismos y procedimientos establecidos para cumplir con las obligaciones y responsabilidades, control de seguridad, así como modificaciones y planes de mejora, elementos de información de contacto, características técnicas del servicio de sello, leyes y estándares, entre otros que constituyen el funcionamiento de la TSA, las que deben ser contempladas por todas las organizaciones externas incluyendo las políticas y prácticas de sello de tiempo aplicables.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.1.2 Declaración de DIVULGACIÓN de TSA

LA TSA de Acepta entrega como parte de estas políticas su información de contacto a los suscriptores y terceros, da a conocer la política que rige su operación incluyendo en esta última: el algoritmo de hash utilizado, vigencia de la firma, la precisión del tiempo registrado en cada uno de los TST emitidos, responsabilidades y obligaciones de las partes que participen del proceso asociado al servicio de la TSA, información que permita verificar la validez del TST, el periodo de retención de los logs de eventos, normativa legal aplicada, limitación de responsabilidades, solución de conflicto entre las partes, resolución que aprueba la operación como Autoridad de sello de Tiempo emitida por INDECOPI.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.2 Gestión del ciclo de vida de las llaves

3.2.1 Generación de LA llave de la TSU

El módulo criptográfico adoptado por Acepta, es capaz de generar llaves en base al algoritmo de encriptación de llave publica SHA2RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS_CO; Así mismo, la TSA de Acepta cuenta para la

generación de los TST solicitados, con un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3.

Respecto al personal que participa en la generación de la llave, por parte de la CA de Acepta, y que es usada por TSU, se declara que ellos pertenecen a los roles de confianza definidos y cualquier actividad a realizar sobre el módulo HSM requiere de un quórum 3 de 8 personas.

Acepta declara que satisface los requerimientos identificados en *CEN Workshop Agreement* 14167-2 [CWA 14167-2] o ISO 15408 al cumplir con la ETSI TS 102 042 que fue la que dio origen al ciclo de vida de la llave aquí descrito.

Para mayor detalle remítase a la Declaración de Prácticas de sello de tiempo de Acepta.

3.2.2 Protección de la llave privada de la TSU

Acepta cuenta con niveles de seguridad del HSM donde se almacena la clave bajo control, a fin de asegurar la confidencialidad e integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3.

En lo que respecta a la generación de la llave de la TSU, el módulo criptográfico utilizado por Acepta mantiene la confidencialidad de la llave en su ciclo de tiempo completo, restringiendo el acceso a éste al personal autorizado solamente. De detectarse un acceso no autorizado, este se registra ya sea de manera física (*tampering* físico) o a través de log a ser usado durante la auditoría. Este equipo contempla además mecanismos de *backup* y respaldo de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos. Acepta declara cumplir con el documento "*CEN Workshop Agreement* 14167-2 [CWA 14167-2]" o ISO 15408 en lo correspondiente al ciclo de vida de su llave criptográfica, realizando la implantación de estos controles de acuerdo a la norma ETSI TS 102 042.

En cuanto a los respaldos, ellos sólo son recuperados por el personal con roles de confianza y bajo un ambiente seguro, de acuerdo a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.2.3 Distribución de la LLAVE pública

El certificado de la TSA incluye su clave pública, la cual se distribuye a través de la página web de Acepta. Este certificado digital utilizado por la TSA es generado por la PSC de Acepta, de acuerdo a las políticas y prácticas de certificación inspeccionadas por INDECOPI para esta PKI, La distribución se basa en establecer la confianza con la TSA de acuerdo al modelo de confianza definido por Acepta asegurando la integridad y autenticidad de la firma de la TSU.

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.2.4 Reemisión de LLAVES de la TSU

Por motivo de seguridad y evitar el repudio a un certificado, Acepta como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo a las políticas y prácticas que rigen la operación de su CA. Sin embargo, la llave privada de la TSU será reemplazada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.
Las claves privadas caducadas se almacenan por un periodo no inferior a 10 años, siendo Acepta la ejecutora del procedimiento y la responsable de esta decisión. Las claves públicas se almacenan por un periodo adicional no inferior a 15 años, para permitir la verificación de sellos de tiempo emitidos con dichas claves.

3.2.5 Termino del ciclo de VIDA de la llave del TSU

La llave privada de la TSU debe ser reemplazada al momento de su expiración o ante un evento de seguridad que vulnere dicha llave. La TSU de Acepta rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida al igual que sus copias de respaldo, a fin de que sus clave privada no pueda ser recuperada.

Detalle del proceso de término del ciclo de vida de la llave de la TSU se encuentra especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo.

Respecto al ciclo de vida del hardware criptográfico el personal de Acepta y terceros involucrados deben cumplir el la normativa del dicho ciclo que a continuación se detalla:

3.2.6.1 Hardware no es intervenido durante su viaje o almacenamiento

Los HSM de Acepta cuentan con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión y en caso que ocurra esto en los HSM, cualquiera sea el motivo, las claves son borradas y destruidas, de acuerdo con los procedimientos del fabricante. Ante este tipo de eventos dichos equipos no entrarán a producción, previo a la reiniciación del equipamiento de acuerdo al quórum definido.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.2.6.2 Administración del HW Criptográfico

El equipo HSM que será utilizado por Acepta tanto para su PSC como TSA, implementa la seguridad de acceso a información criptográfica a través de diferentes niveles a fin de garantizar que los equipos no han sido manipulados y cumplen con los requisitos. Además Acepta dispone de procedimientos asociados para el manejo de los HSM por el personal de confianza, utilizando tarjetas de administración y de operación, como también definiendo un quórum 3 de 8 para la administración del ambiente completo y seguro. Lo anterior se encuentra clasificado de uso interno y revisado de forma periódica por el auditor.

Respecto a las características técnicas los equipos HSM de Acepta cumplen con el estándar FIPS-140.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.3 Sello de tiempo

3.3.1 Token de sello de tiempo

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

Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el suscriptor para que sea sellado con el sello de tiempo
- Un identificador para la política de marca de tiempo
- Un número serial único que será usado para ordenar los TSTs así como para identificar un sello de tiempo específico.

- El tiempo calibrado a 1 segundo de la UTC, indicando la fuente de tiempo confiable (En particular, la fuente confiable de tiempo primaria de Acepta es *ntp.shoa.cl*)
- La firma electrónica que ha sido generada usando una llave que es sólo usada para la firma de los sellos de tiempo.
- La identificación de la TSA y de la TSU.

La TSA de Acepta establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

3.3.2 Sincronización de LOS relojes con UTC

La TSA de Acepta declara utilizar una fuente fiable de tiempo, mediante un servidor basado en el protocolo NTP que sincronice con el tiempo UTC a través de una red de satélites GPS o en caso excepcional contra múltiples fuentes que incluyen el "*National Measurenment Institute*"; lo anterior con una desviación máxima de 1 segundo.

En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la TSA.

Cuando sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempo o por cualquiera de las fuentes fiables mencionadas anteriormente, el *token* de sello de tiempo no será emitido, hasta contar con un tiempo correcto. Además Para la administración del reloj de la TSU requiere de un quórum de 3 de 8 tarjetas.

Para mayor detalle sobre la sincronización de los relojes, remitirsea lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.4 Gestión de la TSA y operaciones

3.4.1 Gestión de la SEGURIDAD

La TSA de Acepta desarrollará una administración activa de la seguridad a través de un Sistema de Gestión de Seguridad de la Información (SGSI), el que considera las mejores prácticas y estándares de la industria. El estándar que aplica la TSA de Acepta como parte de su SGSI es el estándar ISO 27001 así como los controles definidos en la ISO 27002. En particular:

a) Acepta declara que su TSA es responsable por todo los aspectos asociados a la provisión de servicios de sello de tiempo y no subcontrata los servicios de sello de tiempo.
b) Todo su personal tienen acceso a sus prácticas y políticas de sello de tiempo.
c) Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
d) Acepta cuenta con un Comité de seguridad de la información, un oficial de seguridad, un oficial adjunto y una oficina técnica, los que en su conjunto velan por el cumplimiento del plan anual definido por el SGSI.
e) Acepta declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.
f) Acepta no subcontrata los servicios de sello de tiempo.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.4.2 Gestión y clasificación de activos

Los activos de la TSA de Acepta reciben un apropiado nivel de protección. Para ello la TSA de Acepta realiza anualmente un análisis de riesgos siguiendo una metodología y herramientas basadas en la norma ISO 27001, para el cual se hace un levantamiento de los activos.

Todo lo anterior se encuentra documentado y clasificado de uso interno, siendo esta documentación revisada de forma periódica en auditorias.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.4.3 SEGURIDAD del personal

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Acepta.

3.4.3.1 Requerimientos de antecedentes y experiencia

Acepta requiere que todo el personal asociado a la TSA cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, lo cual incluye:

- Conocimientos y formación sobre entornos de certificación digital y sellos de tiempo.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la TSA.

3.4.3.2 Comprobación de antecedentes

En Acepta se realiza una comprobación de los antecedentes, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta antes de asignar un rol de confianza.

3.4.3.3 Roles de confianza

Acepta declara que sus roles de confianza al cumplir su función de TSA corresponden a:

- Oficial de seguridad
- Administrador de Sistemas.
- Administrador de Seguridad.
- Auditor.

3.4.3.4 Requerimientos de formación y reentrenamiento

Acepta considera para el personal asociado a la TSA, la formación y reentrenamiento a través de un plan anual de capacitación. Esto de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.3.5 Frecuencia de rotación de tareas

No es aplicable para Acepta, ya que las personas mantienen su cargo.

3.4.3.6 Sanciones

Acepta informa y entrega al momento del contrato, a cada empleado el Reglamento Interno, el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones.

3.4.3.7 Requerimientos de contratación

Como parte de los requerimientos de contratación, todo trabajador de la PSC y de su servicio de TSA debe firmar un acuerdo de confidencialidad, tal como es especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.3.8 Documentación entregada al personal

El personal de la TSA tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Sello de Tiempo.
- Políticas de Sello de Tiempo.
- Política de privacidad.
- Política de Seguridad de la Información.
- Organigrama y funciones del personal.

3.4.3.9 Control de cumplimiento

De acuerdo al Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

3.4.3.10 Finalización de contratos

La finalización de contratos cuenta con un procedimiento en el cual se suprimen los privilegios de acceso del individuo a las instalaciones e información de la organización, a excepción de la considerada PÚBLICA, una vez informado el individuo de su marcha y de su pérdida de privilegios, se verifica la devolución del material entregado y se les informa al resto de la organización, a los proveedores y entidades externas a Acepta de que el individuo ya no representa a la TSA de Acepta.

3.4.4 Seguridad física y ambiental

La seguridad física y ambiental se detalla en la política de seguridad, dando cumplimiento a la norma ISO 27001 en la cual se basa. Los servicios de Acepta además de acuerdo a la Declaración de prácticas de Sello de tiempo, como también a la norma ETSI TS 102.023.

3.4.4.1 Emisión de sellos de tiempo, así como su administración

La Emisión de sellos de tiempo, es realizada por el personal autorizado así como su administración será de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta, ello a fin de evitar daños, perdidas, interrupción o compromiso de los activos críticos de la TSA.

3.4.4.2 Control de los módulos criptográficos

El control de los módulos criptográficos se llevaran a cabo para evitar la pérdida de información y están de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta y el documento de *"Gestión del ciclo de vida de las llaves"*.

3.4.4.3 Controles físicos y ambientales

3.4.4.3.1 Data Center y Oficinas Centrales

Los sistemas e infraestructura del Servicio de Emisión de sellos, se encuentran alojados en un sitio principal y uno secundario. Las características generales comprenden una Zonificación en Alta Criticidad y una Zona de Media Criticidad.

Ambos cuentan con medidas que mantienen un perímetro de seguridad el cual restringe el acceso sólo a personal autorizado.

Respecto a la casa matriz de Acepta ella cuenta con accesos vigilados, área de recepción así como control de visitas y acceso biométrico del personal.

Para mayor información remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.4.3.1.1 Seguridad Física Data Center

Acepta opera en un par de *Datacenter* seguros y confiables que cuentan con niveles de protección y solidez de la construcción y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos *Datacenter* cuentan con controles definidos, para proteger los elementos que forman parte de la solución de Acepta, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

Para mayor información remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.4.3.1.2 Sistema de Energía Eléctrica

Acepta cuenta en los sitios con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación, por largos periodos de tiempo. Para esto cuenta con energía redundante a través de UPS y grupos electrógenos

Para un mayor detalle sobre el Sistema de Energía Eléctrica se encuentra especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.4.3.1.3 Sistema de Control Ambiental

El Sistema de Control Ambiental en ambos sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos y en caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

Para mayor detalle sobre control ambiental remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.4.3.1.4 Sistema de Extinción y Control de Incendios

El Sistema de Extinción y Control de Incendios cuenta con el suministro e instalación de un sistema de protección contra incendios sobre la base de detección temprana, que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática con FM-200, aprobación UL, e instalado bajo norma NFPA.

3.4.4.3.1.5 Telecomunicaciones

Las especificaciones respecto a las Telecomunicaciones se basan en una plataforma robusta, segura y escalable, utilizando para ello los servicios WAN, estos servicios provistos por los principales carriers del país que nos aseguran redes confiables y con tecnología de última generación.

Para mayor información remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.4.3.1.6 Seguridad Lógica Data Center

Los Datacenter cuentan con aspectos de seguridad lógica, lo cual se encuentra detallado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.5 Gestión de las operaciones

La TSA de Acepta establece que su sistema y componentes son fiables, ya que se encuentran operados de manera correcta con un riesgo mínimo de falla en la emisión, el control de sellos de tiempo, el manejo correcto de los medios, el control y planificación de los sistemas, control y reporte de incidentes.

Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado. Respecto al manejo de medios y seguridad, Acepta declara un apropiado tratamiento de sus activos a través de la realización de un análisis anual de riesgo riesgos basados en la norma ISO 27001, el cual genera como parte de su preparación la lista de activos de la TSA, su nivel de protección así como los procedimientos adicionales a seguir para minimizar su riesgo.

Para el manejo de incidentes y su respuesta, Acepta cuenta con un sistema de gestión de incidentes que asegura que los eventos y debilidades de la seguridad de la información, asociados con los sistemas de información de los procesos de la PSC y su TSA, son comunicados a los roles encargados de la gestión de los incidentes para que realicen correcciones oportunas.

Además considera los siguientes roles de confianza que manejan las operaciones:

- Administrador de Sistemas.
- Administrador de Seguridad.
- Responsable de formación, soporte y comunicación.
- Responsable de Seguridad.
- Auditor.
- Responsable de Documentación.

En cuanto a la Planificación de la capacidad, se debe mantener un manejo de la capacidad para la demanda, monitoreando y proyectando de acuerdo a los futuros requerimientos, de manera que la capacidad de proceso como de almacenamiento siempre sean las adecuadas. Para efectuar esto, Acepta cuenta con un procedimiento formal de gestión de capacidad de sus instalaciones.

Respecto a los procedimientos operacionales y responsabilidades, Acepta cuenta con la operación del servicio de Sello de Tiempo de la TSA, el que opera de manera independiente de otros servicios provistos por la PSC; siendo éstas desarrolladas por el personal confiable como se encuentra definido en la estructura de la PSC de Acepta y en su Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.6 Gestión de acceso a los SISTEMAS

La TSA de Acepta, asegura que el acceso a su sistema (hardware, software y datos) se encuentra protegido compartiendo las medidas de seguridad físicas que dan protección al sistema en un entorno de confianza y está limitado al personal autorizado.

Los administradores de Acepta realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA. Es por ello que se cuenta con Cortafuegos, Administración de usuarios, Restricciones de acceso a la información y sistemas, un control apropiado del personal autorizado, Logs de las operaciones. Adicionalmente, los componentes de la red local se mantienen en *Datacenters* bajo ambiente seguro y con una auditoría periódica.

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.7 Mantenimiento e IMPLEMENTACIÓN de sistemas de confianza

En la TSA de Acepta se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello que se establece monitorear y registrar cada cambio en los sistemas. Para

cualquier cambio en los sistemas se lleva a cabo un análisis de requerimientos de seguridad, procedimientos de control de cambio para nuevas versiones y la generación de las llaves siempre se lleva a cabo dentro del entorno de confianza, por personal critico autorizado.

3.4.8 Compromiso DE los servicios de TSA

La TSA de Acepta declara que ante cualquier compromiso de los servicios de sello de tiempo, se harán efectivos los procedimientos correspondientes al plan de continuidad de Acepta. Si este compromiso afecta a la llave de firma de la TSU o pérdida de precisión de su reloj, se declarará un evento de seguridad y se informará directamente o a través de su sitio web a sus suscriptores y terceros que en ella confía, dicha información del evento. Ante los eventos antes mencionados, la TSA de Acepta no emitirá nuevos TST hasta superar el compromiso declarado

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.9 Cese DE una TSA

En el momento en que Acepta vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a comunicar del cese de sus funciones con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo ya sean suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas.

Además, la TSA procederá revocar los certificados de la TSU y transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca.

En el caso de las claves y copias de respaldo de la TSA de Acepta, estas deben ser borradas y destruidas, de manera que estas no puedan ser recuperadas, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

En el procedimiento para el término de actividades, se dispondrá de los costos necesarios para los requerimientos indicados.

3.4.10 Cumplimiento de REQUERIMIENTOS legales

Acepta como Autoridad de sello de tiempo, actúa en conformidad con la Ley vigente y las directrices técnicas establecidas por los organismos calificadores (ETSI, ISO, RFC, etc.). Además su gestión y operación de servicios se encuentra regulada por la Entidad Acreditadora Indecopi y sus Guías de Acreditación.

Acepta cuenta con procedimientos de control y de seguridad de la información, a objeto de proteger la información personal de sus suscriptores de divulgación, todo ello ante un procesamiento no autorizado o ilegal, así como ante la destrucción o daño de dicha información ya sea de manera accidental o intencional. A menos que sea solicitada por él mismo o por orden judicial u otro requisito legal, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

3.4.11 Registro de información concierne a las operaciones del servicio de sello de tiempo

La TSA de Acepta debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a la información personal de los suscriptores que se ha recolectado yse encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por Acepta en su sitio web, tal como se detalla en la Declaración de Prácticas de Sello de Tiempo de Acepta.

Todos los registros concernientes a la operación del servicio de sello de tiempo se encuentran disponibles sólo al suscriptor o en caso que lo solicite una corte a través de un requerimiento legal.

La integridad de esta información es mantenida por la PSC de Acepta por un periodo de 5 años posterior a la expiración de la validez de la llave usada para la firma por parte de la TSU.

Estos registros incluyen:

- Requerimiento de sello de tiempo
- Sello de tiempo creado
- Eventos relacionados con la administración de la TSA, incluyendo:
  - Registros de eventos correspondientes al ciclo de vida de las llaves de la TSU
  - Registros de eventos correspondientes a los certificados de la TSU
  - Registros relacionados con la sincronización del reloj de usado por la TSU en sus TST
  - Registros asociados a eventos de detección de pérdida de sincronización

Los registros antes mencionados, son almacenados por Acepta y no son de fácil eliminación o destrucción dentro del periodo de tiempo previamente declarado. A estos registros, sólo tiene acceso el personal autorizado por la PSC de Acepta.

3.5 Organización

La Autoridad de Sellado de Tiempo es un servicio adicional que se encuentra soportada por la PSC de Acepta, la cual se encuentra acreditada en su operación por la Entidad Acreditadora de INDECOPI.

La TSA de Acepta cumple con:

- Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias.
- Acepta provee su servicio de sello de tiempo a cualquier suscriptor que cumpla y este de acuerdo con las obligaciones declaradas en las prácticas y políticas de sello de tiempo.
- Acepta para la provisión de sus servicios cumple con la normativa legal vigente en Perú.
- Como parte de su cumplimiento de la Ley N° 27269, con un seguro de responsabilidad civil, ante daños o perjuicios producto de su operación.
- Acepta es anualmente auditada respecto sus estados financieros y el cumplimiento de la normativa vigente.
- Acepta como PSC acreditada por Indecopi, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal.
- Acepta ante un conflicto con un cliente, el cual no pueda ser resuelto favorablemente por las partes, utilizará los Tribunales de Justicia a modo que ellos actúen como árbitro arbitrador del conflicto.
- Acepta mantiene un su repositorio documental todo contrato, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

4 Consideraciones de seguridad

Se debe tener presente que al momento del chequeo de validez de los TST, por parte de un tercero que confía, el certificado de firma de la TSU debe ser válido y no se encuentra revocado, ya que la validez del TST es cierta sólo para el momento en que se efectúa dicho chequeo, pues en un tiempo posterior puede existir un compromiso de la llave privada de la TSU de Acepta que invalida la llave de firma y por ende al TST emitido.

La TSA de Acepta asegura que hash incluido en su TST corresponde al enviado por el suscriptor en su *request.*

Para mayor detalle de las consideraciones de seguridad, remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Acepta.

5 Procedimientos de auditoría de seguridad

5.1 Tipos de eventos registrados

Los tipos de eventos registrados corresponden a los necesarios para mantener la traza de los sellos de tiempo emitidos. Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.2 Frecuencia de procesamiento del log

Acepta implementa una infraestructura y sistema de certificación de tal modo que permita monitorear continuamente las operaciones realizadas; y poder detectar cualquier situación errónea, así como cualquier intento de uso o ingreso no-autorizado al sistema. Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.3 Periodo de Retención para el log de auditoría

Todos los registros correspondientes al registro de eventos con el fin de auditoría se mantienen de tal forma que se permita una adecuada consulta y revisión de tales registros por personal autorizado Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.4 Protección del log de auditoría

Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.5 Procedimientos de respaldo del log de auditoría y registros

Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.6 Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, Acepta y sus PSC acreditadas tienen un accionar sistemático y pro-activo respecto a la detección y evaluación de posibles vulnerabilidades que puedan atentar contra dicha seguridad. Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.7 Identidad/calificaciones de asesores

Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.8 Política para archivo de registros

Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

5.9 Cumplimiento de auditoría y otras evaluaciones

Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

6 Otros negocios y materias legales

6.1 Tarifas

Remítase a la declaración de prácticas de sello de tiempo.

6.1.1 Tarifas para la emisión de sellos

Remítase a la declaración de prácticas de sello de tiempo.

6.1.2 Tarifas de acceso a INFORMACIÓN de sellos

Remítase a la declaración de prácticas de sello de tiempo.

6.1.3 Tarifas para INFORMACIÓN sobre cancelación o estado

Remítase a la declaración de prácticas de sello de tiempo.

6.1.4 Tarifas para OTROS servicios

Remítase a la declaración de prácticas de sello de tiempo.

6.1.5 Políticas de REEMBOLSO

Remítase a la declaración de prácticas de sello de tiempo.

6.2 Responsabilidad Financiera

Acepta cuenta con un seguro de responsabilidad civil y un respaldo económico descrito en sus estados financieros.

6.3 Confidencialidad de información del negocio

De acuerdo a plan de privacidad y política de privacidad de Acepta publicada en su página web.

6.4 Privacidad

De acuerdo a plan de privacidad y política de privacidad de Acepta publicada en su página web.

6.5 Propiedad Intelectual

La prestación de los servicios de sellado de tiempo en ningún caso otorga a los partícipes de la comunidad descritos en 1.3 de estas CPS derecho de propiedad intelectual o industrial alguno. Así, Acepta retiene todos sus derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por Acepta, se entenderá conferido a los miembros de la comunidad antes citada. Para mayor detalle remítase a la declaración de prácticas de sello de tiempo.

6.6 Representación y Garantía

Remítase a la declaración de prácticas de sello de tiempo.

6.7 Exención de Garantías

De acuerdo al alcance de su póliza vigente.

6.8 Limitaciones de responsabilidad

Remítase a la declaración de prácticas de sello de tiempo.

6.9 Indemnizaciones

Acepta dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado.

6.10 Duración y terminación

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC de la IOFE, y su periodo de vigencia es de 05 años al ser este el plazo de las acreditaciones otorgadas por la AAC de acuerdo a la legislación vigente. Esto sin perjuicio que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia de Acepta o determinación de la AAC. Respecto a la terminación se regirá de acuerdo a 3.4.9 de este documento.

6.11 Noticias individuales y comunicaciones con participantes

Toda notificación o comunicación se hará mediante correo electrónico o por escrito dirigido a la dirección señalada en el contacto del presente documento (punto 1.5).

6.12 Enmiendas

6.12.1 Procedimiento para enmendaduras

En caso se actualice algún procedimiento o se requiera hacer alguna enmendadura Acepta presentará a la AAC la nueva versión del documento para su respectiva aprobación y posterior publicación.

6.12.2 Mecanismos y periodos de notificación

Acepta pondrá a disposición de la comunidad de usuarios, así como a otras infraestructuras que la reconocen, la nueva versión de su CP, una vez que la misma haya sido aprobada por la AAC.

Acepta comunicará a los participantes de la IOFE, así como a otras infraestructuras que la reconocen, aquellas modificaciones que impliquen cambios en los términos y condiciones básicas de la prestación de los servicios de certificación que brinda.

El mecanismo de comunicación se efectuará a través de la publicación en la página WEB de Acepta, surtiendo los efectos de una notificación válidamente emitida.

6.12.3 Circunstancias bajo las cuales debe ser cambiado el OID

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

6.13 Resolución de disputas

Remítase a la declaración de prácticas de sello de tiempo.

6.14 Leyes gubernamentales

Estará sujeto a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones.
- Guía de Acreditación de SVA.
- Ley N° 29733, Ley de Protección de Datos Personales.

Así como a las disposiciones que sobre la materia dicte el INDECOPI como Autoridad Administrativa Competente en el marco de la IOFE.

6.15 Cumplimiento con la ley aplicable

Es responsabilidad de Acepta en la prestación de sus servicios, el cumplimiento de la legislación recogida en numeral 6.14.

6.16 Misceláneas

Remítase a la declaración de prácticas de sello de tiempo.

6.17 Otras provisiones

No aplica

7 Revisión y aprobación del documento

7.1 Revisión

Este documento es revisado anualmente a fin de verificar su validez y eficacia, o en un plazo menor en caso de producirse cambios significativos que ameriten su revisión de acuerdo al marco regulatorio, comercial, legal o técnico.

7.2 Control de cambio

Cada vez que se requiera efectuar una modificación, esta debe ser incorporada al documento y reflejada bajo un control de cambio. Para ello se debe ingresar una nueva entrada en el control de cambio de la portada del documento que a continuación se detalla:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha

Con esto se logrará el mantener una traza respecto a las actualizaciones que ha sufrido este documento. Esta nueva versión del documento será almacenada en el sistema documental de Acepta, con su respectivo control de versión, posterior a su aprobación.

Además en caso de existir cambio en la referencia a documentación externa se debe modificar el siguiente cuadro, incorporando este cambio:

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	

7.3 Aprobación

Este documento, así como las modificaciones que él sufra deben ser aprobados por el dueño del documento y en comité de seguridad, a fin de que sea incorporado como la nueva versión vigente al sistema de gestión documental y para posteriormente proceder a su difusión con los empleados y partes externas pertinentes.