ACEPTA

Empresas
a velocidad
digital

PO02

Declaración de Prácticas de Sello de Tiempo

Marzo de 2015

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
Declaración de Prácticas de Sello de Tiempo	1.0	Primera versión	02-03-2015
Declaración de Prácticas de Sello de Tiempo	4.0	Revisión anual	01-10-2016
Declaración de Prácticas de Sello de Tiempo	4.1	Ampliación	03-01-2017
Declaración de Prácticas de Sello de Tiempo	5.0	Revisión anual	01-10-2017
Declaración de Prácticas de Sello de Tiempo	5.1	Ajustes Jurisprudencia	02-04-2018
Declaración de Prácticas de Sello de Tiempo	6.0	Revisión anual	01-10-2018
Declaración de Prácticas de Sello de Tiempo	7.0	Revisión anual	01-10-2019
Declaración de Prácticas de Sello de Tiempo	8.0	Revisión anual	01-10-2020

Declaración de Prácticas de Sello de Tiempo	8.1	Se agrega punto 4.1, Circunstancias de Revocación de la llave de firma TSU e invalidez de los TST emitidos	29-11-2021
Declaración de Prácticas de Sello de Tiempo	9.0	Revisión anual	15-03-2022
Declaración de Prácticas de Sello de Tiempo	10.0	Revisión anual	15-03-2023
Declaración de Prácticas de Sello de Tiempo	10.1	Ajuste punto 1.5	03-07-2023
Declaración de Prácticas de Sello de Tiempo	10.2	Ajustes producto de IAO 2023, en el que se incorporan puntos: • 3.2.7 Deberes y procedimientos para emitir/revocar/suspender/renovar certificados de sello de tiempo • 3.2.8 Sobre la expiración de los certificados • 3.3.3 Procedimiento de Registro	28-09-2023
Declaración de Prácticas 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.

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

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Política de privacidad	Política de privacidad.doc
control de cambio	Procedimiento gestión del cambio.doc
normativa de redes	Normativa de uso de servicios de red
paso a producción	Procedimientos de pasos a producción (carpeta)
adquisición de nuevos componentes	Normativa de adquisición de nuevos componentes.doc
TB01-Estructura de Certifica	TB01.docx
Documentos Externos	
Ley N° 19.799*"ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma".* 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". Ley 19.496 "sobre protección de los derechos de los consumidores". Guía de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación "Servicio de Certificación de Sello de Tiempo". *ISO 27001.* *ISO 27002.*	

ÍNDICE

1 Introducción

1.1 Presentación

En el siguiente documento se presenta la declaración de "Prácticas de sello de tiempo" para la emisión de sello de tiempo de Acepta. Estas son una descripción detallada de los procedimientos o prácticas que Acepta declara convenir en la prestación de sus servicios de sello de tiempo, cuando emite y gestiona en su rol de Autoridad de sello de tiempo (TSA).

Es así como la presente Declaración de Prácticas de sello de tiempo, detalla las normas y condiciones de los servicios de sello de tiempo, que están relacionados con requisitos para la sincronización del tiempo, el sistema de emisión de los sellos de tiempo y otros requerimientos específicos para el proceso. También se describen las medidas de seguridad técnica, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados de sello de tiempo, así como el asegurar que el proceso de certificación es llevado a cabo en un ambiente seguro y que puede dar total confianza a los usuarios de la calidad de los sellos de tiempo y servicios anexos proporcionados por Acepta.

Esta Declaración de Prácticas de sello de tiempo constituye el marco general de normas aplicables a toda la actividad certificadora Acepta, actuando como Autoridad de sello de tiempo (TSA), siendo este documento un complemento a las Políticas de Sello de Tiempo de Acepta.

Cabe indicar que la presente Declaración de Prácticas 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 *"Electronic 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 Prácticas de Sello de Tiempo

Las prácticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los servicios que provee Acepta, que como antes se ha mencionado incluyen 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 prácticas 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 provistos por Acepta.

1.1.2 Alcance

El alcance de la Declaración de Prácticas de Sello de Tiempo detalla las normas y condiciones de los servicios que presta Acepta para la emisión de los mismos.

1.1.3 Referencias

La presente Declaración de Prácticas 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 *"Electronic 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)".*

De manera complementaria a los documentos indicados, se ha utilizado el documento de nombre "Guías de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo, versión 1.1", entregados por el Ministerio de Economía del Gobierno de Chile, como parte del proceso de acreditación.

1.2 Identificación

El presente documento se denomina "Prácticas de Sello de Tiempo de Acepta", las que internamente se citan como Prácticas de Sello de Tiempo y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.201. Este documento se encuentra disponible, en forma pública, en https://sovos.com/es/politicas-y-practicas/.

Acepta tiene el identificador (OID) 1.3.6.1.4.1.6891 el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

Las políticas de las CPS y de cada tipo de certificado están registradas con un número único internacional, llamado ObjectIdentifier (OID). La siguiente tabla resume todos los OID administrados por Acepta:

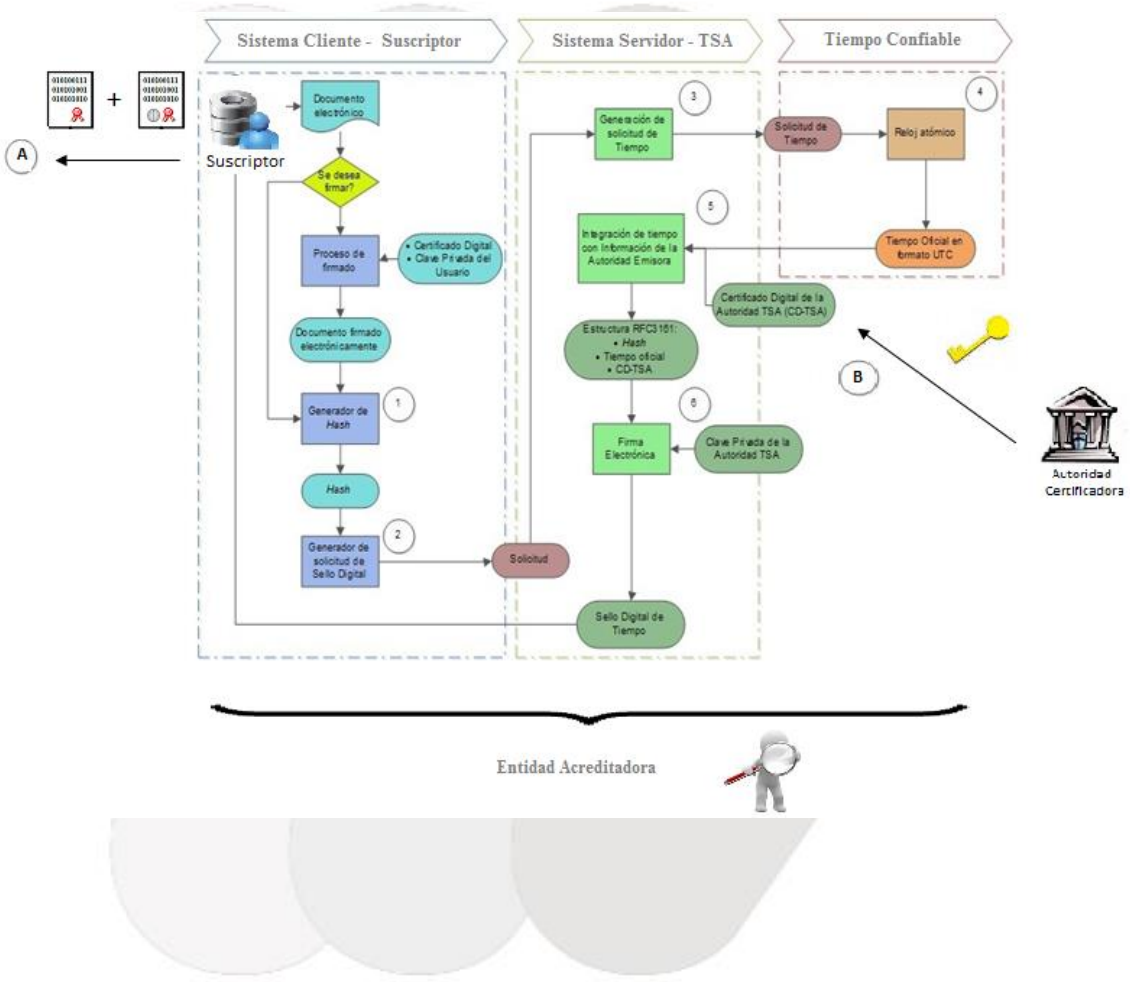
Descripción	OID
Prácticas de Certificación	1.3.6.1.4.1.6891.1
Políticas de certificados Clase 3	1.3.6.1.4.1.6891.2
Políticas de certificados de Firma Electrónica Avanzada	1.3.6.1.4.1.6891.3
Políticas de certificados de Sitio Web	1.3.6.1.4.1.6891.4
Extensión para indicar declaraciones del titular de un certificado X.509	1.3.6.1.4.1.6891.9
Extensión para certificados X.509 en la que se incluye el XML de un CAF.	1.3.6.1.4.1.6891.50.1
Identificador permanente administrado por Acepta para nombrar Servidores.	1.3.6.1.4.1.6891.100.1
Identificador permanente administrado por Acepta para nombrar Servicios.	1.3.6.1.4.1.6891.100.2
Políticas de Sello de Tiempo	1.3.6.1.4.1.6891.200
Prácticas de Sello de Tiempo	1.3.6.1.4.1.6891.201

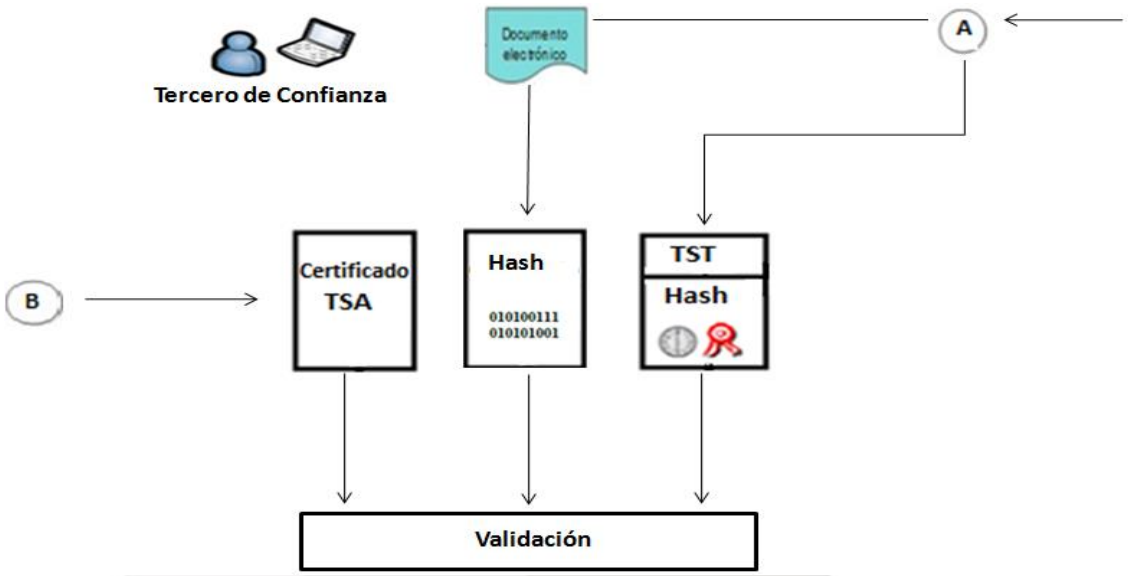
1.3 Comunidad de usuarios y aplicabilidad

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.

Estos tienen como objetivo cumplir con los requerimientos por largos periodos de validez y poseen las características para garantizar no repudio en los procesos que requiera la certificación del tiempo.

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 d 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 prácticas de sello de tiempo declaradas por 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 Ministerio de Economía en el caso de Chile. Para los certificados válidos en el ámbito tributario la entidad acreditadora es el Servicio de Impuestos Internos en Chile y para los certificados de sitio Web Acepta trabaja sin una entidad acreditadora.

1.3.2 Aplicabilidad de los certificados

Los sellos de tiempo emitidos por Acepta se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Prácticas de Certificación, en las correspondientes Políticas de Certificación de Sello de Tiempo, y en concordancia con la normativa vigente.

1.3.2.1 Uso

El uso de los sellos de tiempo aquí descrito, está acotado a generar un certificado el cual contenga el resumen del documento, la hora obtenida desde de una fuente confiable - usada en la generación del sello de tiempo - así como la firma de la TSA que lo emite. El conjunto de estos elementos permiten demostrar que una serie de datos han existido y no han sido alterados desde un instante de tiempo específico y confiable.

Las normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denomina "Política de certificación 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 tengan establecida en este documento y en las correspondientes Políticas de sello 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 las políticas de sello de tiempo, definidas por Acepta, en cada uno de los sellos de tiempo emitidos. Acepta es periódicamente inspeccionada por la Entidad Acreditadora a fin de asegurar la correcta implantación de las prácticas de certificación definidas para la TSA, del cumplimiento de las obligaciones descritas en este documento para cada una de las partes, así como el haber cumplido con la implementación de los controles y procedimientos identificados en la política para garantizar la confianza en los sellos de tiempo que emite. Todo lo anterior se demuestra con el Plan de seguridad, que rige las acciones de Acepta, y en control de su cumplimiento a través de las reuniones periódicas de su Comité de Seguridad.

1.5 Detalle de los contactos y administración de la TSA

Cualquier consulta puede ser realizada al siguiente contacto:

- **Nombre**: Acepta.com S.p.A.
- **Dirección**: Enrique Foster Sur N°20 piso 5, Las Condes, Santiago de Chile
- **Portal de Clientes**: https://acepta.portalbeaware.com/login
    - Cree su cuenta con su Nombre, apellido, RUT y mail
    - Recibirá mail de confirmación
    - Una vez confirmado el mail, recibirá su clave
    - Ingrese su caso ingresando con su mail y clave registradas

- **Número telefónico:** (+56-2) 24968100
- **Autoservicio de asistencia:** https://asistencia.acepta.com/

1.6 Definiciones y Acrónimos

El alcance de las definiciones del documento de Prácticas de Certificación 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 Stamp Protocol (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

- 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 la política, así como en la presente Declaración de Prácticas de sello de tiempo. Para ello Acepta declara que ha desarrollado:
  - Un análisis de riesgo de sus activos
  - Un sistema de SGSI (Sistema de Gestión de Seguridad de la Información) a fin de mitigar los riesgos previamente detectados
  - Un seguimiento de la implantación de las medidas y controles propuestos por el SGSI
- Definir en sus prácticas y política de sello de tiempo las obligaciones de los distintos actores del proceso.
- Realizar una revisión periódica de las prácticas aquí descritas.
- Mantener actualizada estas prácticas y contar con la aprobación formal, ante cambios en las mismas, por parte del Comité de Seguridad.
- Proveer a todos los suscriptores y terceros de confianza, por medio de su sitio web https://sovos.com/es/politicas-y-practicas/ de:
  - La información de contacto.
  - La política, la declaración de prácticas y los documentos relacionados a los servicios de sello de tiempo, garantizando el acceso a la versión final de los documentos mencionados.
  - El algoritmo de hash utilizado como parte de las mismas políticas y prácticas publicadas.
  - La vigencia de la raíz utilizada para la firma de sus sellos de tiempo.
  - La precisión del tiempo utilizado como parte de las mismas políticas y prácticas publicadas.
  - Las prohibiciones de uso de sus sellos de tiempo, como parte de las mismas políticas y prácticas publicadas.
  - Las obligaciones tanto de los suscriptores como de los terceros de confianza, información contenida en las políticas y prácticas publicadas.
  - Los mecanismo de verificación de los *tokens* emitidos por Acepta.
  - El periodo de permanencia de los log que maneja la TSA.
  - Las leyes, reglamentos y estándares bajo los cuales se regula la actividad de la TSA.
  - Un punto de contacto para presentar sus reclamos o no conformidades al servicio.
  - La resolución de funcionamiento, emitida por la Entidad Acreditadora.
- Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, así como también del hardware criptográfico. Tal como se indica en el punto “Administración del ciclo de vida de la llave”, incluida en este mismo documento.

- Mantener un identificador único, para cada *token* de sello de tiempo emitido, así como el incluir una referencia a la política bajo la cual fue emitido; tal como se indica en el punto "Sello de tiempo" de este documento
- Mantener sincronizado el reloj de la TSU con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.
- Contar con la infraestructura requerida para prestar el servicio de sello de tiempo conforme al nivel de calidad comprometido.
- Mantener los controles de seguridad física, de procedimiento y personales definidos para estos servicios, de acuerdo a lo comprometido en este documento.
- Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de Acepta de acuerdo con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- 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.
- Garantizar mediante revisiones y auditorias que todos los requerimientos de la TSA cumplen con los controles requeridos por la legislación aplicable, las políticas, prácticas y procedimientos internos.

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

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 para el tiempo UTC que está incluido en los sellos se asegura una desviación máxima 1 segundo.
- La TSA de Acepta garantiza un nivel de servicio superior al 95%, sin considerar los procesos de mantenimiento de sistemas y equipos. Los procesos de mantenimiento técnicos son planificados anticipadamente, teniendo una duración determinada y se debe dar aviso a los subscriptores del servicio, utilizando los medios de difusión disponibles.
- La TSA de Acepta garantiza que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo (TSA), a través de su política de privacidad de datos personales disponible en su sitio web.

2.2 Obligaciones del suscriptor

- El suscriptor debe verificar que el *token* de *time-stamping* se ha firmado de manera correcta, confirmando que la llave privada de la TSA que firma dicho *token* se encuentra vigente – a través de la CRL o servicio OCSP - y que no ha sido comprometida.
- Conocer las normas estipuladas en las políticas y prácticas de certificación de sello de tiempo de Acepta, y asentir lo que allí se estipule en forma previa a la emisión de un sello de tiempo.
- Conocer y aceptar el propósito y alcance de un sello de tiempo obtenido en Acepta o en algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por Acepta.

2.3 Obligaciones de partes que confían

- Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Deberá verificar que la llave de la TSA no ha sido comprometida hasta el momento de la verificación, utilizando para ello la CRL publicada por Acepta.

  En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la TSA, se debe verificar que el número de serie del certificado de la TSA no se encuentra en la CRL, o determinar la validez del certificado de la TSA en el momento que se generó el sello.

- Conocer y aceptar el propósito y alcance de un sello de tiempo emitidos por Acepta o algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por Acepta.

- Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado, y/o a los sellos de tiempo emitidos, lo cual puede ser considerado como causa de revocación del mismo.

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.

Los servicios de sellado de tiempo de Acepta no han sido diseñados, autorizados o destinados para su aplicación en transacciones relacionadas con actividades que requieran funcionamiento a prueba de errores, como es el caso de instalaciones nucleares, sistemas de navegación o tráfico aéreo, sistemas de comunicación o de control de armamento, sistemas de equipos médicos o de todo otro sistema digital en que un error pueda conducir a la muerte, a las lesiones de personas, o a daños ambientales. Acepta no será responsable en caso de producirse daños por el uso de sus servicios de sello de tiempo en ámbitos como los indicados en esta cláusula.

Acepta declara que las responsabilidades por ella asumidas en esta declaración de prácticas y en los contratos o acuerdos de suscripción que a ellas se remitan serán aseguradas y reaseguradas conforme a las prácticas que habitualmente se aplican para los seguros de responsabilidad civil, y en concordancia con lo estipulado por la legislación que exista o llegare a existir. En particular la TSA de Acepta cuenta con un seguro en conformidad al artículo 14 de Ley 19799 para Chile. La cobertura señalada no podrá ser invocada directamente por el suscriptor o signatario titular de los sellos de tiempo, a menos que este sea la parte perjudicada. Los límites de responsabilidad a aplicar en cada sello se señalan en las políticas y prácticas de sello de tiempo correspondientes.

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° 19.799 (Chile), 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° 19.628 (Chile) relativas a la protección de datos personales o en la Ley 19.496 (Chile), sobre protección de los derechos de los consumidores. 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.

2.4.3 Fuerza Mayor

Acepta queda exenta de responsabilidad en caso de pérdida o perjuicio, en los servicios que presta, producto de:

- Guerra, desastres naturales o cualquier otro caso de fuerza mayor.

Los cuales le hagan imposible proveer los servicios de *time-stamping* de acuerdo a lo definido y publicado en sus políticas y prácticas de certificación.

3 Requerimientos en prácticas de la TSA

3.1 Prácticas y declaraciones de divulgación

3.1.1 Declaración de prácticas de TSA

La TSA de Acepta, a partir del análisis de riesgo aplicado al servicio de la TSA, ha generado una planificación orientada a mitigar los riesgos detectados, a través de un Sistema de Gestión de Seguridad de la Información (SGSI); el cual es controlado y aprobado formalmente por el comité de seguridad de Acepta. Esta planificación se encuentra alineada con las políticas y prácticas que detallan el servicio prestado desde el punto de vista de los actores participantes del proceso, sus obligaciones, del personal a cargo de la prestación del servicio, de los aspectos técnico asociados a dicha prestación, de los aspectos documentales y organizativos así como de los cumplimientos legales que rige la actividad de Acepta como TSA.

3.1.2 Declaración de divulgación de TSA

La presente declaración de prácticas de sello de tiempo detallan la implementación de los controles que son necesarios para cumplir con la política de sellado de tiempo, garantizando fiabilidad y confianza del servicio de sellos. Entre los elementos más relevantes que considera este documento se encuentran:

- La información de contacto.
- Características del servicio de sello de tiempo
- El algoritmo de hash
- La precisión del tiempo
- Las prohibiciones de uso de sus sellos de tiempo
- Las obligaciones tanto de los suscriptores como de los terceros de confianza
- Los mecanismo de verificación de los *tokens* emitidos por Acepta.
- El periodo de permanencia de los log que maneja la TSA.
- Las leyes, reglamentos y estándares bajo los cuales se regula la actividad de la TSA.
- Un punto de contacto para presentar sus reclamos o no conformidades al servicio.
- La resolución de funcionamiento, emitida por la Entidad Acreditadora.

Acepta declara que tendrá a disposición pública, a través de su sitio web, la información relativa a los servicios prestados y formalizados en la Política y declaración de práctica de la TSA. De igual forma como parte de su proceso de Certificación ante la Entidad Acreditadora, Acepta deja a disposición de sus suscriptores como también de los terceros, de la Resolución que aprueba la operación como Autoridad Certificadora de Tiempo emitida por el Ministerio de Economía de Chile.

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_COP.1, y que se evidencia en la documentación asociada al proceso TB01; así mismo cuenta con capacidad de firmar, cifrar y distribuir las llaves tal como se solicita en el criterio común de distribución de llaves criptográficas *CC P2 FCS_CKM.2*.

Para controlar el acceso a la llave privada de Acepta y de sus Autoridades Intermedias, la PSC implementó un sistema criptográfico, basado en el equipo HSM especializado de la marca Thales, modelo NShield N6000 y una aplicación nativa de la marca para realizar operaciones de criptografía contra el equipo, el cual implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

1. **Tarjetas de administración (ACS):** Es un grupo de tarjetas físicas que guardan la llave para encriptar el material criptográfico. Ellas habilita y protege el ambiente completo del sistema.
2. **Tarjetas de operación y protección (OCS):** Es un grupo de tarjetas físicas autorizadas explícitamente para almacenar el material criptográfico, y además restringen el acceso a este material estando este presente físicamente en las tarjetas definidas. Estas tarjetas permitirán a las aplicaciones externas utilizar el sistema para realizar el trabajo de almacenamiento seguro de llaves.

Para acceder a funcionalidades del equipo HSM Thales, sobre el que se ejecutan las operaciones, se utilizan estos medios físicos de protección lógica (ACS y OCS), los que controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la Autoridad Certificadora, bajo las ACS y OCS, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de tarjetas físicas para poder realizar tareas sobre el material criptográfico en el equipo HSM Thales, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 3 de 8 tarjetas.

La llave usada por la TSU de Acepta son generadas de acuerdo a las Políticas y Prácticas definidas para el proceso de Firma Electrónica Avanzada; utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la TSA de Acepta utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, el cual sólo puede ser acezado por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de llaves del equipo HSM.

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.

3.2.2 Protección de la llave privada de la TSU

Acepta lleva a cabo un conjunto de acciones de manera tal de asegurar que la llave privada de la TSU, usada para firmar los sellos de tiempo, permanece de manera confidencial y mantenga su integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3. Cuando la llave privada es respaldada, ella son copiadas, almacenadas y recuperadas sólo por el personal con roles de confianza y bajo un ambiente seguro.

Así, Acepta realiza la protección de las llaves a través de:

- **Módulos criptográficos**: El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los nuevos HSM de Acepta cumplan el criterio FIPS 140-2 Nivel 3 o equivalente.
- **Control multipersona de la llave privada**: Las claves privadas utilizadas por las autoridades de certificación de Acepta y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 3personas de un total de 8 para modificar el ambiente criptográfico.
- **Depósito de la llave privada**: La clave privada está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.
- **Copia de respaldo de la llave privada**: Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la AC (raíz o intermedias) que se puede aplicar en caso de contingencia para la TSA. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- **Introducción de la clave privada en el módulo criptográfico**: Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las entidades de Acepta que hacen uso de dichos módulos.
- **Método de activación de la clave privada**: Las claves privadas de las autoridades de certificación de Acepta y que componen su jerarquías, se activan mediante la inicialización del software de AC y la activación del hardware criptográfico que contiene las claves.
- **Método de desactivación de la clave privada**: Un Administrador puede proceder a la desactivación de la clave privada de las AC de Acepta o de sus claves intermedias (Clave de la TSA), mediante la detención del software de la AC.
- **Método de destrucción de la clave privada**: Existe un procedimiento de destrucción de claves de la AC, así como de las claves intermedias de la jerarquía.

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.

3.2.3 Distribución de la llave pública

El certificado digital utilizado por la TSA de Acepta es generado por la PSC de Acepta, de acuerdo a las políticas y prácticas de certificación inspeccionadas por el Ministerio de Economía de Chile, para esta PKI.

La forma en que se establece la confianza con una TSA - descrita para que un tercero que desee confiar - se basa en la instalación del certificado raíz de la TSU respecto a la cual se desea confiar. Es así que Acepta, como parte de los servicios que provee a sus clientes y terceros, publica en su sitio web los certificados raíces tanto de su propia TSA como de las TSA certificadas ante el Ministerio de Economía de Chile. Estos certificados, se encuentran disponibles en el sitio web de Acepta, a través de una conexión segura (https).

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido firmado por laTSA podrá ser validado por el cliente, ya que el certificado raíz de la TSA contiene la llave ***pública*** que permitirá verificar el sello emitido.

A continuación se presenta la secuencia general del modelo de confianza:

- Se descarga certificado raíz de la TSA que ha emitido el sello a validar. Este certificado debe ser descargado a través de un canal seguro, que debe poseer el sitio de descarga de dicha raíz.
- Descargado el certificado raíz, este se procede a instalar en el repositorio de entidades emisoras raíz de confianza del equipo cliente.
- El sistema indicará si la importación e instalación del certificado ha sido correcta. De ser así, cualquier mensaje que sea firmado con un certificado de sello de tiempo, que ha sido emitido y firmado con esta raíz, podrá ser validado automáticamente en el equipo cliente. Una forma de validación adicional de esta instalación, es verificar si el almacén de raíces de confianza incluye a este certificado recién instalado.

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido emitido y firmado por esta TSA podrá ser validado por el cliente, ya que el certificado raíz de la TSA contiene la llave pública que permitirá verificar el certificado emitido. Una forma de complementar esta cadena de confianza, es instalar además del certificado raíz de la TSU (raíz intermedia de la PSC), el certificado raíz de la PSC utilizado para firmar el certificado de la TSU.

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.

3.2.5 Termino del ciclo de vida de la llave del TSU

La llave privada de la TSU será reemplazada al momento de su expiración. La TSU rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida.

La TSA de Acepta tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que Acepta vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo: suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas.

Acepta comunicará a cada uno de sus suscriptores del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los suscriptores, los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

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 equipos HSM con que cuenta Acepta y que son usados para firmar el certificado utilizado por la TSU para la firma de sus sellos de tiempo; así como para la firma de los mismos sellos de tiempo, cuenta con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión. Así mismo, para evitar la intrusión de dispositivos en el hardware del módulo de seguridad, este dispositivo se coloca en la parte posterior a los ventiladores del HSM. El equipo HSM posee varios niveles de detección de intrusión física a la funcionalidad criptográfica, informando estos eventos al administrador y en último caso obligando a reiniciar el equipo a sus condiciones de salida de fábrica. Los eventos antes mencionados son desplegados en la pantalla del equipo.

Ante la detección de los eventos que se indican previamente, no se debe poner en producción dicho equipo, ya sea que los eventos se han producido durante el almacenamiento o transporte del equipo. El administrador de dicho equipo debe proceder a reiniciar el equipo a sus condiciones de salida de fábrica. Posterior a esto, se debe reconectar el equipo así como recuperar la información clave del equipo, haciendo uso del quórum que otorgan el set de tarjetas de administración definidas.

En particular si se ha detectado apertura de la tapa del equipo, este genera un evento indicando dicha intrusión, lo que implica que la seguridad del equipo se ha comprometido. Bajo este escenario no se debe pasar a producción dicho equipamiento bajo motivo alguno.

Si el evento indicado, se produce durante el transito del equipo desde el fabricante de dicho equipo, el administrador debe contactarse inmediatamente con el fabricante. En cambio de ocurrir este evento posterior a la instalación, adicionalmente se deben revisar las políticas y procedimientos de seguridad que permitieron dicho incidente.

Entre las revisiones que deben realizarse al equipo, tanto posterior a su transporte o durante su almacenamiento es:

- Controlar que los sellos de seguridad no han sido alterados.
- Que las tapas permanecen completamente ajustadas al chasis del equipo.
- Que no se presentan daños aparentes a la estructura general del equipo.
- Que no se detecten daños evidentes en ventilaciones del equipo o que se haya intentado introducir algún componente a través de estos espacios.

3.2.6.2 Administración del HW Criptográfico

El equipo HSM utilizado por Acepta tanto para su PSC como TSA, implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

1. **Tarjetas de administración (ACS):** Es un grupo de tarjetas físicas que guardan la llave para encriptar el material criptográfico. Ellas habilitan y protegen el ambiente completo del sistema.
2. **Tarjetas de operación y protección (OCS):** Es un grupo de tarjetas físicas autorizadas explícitamente para almacenar el material criptográfico, y además restringen el acceso a este material estando este presente físicamente en las tarjetas definidas. Estas tarjetas permitirán a las aplicaciones externas utilizar el sistema para realizar el trabajo de almacenamiento seguro de llaves.

Para acceder a funcionalidades del equipo HSM Thales, sobre el que se ejecutan las operaciones de instalación, respaldo y recuperación, se utilizan estos medios físicos de protección lógica (ACS y OCS), los que controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la Autoridad Certificadora, utilizada para la generación del certificado de la TSU, bajo las ACS y OCS, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de tarjetas físicas para poder realizar tareas en el equipo HSM Thales sobre el material criptográfico, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 3 de 8 tarjetas.

Una vez instalado de manera exitosa el hardware y software asociado al HSM, Acepta ha definido como criterio de verificación del correcto funcionamiento de los equipos, la emisión de un certificado de prueba, partiendo desde su solicitud hasta su emisión y a continuación la revocación del mismo. Con este ciclo se probará la correcta generación de claves, servicios OCSP y listas de revocación de certificados. Una vez desarrollada esta actividad, se podrá proceder a generar las llaves intermedias utilizadas por los distintos servicios de la PSC, en particular para este caso, la llave de la TSU utilizada para la firma de los sellos de tiempo a emitir

Finalmente, en caso de requerir mover el equipo a otra instalación o el envío del mismo a la fábrica por motivos de garantía, Acepta ha definido que se debe dejar el equipo a sus condiciones originales que tenía a la salida de fábrica, borrando con ello todo su contenido de configuraciones interna del equipo HSM. En particular, para el caso de equipos Thales, esto se puede realizar a través del menú de opciones de administración, opción *"factory state"*. Esto llevará a que el equipo borre todo su contenido. Lo anterior no afectará el *security world data* almacenada en el RFS, por tanto en caso de no existir intrusión, el contenido de dicho equipo puede ser restaurado a partir de esta data más las llaves ACS y el quórum definido.

3.2.7 Deberes y procedimientos para emitir/revocar/suspender/renovar certificados de sello de tiempo

A continuación se definen los deberes y procedimientos asociados al ciclo de vida de los sellos de tiempo:

- **Emisión**: Al ser parte del Proceso de Acreditación definido por el Regulador, hacen que el procedimiento de registro de los solicitantes, que incluye su autenticación y verificación de identidad, es realizada en forma y de acuerdo con los niveles de protección requeridos, ello bajo lo detallado en las Prácticas de Certificación de Firma Electrónica Avanzada en su capítulo 4
- **Revocación**: La llave privada de la TSU debe ser reemplazada al momento de su expiración o ante un evento de seguridad que vulnere dicha llave, lo que lleva a una revocación de la misma. La TSU de Acepta rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado o se haya revocado. Después de expirada o revocada, la llave privada es destruida al igual que sus copias de respaldo, a fin de que su clave privada no pueda ser recuperada.
- **Suspensión**: Cuando sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempo o por cualquiera de las fuentes fiables mencionadas, el token de sello de tiempo no será emitido, y se suspenderá el proceso hasta contar con un tiempo correcto. Además, para la administración del reloj de la TSU requiere de un quórum de 3 de 8 tarjetas
- **Renovación**: 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 renovada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable o que se haya vulnerado dicho certificado.

3.2.8 Sobre la expiración de los certificados

El certificado TSU usado para firma con sello de tiempo, tiene una vigencia de 20 años a contar de su emisión, pudiéndose revocar anticipadamente antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable o que se haya vulnerado dicho certificado. Al revocarse este certificado de firma de sellos de tiempo, pasan a ser inválidos todo sello de tiempo emitido con dicho certificado de firma de sello de tiempo revocado.

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 una fecha y hora proveniente de una fuente confiable de tiempo. En particular cada sello de tiempo TST incluye, de acuerdo al estándar RFC3161 lo siguiente:

- 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
- 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.

3.3.2 Sincronización de los relojes con UTC

En Acepta la TSA utiliza una fuente fiable de tiempo, mediante un servidor NTP que se sincroniza 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*", el cual provee tiempo UTC(k); lo anterior con una desviación máxima de 1 segundo. Esta fuente de tiempo está basada en el protocolo NTP (*Network Time Protocol*) haciendo que la exactitud no disminuya por debajo de los requerimientos.

De manera más específica:

- La calibración de la TSU es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la TSU se encuentra protegido contra amenazas ambientales que puedan afectar su precisión fuera del rango declarado.
- En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la TSA.
- En caso de detectarse una desviación más allá de la precisión declarada, la TSU no generará nuevos TST hasta que el tiempo correcto es restaurado.
- Acepta declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el TST.
- La administración del reloj de la TSU requiere de un quórum de 3 de 8.

3.3.3 Procedimiento de Registro

Los sellos de tiempo, al ser parte del Proceso de Acreditación definido por el Regulador, hacen que el procedimiento de registro de los solicitantes, que incluye su autenticación y verificación de identidad, es realizada en forma y de acuerdo con los niveles de protección requeridos, ello bajo lo detallado en las Prácticas de Certificación de Firma Electrónica Avanzada en su capítulo 4.

3.4 Gestión de la TSA y operaciones

3.4.1 Gestión de la seguridad

La TSA de Acepta desarrolla una administración activa de la seguridad a través de desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI), el que considera las mejores prácticas y estándares de la industria. Este Sistema de Gestión se basa en un análisis de riesgo desarrollado por la TSA de Acepta, a fin de detectar sus brechas de seguridad y planificar las mitigaciones de las mismas a través de un plan de trabajo que incluye medidas documentales, técnicas y organizativas. 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:

- Acepta declara que su TSA es responsable por todo los aspectos asociados a la provisión de servicios de sello de tiempo
- Todo su personal tienen acceso a sus prácticas y políticas de sello de tiempo.
- Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
- 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; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación.
- Acepta declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Ministerio de Economía de Chile.
- La TSA de Acepta no subcontrata los servicios de sello de tiempo.

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 MAGERIT y utilizando para ello la herramienta PILAR, ambos elementos basados en la norma ISO 27001. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA de Acepta generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente. Para el cumplimiento de este plan, así como su seguimiento, 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 su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Ministerio de Economía.

3.4.3 Seguridad del personal

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

3.4.3.2 Comprobación de antecedentes

Mediante CV y entrevistas realizadas al momento de la vinculación.

3.4.3.3 Roles de confianza

- **Oficial de seguridad:** es responsable de la administración e implementación de las prácticas de seguridad.
- **Administrador de Sistemas:** está autorizado a instalar, configurar y mantener los sistemas de confianza de la TSA, para la administración de sello de tiempo, Además es responsable por la operación de los sistemas y autorizado para realizar el respaldo y recuperación.
- **Administrador de Seguridad**. Es el encargado de verificar la mantención de los sistemas de confianza de la TSA.
- **Auditor:** es el encargo de revisar archivos y log de auditoría de la TSA.

3.4.3.4 Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que Acepta ha trabajado, se considera para el personal asociado a la TSA, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de Acepta para la PSC de Acepta. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

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 del Reglamento Interno, el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones del cargo.

3.4.3.7 Requerimientos de contratación

Como parte del contrato, todo trabajador de la PSC, firma un acuerdo de confidencialidad, el cual se detalla a continuación:

"El TRABAJADOR se obliga en este acto y por el presente instrumento a mantener la más absoluta y total confidencialidad y reserva de toda información que pueda llegar a su conocimiento, de forma directa o indirecta, relativa a los negocios, clientes y/o actividades particulares o generales de ACEPTA.COM S.A., en específico respecto de aquellos datos personales que sean objeto de

procesamiento o tratamiento por ACEPTA.COM S.A. como asimismo sobre cualesquiera otros datos y antecedentes relacionados con dichas bases de datos, estándole en consecuencia prohibido reproducir, transmitir, comentar y en general hacer cualquier uso de esa información para beneficio propio o de terceros.

La infracción de esta obligación será considerada siempre un incumplimiento grave por parte del trabajador a las obligaciones que le impone el contrato, sin perjuicio de las acciones civiles y/o penales a que dicho incumplimiento pueda dar lugar."

3.4.3.8 Documentación entregada al personal

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

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad
- Política de Seguridad de la Información
- Organigrama y funciones del personal

Adicionalmente, se facilitará el acceso a la documentación técnica necesaria para llevar a cabo sus funciones.

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

El oficial de seguridad con el apoyo del área de sistemas y RRHH, procederá a:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización
- Suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización
- Supresión de acceso a toda información, a excepción de la considerada PÚBLICA
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios.
- Informar a los proveedores y entidades externas a Acepta la marcha de individuo y de que ya no representa a la TSA de Acepta.
- Verificar la devolución del material proporcionado por la Acepta. Por ejemplo:
    - Equipo computacional
    - Llaves mobiliario oficinas
    - Teléfono móvil
    - etc.

3.4.4 Seguridad física y ambiental

Acepta en su calidad de PSC y TSA, opera en un par de *Datacenter* seguros y confiables bajo certificación ISO 27001, estando sus servicios en acuerdo a estas prácticas de certificación como también de acuerdo a la norma ETSI TS 102.023.

Específicamente la TSA de Acepta cumple con los puntos más abajo indicados

3.4.4.1 Emisión de sellos de tiempo, así como su administración

a) Los accesos físicos solo son limitado al personal autorizado y relacionados al servicio de sello de tiempo.
b) El plan SGSI implementa un conjunto de controles a fin de evitar la pérdida de información, o el compromiso de la continuidad operacional por falla de alguno de los componentes que participan del proceso. Por esto mismo Acepta cuenta con un plan de continuidad operacional tanto para su PSC con TSA, los cuales son probados periódicamente a fin de verificar su operación, así como para realizar mejoras que podrían resultar de estos simulacros.
c) El plan SGSI implementa controles a fin de evitar la pérdida de información de la TSA; controles que son auditados mensualmente en su cumplimiento.

3.4.4.2 Control de los módulos criptográficos

Acepta mantiene los controles de sus módulos criptográficos tanto para la generación de la llave así como la protección de las mismas tal como se indican en la "Gestión del ciclo de vida de las llaves" de este mismo documento.

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 Certificados, se encuentra alojado en un Sitio Principal y uno secundario. Las características generales del recinto Principal comprenden una Zonificación en Alta Criticidad (Sitio de Producción) y una Zona de Media Criticidad(recintos de Operaciones y Cintoteca).

- Zona Alta Criticidad: Sitio de Producción:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio.
  - Acceso restringido.
  - Sistema de video vigilancia.
  - Piso falso de 30cm de altura con cámara plena para distribución de aire para climatización de todos los equipos de la sala.
  - Acceso por rutas físicas redundantes para fibras ópticas carriers.
  - Equipos de Climatización precisa redundantes en configuración 1+1.
  - Equipos de energía ininterrumpida UPS redundantes en configuración1+1. La iluminación de la sala se encuentra respaldada por el sistema UPS y el grupo electrógeno.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Soporte generación autónoma de energía de emergencia mediante Grupo Electrógeno de operación continua. Todos los equipos están respaldados.

- Zona Criticidad Media: Operaciones:
  - Espacio cerrado de oficinas dotado de puestos de trabajo para personal operación y administración.
  - Acceso restringido mediante tarjeta magnética u botonera con clave.
  - Sistema de Video Vigilancia.
  - Iluminación y puestos de trabajo respaldados por el grupo electrógeno.
- Zona Criticidad Media: Cintoteca:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio, alejado del Sitio de Producción.
  - Puerta de acceso corta fuego y de seguridad.
  - Acceso restringido mediante cerradura de seguridad.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Iluminación respaldada con grupo electrógeno.

Respecto al sitio secundario sus principales características son:

- Acceso restringido y controlado.
- Climatización full redundante calculada de acuerdo a la carga térmica de la sala.
- Alimentación del sistema eléctrico independiente de otros consumos propios del lugar en que se encuentra ubicado el sitio secundario.
- Sistema de respaldados con UPS redundante y grupo electrógeno.
- Sistema de detección temprana de incendio y extinción vía agente limpio FM-200.
- Sistema de detección de sobre temperatura para monitorear permanentemente el funcionamiento del sistema de Aire Acondicionado.
- Sistema de detección de intrusos.
- Acceso por rutas físicas redundantes para fibras ópticas carriers.
- Acceso a través de una puerta cortafuego de características para resistencia al fuego F-60.
- Sistemas de Circuito Cerrado de Televisión.

Todo esto, conforme a la normativa ISO 27001. Los certificado que avalan la acreditación 27001 de ambos sitios, se encuentran actualmente en repositorio Documental Alfresco.

Por otra parte, el edificio donde se encuentran la Casa Matriz de Acepta, cuenta con accesos vigilados por un circuito cerrado de cámaras de seguridad, sensores de intrusión para controlar y detectar el acceso a áreas restringidas y guardias en la entrada del edificio, con lo cual se pretende mantener un control de acceso mínimo a las instalaciones.

Adicionalmente, en estas dependencias podemos encontrar:

- Entradas cerradas con un sistema de ingreso dactilar.
- Área de recepción atendida por personal.
- Control de acceso a visitas.

A través de estas medidas se mantiene un perímetro de seguridad que restringe el acceso sólo a personal autorizado.

3.4.4.3.1.1 Seguridad Física Data Center

Los sistemas de Acepta, como Entidad de Certificación, se encuentran alojados en un Sitio Principal y uno secundario. Ambos sitios cuentan con niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos sitios cuentan con diversos perímetros de seguridad, diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico, sistemas de video vigilancia y de grabación, de detección de intrusiones entre otros.

Los sitios además cuentan con un sistema central de vigilancia mediante circuito cerrado de televisión, distribuidas en lugares estratégicos del piso, las que permanentemente están grabando las actividades y registrando los accesos de personas a lugares que requieren acceso restringido. El centro de control es monitoreado por guardias de seguridad las 24 horas del día, todos los días de la semana, lo que permite llevar un registro y control total de acceso.

Se ha reforzado el control del ingreso a áreas de alta seguridad, como es el área de servidores, a través de la instalación de puertas reforzadas que permanecen constantemente cerradas y que sólo pueden ser abiertas por personas previamente autorizadas por la Gerencia del CGSI, bajo la estrecha supervisión de Guardias de Seguridad.

Los controles definidos en ambos sitios, 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.

3.4.4.3.1.2 Sistema de Energía Eléctrica

El suministro eléctrico para el sitio principal está garantizado a través de diversas alternativas que operan en forma concurrente. En particular, el sitio principal se ubica en el llamado Anillo Protegido del microcentro de Santiago, el cual cuenta con múltiples alimentadores que aseguran la disponibilidad de energía eléctrica. Adicional a esto, se han incorporado la instalación de un grupo electrógeno dimensionado para proporcionar energía eléctrica a todas las instalaciones del sitio ante fallas de los proveedores de energía. Todo el sistema de suministro eléctrico está reforzado por una serie de UPS's instaladas en cascada, que garantizan la operación por un tiempo más que suficiente para activar el generador y asegurar la continuidad del servicio. También se cuenta con tableros eléctricos redundantes de modo de asegurar el funcionamiento antes fallas de la distribución de los equipos.

Respecto al sitio secundario, sus instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. En resumen ambos sitios cuentan con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación por largos periodos de tiempo.

3.4.4.3.1.3 Sistema de Control Ambiental

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. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Ambos cuentan además con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

3.4.4.3.1.4 Sistema de Extinción y Control de Incendios

Dado los riesgos de incendio a que pueden estar sujetos los sitios, es que tanto el sitio principal como el secundario cuentan 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

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de Acepta, es que se ha diseñado en ambos sitios una plataforma robusta, segura y escalable, utilizando como base para ello los servicios WAN, estos servicios provistos por los principales carriers del país, nos aseguran, redes confiables y con tecnología de última generación.

El objetivo principal de este diseño es cumplir con los niveles de servicio comprometidos por Acepta, por lo que se contempla respaldos en todos los puntos críticos. Adicionalmente, cabe destacar que las redes de transporte del carrier están diseñadas para entregar una alta disponibilidad, comuna arquitectura redundante interna, lo cual permite garantizar el servicio de conectividad sobre su red.

3.4.4.3.1.6 Seguridad Lógica Data Center

Ambos sitios cuentan los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

3.4.5 Gestión de las operaciones

La TSA de Acepta asegura que su sistema y componentes son seguros y se encuentran operados de manera correcta, con un riesgo mínimo de falla.

Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado. Lo anterior a través de la aplicación de normativas de desarrollo de aplicaciones, protección de malware, adquisición de nuevos componentes y procedimiento de paso a producción.

- **Manejo de medios y seguridad:** 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 MAGERIT y utilizando para ello la herramienta PILAR, ambos elementos basados en la norma ISO 27001. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA de Acepta generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente. Para el cumplimiento de este plan, así como su seguimiento, 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 su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Ministerio de Economía de Chile.
- **Planificación de la capacidad:** El manejo de la capacidad para la demanda es monitoreado y proyectado de acuerdo a los futuros requerimientos, de manera que la capacidad de proceso como de almacenamiento siempre sean las adecuadas. Acepta cuenta con un documento de Gestión de Capacidad, cuyo objetivo es definir la provisión de recursos y servicios de manera óptima y efectiva en costos de manera de que ellos calcen con la demanda de los clientes presentes y futuros que Acepta atiende. Este proceso ayuda a identificar y reducir las ineficiencias asociadas con la sub utilización de los recursos, niveles de demanda no satisfechas por Acepta así como el proveer los niveles de servicio comprometidos de una manera eficiente en costos. Es así como la mantención y ejecución de lo descrito por este documento, ayuda a asegurar que todo componente de la infraestructura sean capaces de desarrollar todas las funciones que de ellos se esperan de la manera más eficiente que sea posible.
- **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, de una manera que permite el que se realicen las acciones correctivas oportunas, documentadas y estructuradas para resolver estos incidentes en el menor tiempo posible.

  La gestión de incidentes en Acepta, a través de su mesa de ayuda, proporciona el punto único de contacto entre Acepta y sus clientes, actuando como interfaz entre los usuarios y las funciones de TI y también como filtro para asegurar que todos los miembros de los equipos de Acepta puedan completar su trabajo en una forma estructurada.

  El sistema de gestión de incidentes, adicional a los incidentes de seguridad, permite la recepción de los reportes de fallas y consultas que afectan el normal funcionamiento de los servicios asociados al proceso de emisión de certificados, así como el canal para la recepción de solicitudes de mantenimiento correctivo, preventivo y perfectivo de las aplicaciones, y también la creación, modificación y eliminación de cuentas de usuarios para las aplicaciones, etc.

En este documento, que describe la gestión de incidentes de seguridad en Acepta, se ha estructurado siguiendo los lineamientos planteados tanto en el Anexo Guías de Evaluación Procedimientos de Acreditación v2.1 la cual tiene como referencia la ISO 27002 como, a la vez, la norma ISO 27035 Técnicas de seguridad y Gestión de incidentes de seguridad de la información (antigua ISO 18044) la cual identifica como contenido los siguientes pasos:

- Alcance en la gestión de incidentes: Activos (Procesos o Servicios) que van a ser gestionados a través del sistema de gestión de incidentes.
- Definición de los Niveles de Falla.
- Roles, responsabilidades y estrategias de comunicación y de contacto en caso de un incidente.
- Reporte de eventos de seguridad de la información
  - Procedimiento General de gestión del incidente, incluyendo:
    - Reconocimiento del incidente
    - Recepción de caso
    - Registro de caso en formulario estándar formal
    - Análisis del incidente
    - Resolución del incidente
    - Cierre del incidente (retroalimentaciones, registros de causas y soluciones)
  - Niveles de escalamiento y tiempos de respuesta
- Reporte de debilidades de seguridad de la información
  - Procedimiento General de Reporte de debilidades, incluyendo:
    - Reconocimiento de debilidad
    - Recepción de caso
    - Registro de caso en formulario estándar formal
    - Análisis de la debilidad
    - Resolución de la debilidad de corresponder
    - Cierre (retroalimentaciones, registros de causas y soluciones)
  - Niveles de escalamiento y tiempos de respuesta
- La gestión de incidentes y mejoras en la seguridad de la información
  - Roles y responsabilidades
  - Procedimiento
  - Registro de evidencias
  - Registro de acciones tomadas
  - Aprender de los incidentes de la seguridad de la información
    - Indicadores (KPI) de gestión de incidentes
- Pruebas del plan de gestión de incidentes
  - Periodicidad de ejercicios
  - Mantención del plan
    - Tipos de cambios a considerar
    - Actividades de mantención
    - Periodicidad de mantención
    - Resultados finales
  - Revisión del plan
- La gestión de incidentes
  - Sensibilización
    - Capacitación
  - Monitoreo

- **Procedimientos operacionales y responsabilidades**: La operación del servicio de Sello de Tiempo de la TSA de Acepta opera de manera independiente de otros servicios provistos por la PSC: estas operaciones son desarrolladas por personal confiable definida en la estructura de la PSC de Acepta y sus Prácticas de Certificación. Dentro de los roles de confianza se tiene:
    - Administrador de Sistemas: A cargo de
        - La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos.
        - Activar los servicios de la TSA
        - Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.
        - Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas.
        - Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación.
    - Administrador de Seguridad
        - Debe cumplir y hacer cumplir las políticas de seguridad de Acepta, y debe encargarse de cualquier aspecto relativo a la seguridad de la TSA Acepta, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Esta función estará soportada a través de una oficina de seguridad técnica, además del oficial de seguridad.
    - Responsable de formación, soporte y comunicación
        - Se encarga del mantenimiento de contenidos de la web de Acepta.
        - Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la plataforma de la TSA de Acepta.
        - Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los registros de los agentes de Call Center.
        - El Responsable de formación, soporte y comunicación contará con la colaboración de las áreas de RRHH, Marketing o Post venta de estimarse necesario.
    - Responsable de Seguridad
        - Se asigna esta tarea al Comité de Seguridad de la Información de Acepta, asumiendo la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas.
        - Gestionará que los sitios donde se encuentran los sistemas de Acepta, cumplan con gestionar los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

- Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.
- Es responsable de autorizar movimientos de material fuera de las instalaciones del PSC.
- Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de l PSC de Acepta.

- Auditor
  - Encargado de realizar auditorías internas. En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de la TSA de Acepta y su personal. Para esta labor se hará uso de Auditores internos como también la contratación de una auditoría externa anual.
- Responsable de Documentación
  - Se encargará de mantener el repositorio de documentación y los archivos de documentación en papel.
  - Controlará que cada área lleve a cabo la actualización de documentos cuando se requiera.
  - Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación.

3.4.6 Gestión de acceso a los sistemas

La TSA de Acepta, declara y asegura que el acceso a su sistema (hardware, software y datos) sólo está limitado al personal autorizado. En particular, la PSC de Acepta cuenta con:

- Cortafuegos apropiados para proteger la red interna de accesos no autorizados incluyendo a suscriptores y terceros que confían. El documento guía para este compromiso son la "Normativa de uso de los servicios de red".
- Administración de usuarios, para mantener la seguridad de los sistemas, incluyendo administración de cuentas, logs y modificación o eliminación de accesos. EL documento guía de este compromiso es la "Política de control de acceso lógico".
- Restricciones de acceso a la información y sistemas de aplicación de acuerdo a la política de control de acceso, así como desagregación de funciones en los roles de confianza definidos.
- Un control apropiado del personal autorizado tanto en su identificación como autenticación, previo a tener acceso a las aplicaciones relacionadas con los sellos de tiempo. En particular Acepta cuenta con un inventario de activos, incluyendo los roles y personas que cubren cada rol.
- Logs de las operaciones que realiza el personal para auditorías posteriores

Adicionalmente, los componentes de la red local se mantienen en *Datacenters* bajo ambiente seguro y con una auditoría periódica.

Los administradores de Acepta realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA.

3.4.7 Mantenimiento e implementación de sistemas de confianza

La TSA asegura que sus sistemas y productos están protegidos contra modificaciones no autorizadas. Para ello, la TSA de Acepta y su PSC previo a cualquier cambio en sus sistemas o productos lleva a cabo:

- Un análisis de requerimientos de seguridad es llevado a cabo durante el diseño y especificación de requerimientos. Es así como, cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente las actividades para determinar e implementar los requerimientos de seguridad necesarios. Esto ocurrirá tanto cuando se vaya a adquirir un producto o cuando este se desarrolle internamente; estableciendo igualmente los requerimientos de seguridad que debe cumplir y revisando dicho cumplimiento antes de su compra o desarrollo. Lo anterior se encuentra documentado en la "Política de adquisición de componentes nuevos".
- Un procedimiento de control de cambio para nuevas versiones, modificaciones y/o correcciones de emergencia al software. El propósito de este Procedimiento es establecer las actividades necesarias para llevar a cabo los cambios y actualizaciones en los sistemas de una manera eficiente, incluido las nuevas versiones y los pasos a producción, minimizando el impacto y las incidencias que se puedan producir debido a ellos. Acepta documenta estos pasos a través de su Procedimiento de Gestión de Cambio.
- Respecto a la generación de la llave de la TSA, utilizada por la TSU en la entrega de sus sellos de tiempo TST, siempre es creada en un ambiente seguro tal como se describe en Generación de la llave de la TSU de este mismo documento.

3.4.8 Compromiso de los servicios de TSA

La TSA de Acepta declara que ante cualquier evento de seguridad que afecte sus servicios, incluyendo compromiso de la llave de firma de la TSU o perdida de precisión declarada de su reloj, esto es informado directamente o a través de su sitio web a sus suscriptores y terceros que en ella confía. El PSC de Acepta y en particular su TSA 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 Acepta 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 Acepta no emitirá nuevos TST hasta superar el compromiso declarado.
- Ante perdida de la precisión, compromiso del mismo o sospecha de compromiso en el tiempo de la TSA; Acepta 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 usuario o la seguridad de los servicio de la TSA de Acepta.

3.4.9 Cese de una TSA

La TSA de Acepta tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que Acepta vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo: suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas.

Acepta comunicará a cada uno de sus suscriptores del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los suscriptores, los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

3.4.10 Cumplimiento de requerimientos legales

Acepta como Autoridad de sello de tiempo, actúa en conformidad con la Ley N° 19.799, su reglamento, así como la Ley N° 19.628 relativas a la protección de datos personales, la ley N° 19.496 sobre los derechos de los consumidores y las directrices técnicas establecidas por los organismos calificadores (ETSI, ISO, RFC, etc.). Además su operación se encuentra regulada por la Entidad Acreditadora del Ministerio de Economía de Chile 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, manteniendo la confidencialidad y la integridad de los datos; 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. Acepta usa esta información sólo para los fines que fueron entregados por parte del suscriptor.

La información con data del suscriptor es protegida de divulgación, a menos que sea solicitada por él mismo o por orden judicial u otro requisito legal.

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

La TSA de Acepta mantiene registros de la información relevante, concerniente a su operación. La información personal de los suscriptores, que ha recolectado la PSC de Acepta como parte de su operación, está protegida de acuerdo con la Política de Privacidad de datos personales publicados por Acepta en su sitio web.

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. Lo anterior a fin de proteger la confidencialidad de dichos datos. 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 se encuentra soportada por la PSC de Acepta, la cual se encuentra acreditada en su operación por la Entidad Acreditadora del Ministerio de Economía de Chile. En particular la TSA de Acepta cumple con:

- Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias que contravengan la Ley N° 19.496 sobre los derechos de los consumidores para Chile.
- 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 Chile, respecto a la formación y operación de empresas y personas jurídicas.
- Acepta como parte de su cumplimiento de la Ley 19799 (Chile), articulo 14, cuenta 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 certificada por el Ministerio de Economía en Chile, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continúa de este personal a través de sus planes anuales de capacitación.

- 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

Cuando una parte que confié en los TST emitidos por Acepta requiera chequear su validez, debe asegurar que el certificado de firma de la TSU de Acepta es verdadero (modelo de confianza) y no se encuentra revocado, ya sea a través de la CRL de Acepta o del servicio OCSP que ella provee a sus usuarios externos.

La validez de un TST es cierta sólo para el momento en que se efectúa el chequeo antes mencionado y debe ser verificado si se hace necesario en un tiempo posterior, ya que puede existir un compromiso de la llave privada de la TSU de Acepta.

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

4.1 Circunstancias de Revocación de la llave de firma TSU e invalidez de los TST emitidos

ACEPTA declara que la llave usada por la TSU de Acepta son generadas de acuerdo a las Políticas y Prácticas definidas para el proceso de Firma Electrónica Avanzada; utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la TSA de Acepta utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, el cual sólo puede ser acezado por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de llaves del equipo HSM.

La TSA de Acepta tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por las siguientes circunstancias:

- Un evento de seguridad que vulnere a la llave de la TSU
- Por un cese de actividades.
- Por requerimiento del titular (en este caso ACEPTA como dueño del certificado de firma de su TSU)

Para esto, ACEPTA hace uso de las mismas funcionalidades de su autoridad certificadora para la revocación del certificado de la TSU, ello de acuerdo a lo declarado en el punto 3.4 del documento PO02 de Firma electrónica Avanzada, acotando ello a los siguientes puntos:

Tendrá lugar cuando Acepta constate alguna de las siguientes circunstancias:

a) Por solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso que el certificado esté emitido para un cargo de dicha empresa). En este caso ACEPTA es quien solicita la revocación.
b) Resolución judicial ejecutoriada.
c) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.
d) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos, y por ende se haya vulnerado la llave de firma de la TSU
e) Si el titular no proporciona sus datos actualizados al momento de solicitar el certificado.

Para todo estos casos ACEPTA responde al titular del certificado, el cual al momento de revocarse, invalida todo los TST firmados con la TSU revocada. Es responsabilidad de quién confíe en los TST de ACEPTA, el verificar el estado del certificado de la TSU (CRL y/o Servicio OCSP). Sólo se entenderá como válido un TST, si la TSU firmante está vigente.

5 Revisión y aprobación del documento

5.1 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.

5.2 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	

5.3 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.