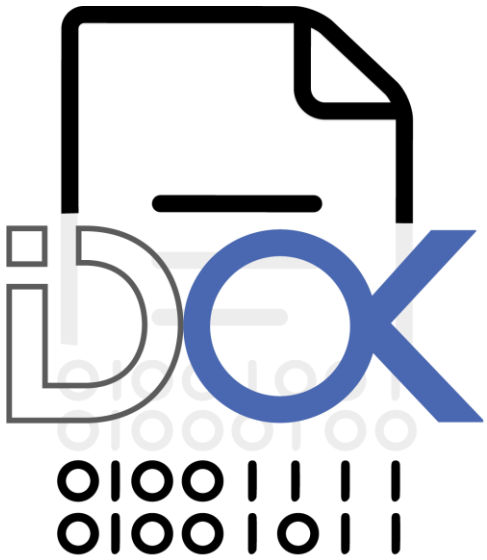

PO01 – POLÍTICA DE SELLO DE TIEMPO

Resumen

Documento conteniendo la Política de Sello de Tiempo

1. Información del Documento

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	PO01 Política de Sello de Tiempo
Creado por:	Oficial de Seguridad IDOK

Responsable del Documento:	Oficial de Seguridad IDOK	**Fecha de Creación:**	26 de septiembre de 2018
Aprobado por:	Gerencia General IDOK	**Fecha de Aprobación:**	8 de octubre de 2018

CONTROL DE VERSIONES

Versión	Fecha de Vigencia	Aprobación	Comentario
001	26 de septiembre de 2018	Oficial de Seguridad	Creación del documento
002	14 de julio de 2020	Oficial de Seguridad	Revisión del documento
003	5 de marzo de 2021	Oficial de Seguridad	Actualización del documento

2. Introducción

La Política de Sello de Tiempo (PST) es el conjunto de reglas que definen la forma en que opera el servicio de Sello de Tiempo de modo de entregar la confianza necesaria a sus usuarios.

Para cumplir con lo anteriormente expuesto, la PST expone en el presente documento las políticas que rigen al servicio en cada una de sus fases: al gestionar la información relacionada con el enrolamiento del Sello de Tiempo; durante la verificación del Sello de Tiempo; cuando se requiera verificar la vigencia de la llave privada a través de la CRL u OCSP; o si la llave privada llega a ser comprometida.

3. Alcance

El alcance de la Política de Sello de Tiempo (PST) detalla las condiciones de los servicios de certificación que presta IDOK para la emisión de sus certificados de la Autoridad de Sello de Tiempo (TSA: Time Stamping Authority).

4. Referencias y glosario

La presente declaración de Política de Sello de Tiempo se ha generado siguiendo las especificaciones de documentos y referencias que se indican a continuación:

- RFC 3628 “Policy Requirements for Time-Stamping Authorities”.
- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamping Protocol (TSP)”.
- ETSI TS 102 023 “Electronic Signatures and Infrastructures (ESI) Policy Requirements for Time-Stamping Authorities”.
- Guía de Evaluación: Procedimiento de Acreditación Prestadores de Servicios de Certificación de Servicios de Certificación de Sello de Tiempo” en su versión 1.0 Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.

Glosario

- **Hashing**: Son una secuencia de caracteres que representan un documento. Esta secuencia es de tamaño fijo y reducido. La principal característica es que es una representación única del documento original y que si existe una alteración mínima el resultado es absolutamente distinto y deja de representar al documento original.
- **Tercera parte**: receptor de un token de sello de tiempo quien confía en este token de sello de tiempo.
- **Suscriptor**: entidad requiriendo el servicio provisto por una TSA y cual está explícitamente o implícitamente de acuerdo a sus términos y condiciones.
- **token de sello de tiempo**: objeto de datos
- **time-stamp token**: objeto asociado a la representación de un dato en un lapso de tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los tokens de sellado de tiempo deben emitirse de acuerdo al RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".
- **TSA**: **Time Stamping Authority** (autoridad de sellado de tiempo) autoridad cual emite token de sellado de tiempo.
- **Declaración de divulgación de la TSA**: conjunto de declaraciones sobre las políticas y prácticas de la TSA que particularmente requieren énfasis o de la divulgación a los suscriptores y terceras partes de confianza, por ejemplo, para cumplir con requisitos regulatorios.
- **Declaración de prácticas de la TSA**: declaración de prácticas que una TSA emplea para la emisión de tokens de sello de tiempo.
- **Sistema TSA**: composición de productos de tecnologías de la información y componentes organizados para soportar la provisión del servicio de sellado de tiempo.
- **Políticas de sellado de tiempo**: conjunto de reglas que indican la aplicabilidad de un token de sello de tiempo para una comunidad particular y/o clase de aplicación con requerimiento de seguridad comunes.
- **Unidad de sellado de tiempo**: conjunto de hardware y software que es administrado como una unidad y tiene una sola clave de firma para el token de sello de tiempo activo a la vez.
- **Coordinated Universal Time (UTC)**: escala de tiempo basada sobre la segundo como se define en las recomendaciones ITU-R TF.460-5 [TF.460-5]. Para propósitos más prácticos UTC es equivalente al tiempo solar en el primer meridiano. Más específicamente, UTC es el compromiso entre el altamente estable tiempo atómico (Temps Atomique International - TAI) y tiempo solar derivado de la rotación irregular de la tierra.

Para el propósito del presente documento, las siguientes abreviaciones aplican:

TSA: Autoridad de Sellado de Tiempo
TSU: Unidad de Sellado de Tiempo
TST: Token de Sellado de Tiempo
UTC: Hora Universal Coordinada

5. Comunidad de Usuarios y Aplicabilidad

Esta política está dirigida a satisfacer los requisitos de sellado de tiempo de la firma digital, para períodos de validez de largo plazo, pero es generalmente aplicable a cualquier requisito de calidad equivalente.

Esta política puede ser usada por el servicio público de sellado de tiempo o por una comunidad cerrada.

4.1 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; para los

certificados válidos en el ámbito tributario la entidad acreditadora es el Servicio de Impuestos Internos.

4.2 APLICABILIDAD DE LOS SELLOS DE TIEMPO.

Los sellos de tiempo emitidos por la autoridad de sellado de tiempo se utilizarán únicamente conforme a la función y finalidad que están establecidas en esta Práctica de Sellado de Tiempo, en concordancia con la normativa vigente para garantizar el no repudio.

El uso de los sellos de tiempo está limitado a demostrar que un documento o una serie de datos han existido y no han sido modificados desde un instante de tiempo específico y confiable.

5.2.1. Uso

El uso de los sellos de tiempo aquí descrito está acotado a demostrar que una serie de datos han existido y no han sido alterados desde un instante de tiempo específico y confiable. El conjunto de normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denomina "Política de certificación de Sello de Tiempo".

5.2.2. Usos prohibidos

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

5.2.3. Estructura de los sellos de tiempo

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

6. Procedimiento de registro

Los usuarios que utilizan el servicio de TSA, se controlan a través de su ip pública, por lo que el procedimiento de registro conta de lo siguiente:

- Validación del usuario en la plataforma
- Notificación de IP pública
- Seguimiento de las transacciones

7. Conceptos generales

7.1. SERVICIO DE SELLADO DE TIEMPO

La entrega del servicio de sellado de tiempo es dividida en los siguientes servicios, para el propósito de los requerimientos de clasificación:

- Time-stamping provision: este servicio genera los tokens de sello de tiempo.
- Time-stamping management: servicio que monitorea y controla las operaciones de sellado de tiempo para garantizar que el servicio es provisto como lo especifica la TSA. Este servicio es responsable por la instalación y desinstalación de los servicios de provisión de sellos de tiempo (Time-stamping provisión). Por ejemplo, la administración del sellado de tiempo garantiza que los relojes usados para el sellado de tiempo están correctamente sincronizados con UTC.

Esta subdivisión de servicios es solamente para propósitos de clarificación de los requisitos especificados en el presente documento y no coloca restricciones para cualquier otra subdivisión en la implementación del servicio de sellado de tiempo.

7.2. AUTORIDAD DE SELLADO DE TIEMPO

La autoridad a emitir "tokens" de sello de tiempo, de confianza para el usuario del servicio de sellado de tiempo, ejemplo: suscriptores y terceras partes de confianza, es llamada Autoridad de Sellado de Tiempo (TSA). La TSA tiene la responsabilidad absoluta por el servicio de sellado de tiempo.

La TSA tiene la responsabilidad de la operación de una o más TUS que crea y firma en nombre de la TSA. La TSA responsable de emitir un token de sello de tiempo es identificable.

La TSA puede utilizar otras partes para proporcionar partes de los servicios de sellado de tiempo. Sin embargo, la TSA siempre mantiene la responsabilidad total y asegura que se cumplen los requisitos de las políticas identificadas en el presente documento. Por ejemplo, una TSA podrá subcontratar todos los servicios de componentes, incluidos los servicios que generan tokens de sello de tiempo utilizando las claves de la TSU. Sin embargo, la clave privada o claves utilizadas para generar los tokens de sello de tiempo pertenecen a la TSA que mantiene la responsabilidad total de cumplimiento de los requisitos de este documento.

Una TSA puede operar varias unidades identificables de sellado de tiempo. Cada unidad tiene una clave diferente.
Una TSA es un proveedor de servicio de certificación, como se define en EU Directive on Electronic Signatures (artículo 2(11)), que emite tokens de sello de tiempo.

7.3. SUSCRIPTOR

El suscriptor puede ser una organización que comprende varios usuarios finales o un usuario individual.

Cuando el suscriptor es una organización, algunas de las obligaciones que aplica a esta organización, tendrán que aplicarse también a los usuarios finales. En cualquier caso, la organización será la responsable.

Cuando el suscriptor es una organización, alguna de las obligaciones que aplica a la organización tendrá que aplicar también a los usuarios finales. En cualquier caso, la organización se hace responsable si no se cumplen correctamente las obligaciones de los usuarios finales y por lo tanto se espera que la organización informe adecuadamente a sus usuarios finales.

Cuando el suscriptor es un usuario final, éste será directamente el responsable si sus obligaciones no son completamente cumplidas.

7.4. POLÍTICA DE SELLADO DE TIEMPO Y DECLARACIÓN DE PRÁCTICAS DE LA TSA

Esta sección explica lo relativo a los roles de la política de sellado de tiempo y a la declaración de prácticas de la TSA de IDOK.

Esto no coloca restricciones específicas sobre la política de sellado de tiempo o la declaración de prácticas.

7.4.1. Propósito

En general, la política de sellado de tiempo establece "a lo que hay que adherirse", mientras una declaración de prácticas de TSA establece "la forma de cómo se adhiere", ejemplo: el proceso que se utilizará para la creación de sellos de tiempo, mantenimiento de la precisión de su reloj. La relación entre la política de sellado de tiempo y la declaración de prácticas de la TSA es de naturaleza similar a la relación de otras políticas empresariales las cuales indican los requisitos de la empresa, mientras las unidades operacionales definen las prácticas y procedimientos de cómo estas políticas son llevadas a cabo.

El presente documento especifica una política de sellado de tiempo para cumplir con los requisitos para un servicio de sellado de tiempo confiable. IDOK especifica en su declaración de prácticas de TSA cómo estos requisitos son llevados a cabo.

7.4.2. Nivel de Especificación

La declaración de práctica de TSA es más específica que una política de sellado de tiempo. Una declaración de prácticas de TSA es una descripción más detallada de los términos y condiciones, así como las prácticas empresariales y operativas de una TSA en emitir y gestionar de otra forma los servicios de sellado de tiempo. La declaración de prácticas de una TSA refuerza las reglas estabilizadas por una política de sellado de tiempo. Una declaración de prácticas de TSA define como una TSA específica, cumple los requisitos técnicos, organizacionales y procedimentales identificados en la política de sellado de tiempo. Incluso la documentación interna de bajo nivel puede ser apropiada para un TSA que detalla los procedimientos específicos necesarios para completar las prácticas identificadas en la declaración de prácticas de TSA.

7.4.3. Enfoque

El enfoque de una política de sellado de tiempo es significativamente diferente a la declaración de prácticas de TSA. Una política de sellado de tiempo es definida independientemente de los detalles específicos del ambiente de operaciones de una TSA, mientras que la declaración de prácticas de la TSA se adapta a la estructura organizativa, procedimientos operacionales, comodidades y ambiente computacional de la TSA. Una política de sellado de tiempo puede ser definida por el usuario de servicio de sellado de tiempo, mientras que la declaración de prácticas de la TSA es siempre definida por el proveedor.

8. Políticas del servicio de Sello de Tiempo

8.1. GENERAL

Una política de sellado de tiempo es un "conjunto de reglas que indican la aplicabilidad de un token de sello de tiempo a una comunidad particular y/o clase de aplicación con requerimientos comunes de seguridad".

El presente documento define requisitos de base para una política de sello de tiempo emitiendo tokens de sello de tiempo, soportado por certificados de clave pública, con una precisión igual o mejor a un segundo. Sin medidas adicionales, la parte confiante puede no ser capaz de garantizar la validez de un token de sello de tiempo más allá del fin del período de validez que soporta el certificado.

Una TSA puede definir su propia política la cual mejora la política definida en este documento. Tal política debe incorporar o restringir aún más los requisitos identificados en este documento.

Si la TSA provee una precisión mejor a un segundo, y si todas las TSUs tienen la misma característica, entonces la precisión debe ser indicada en la declaración de divulgación de la TSA que cada token de sello de tiempo es emitido con una precisión mejor a un segundo. Es requerido que el token de sello de tiempo incluya un identificador para la política aplicable.

8.2. IDENTIFICACIÓN

El identificador de objeto [X.208] de la política base de sellado de tiempo es:
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1)

En la declaración de divulgación TSA puesta a disposición de los suscriptores y partes de confianza, una TSA también incluirá el identificador de la política de sello de tiempo para indicar su conformidad.

8.3. COMUNIDAD DE USUARIOS Y APLICABILIDAD

Esta política está dirigida a satisfacer los requisitos de sellado de tiempo de la firma digital, para períodos de validez de largo plazo, pero es generalmente aplicable a cualquier requisito de calidad equivalente.
Esta política puede ser usada por el servicio público de sellado de tiempo o por una comunidad cerrada.

8.4. CONFORMIDAD/CUMPLIMIENTO

La TSA debe usar el identificador de la política de sellado de tiempo en los tokens de sello de tiempo, como se muestra en la sección 9.2 o definir su propia política de sellado de tiempo, que incorpore o restrinja aún más los requisitos identificados en este documento:

a) Si la TSA afirma conformidad con el identificador de la política de sellado de tiempo y pone a disposición de los suscriptores y terceras partes confiantes la solicitud que evidencia la conformidad referenciada;
b) Si la TSA ha sido evaluada para cumplir con la política de sello de tiempo identificada por una tercera parte independiente.

Una TSA que cumple debe demostrar que:

a. Este cumple sus obligaciones como se define en la sección 9.1;
b. Este ha implementado controles que cumple con los requisitos especificados en la sección "Requerimientos sobre las prácticas de la TSA".

9. Obligaciones y Responsabilidades

9.1. Obligaciones de la TSA

9.1.1. General

- La TSA debe asegurar que todos los requerimientos sobre la TSA, son implementados como aplicables a la selección política de sellado de tiempo.
- La TSA debe asegurar conformidad con los procedimientos descritos en esta política, incluso, cuando la funcionalidad de la TSA sea realizada por subcontratistas.
- La TSA debe también asegurar adherencia a cualquier obligación adicional indicada en el sello de tiempo directa o incorporado por referencia.
- La TSA debe proveer todos sus servicios de sellado de tiempo consistente con su declaración de prácticas.

9.1.2. Obligación de la TSA hacia los suscriptores

La TSA debe cumplir obligaciones como declara en sus términos y condiciones, incluyendo la disponibilidad y precisión de sus servicios.

9.2. Obligaciones del suscriptor

El presente documento no especifica obligaciones del suscriptor más allá del estado de cualquier requerimiento específico de la TSA, en los términos y condiciones. Es recomendable que cuando se obtenga el token de sello de tiempo, el suscriptor verifique que el token de sello de tiempo ha sido correctamente firmado y que la clave privada usada para firmar el token de sello de tiempo no haya sido comprometida.

9.3. Obligaciones de partes confiantes

Los términos y condiciones disponibles para las partes confiantes deben incluir obligación sobre las terceras partes que, cuando confía en un token de sellado de tiempo, este deberá:

a. verificar que el token de sellado de tiempo ha sido correctamente firmado y que la clave privada usada para firmar el sello de tiempo no ha sido comprometida hasta el tiempo de la verificación. Durante la validez del certificado de la TSU, la validez de la clave de firma puede ser chequeada usando el estado de revocación para el certificado de la TSU. Si el tiempo de verificación excede el fin del periodo de validez del correspondiente certificado.

   b. Tener en cuenta cualquier limitación sobre el uso de sellos de tiempos indicados por la política de sello de tiempo.
   c. Tomar en cuenta cualquier otra precaución prescripta en acuerdos o en otra parte.

9.4. RESPONSABILIDAD

El presente documento no especifica ningún requerimiento sobre responsabilidades.
En particular, debe destacarse que una TSA puede rechazar o limitar cualquier responsabilidad a menos que esté estipulado por las leyes aplicables.

10. Requerimientos sobre las prácticas de la TSA

Los requisitos de esta política no pretenden implicar ninguna restricción sobre el cobro por los servicios de la TSA.

Los requisitos son indicados en términos de objetivos de seguridad, seguido por requerimientos más específicos, para el control, para cumplir aquellos objetivos donde es necesario proveer confianza de los objetivos serán satisfechos.

Los detalles de los controles requeridos para satisfacer un objetivo son balanceados, entre lograr la confianza necesaria, mientras minimiza las restricciones sobre las técnicas que una TSA puede emplear en la emisión de tokens de sellado de tiempo. En el caso de la sección 9.6 (Operación y Gestión de la TSA), se hace referencia a una fuente más detallada de requisitos de control. Debido a estos factores, la especificación de los requisitos dados bajo un determinado tema, puede variar.

La provisión de un token de sellado de tiempo, en respuesta a un requerimiento, es a criterio de la TSA, dependiendo del acuerdo de nivel de servicio con el suscriptor.

10.1 PRÁCTICAS Y DECLARACIÓN DE DIVULGACIÓN

10.1.1 Declaración de prácticas de la TSA

La TSA debe asegurar, que esta demuestra fiabilidad necesaria, para proveer servicios de sellado de tiempo.

En particular:

a. La TSA debe tener una evaluación de riesgos llevada a cabo con el fin de evaluar activos del negocio y amenazas para aquellos activos en el orden de determinar los controles de seguridad necesarios y procedimientos operacionales.

b. La TSA debe tener una declaración de las prácticas y procedimientos usados para direccionar todos los requerimientos identificados en esta política de sellado de tiempo. Esta política no hace requerimientos en cuanto a la estructura de la declaración de prácticas de la TSA.

c. La declaración de práctica de la TSA debe identificar las obligaciones de todas las organizaciones externas soportando los servicios de la TSA, incluyendo las políticas y prácticas aplicables.

d. La TSA debe poner a disposición de los suscriptores y terceras partes (partes confiantes) su declaración de prácticas y otra documentación relevante, como necesaria para evaluar conformidad a la política de sellado de tiempo. La TSA generalmente no está obligada a hacer público todos los detalles de su política.

e. La TSA debe divulgar a todos los suscriptores y terceras partes los términos y condiciones con respecto al uso del servicio de sellado de tiempo.

f. La TSA debe tener un comité ejecutivo con autoridad suficiente para aprobar la declaración de prácticas de la TSA.

g. El senior management de la TSA debe asegurar que las prácticas son propiamente implementadas.

h. La TSA debe definir un proceso de revisión para las prácticas incluyendo responsabilidades para el mantenimiento de la declaración de prácticas de la TSA.

i. La TSA dará la debida notificación de los cambios que se propone hacer en su declaración de prácticas y deberá seguido a la aprobación (punto f) ponerla inmediatamente a disposición, como lo requiere el punto d.

10.1.2 Declaración de Divulgación de la TSA

La TSA debe notificar a todos los suscriptores y potenciales terceras partes confiantes, los términos y condiciones con respecto al uso del servicio de sellado de tiempo. Esta declaración deberá al menos especificarse para cada una de las políticas soportadas por la TSA:

a. Información de los contactos de la TSA

b. La política de sellado de tiempo está siendo aplicada.

c. El último algoritmo de hash que puede ser usado para representar el digesto de datos, a ser sellado (No se requiere ningún algoritmo hash).

d. El tiempo de vida de la firma, usado para firmar el token de sellado de tiempo (depende del algoritmo de hash siendo usado, el algoritmo de firma siendo usado y la longitud de la clave privada).

e. La precisión del tiempo en los tokens de sellado de tiempo con respecto al UTC.

f. Cualquier limitación sobre el uso del servicio de sellado de tiempo.

g. Las obligaciones del suscriptor.

h. Las obligaciones de las terceras partes confiantes.

i. Información de como verificar los tokens de sellado de tiempo, tal que las terceras partes confiantes se considere una "tercera parte responsable" sobre los tokens de sello de tiempo y cualquier posible limitación sobre el periodo de validez.

j. El periodo de tiempo durante el cual los logs de eventos serán retenidos.

k. El sistema legal aplicable, incluyendo cualquier reclamo para cumplir los requerimientos sobre el servicio de sellado de tiempo, bajo las leyes nacionales.

l. Limitaciones de responsabilidades.

m. Procedimientos para quejas y solución de controversias.

n. Si la TSA ha sido auditada para satisfacer la política de sellado de tiempo, y de ser así, qué organismo independiente lo realizó. Es también recomendable que la TSA incluya en su declaración de divulgación la disponibilidad de su servicio, por ejemplo, el tiempo medio de espera entre fallas del servicio de sellado de tiempo, tiempo medio de recuperación seguido a una falla, y las provisiones hechas para recuperaciones ante desastres, incluyendo los servicios de backup.

   Esta información debe estar disponible a través de medios de comunicación durables. Esta información debe estar en un lenguaje entendible. Esta puede ser transmitida electrónicamente. Alternativamente este puede provisto en el acuerdo con suscriptores y terceras partes confiantes. Esta declaración puede ser incluida en la declaración de prácticas provista, que son visibles para el lector.

10.2 ADMINISTRACIÓN DEL CICLO DE VIDA DE LAS CLAVES

10.2.1 Generación de la clave de la TSA

La TSA debe asegurar que todas sus claves criptográficas son generadas bajo circunstancias controladas.

En particular:

a. La generación de la clave/s de firma de la TSU debe ser realizada en un ambiente físico seguro por personal con roles de confianza, bajo al menos un control doble. El personal autorizado a llevar a cabo esta función deberá ser limitado a aquellos que sean requeridos para hacerlo, bajo las prácticas de la TSA.
b. La generación de la clave de firma debe ser llevada dentro de un módulo criptográfico que o bien:

   - Cumpla los requisitos identificados en FIPS 140-1
   - Cumpla con los mensajes identificados en CEN Workshop Agreement 14167-2

- Es un sistema digno de confianza que está asegurado para EAL4 o superior de acuerdo a la ISO 15408, o algún criterio de seguridad equivalente. Se tratará de un objetivo de seguridad o perfil de protección que cumpla con los requisitos del documento actual, basado en un análisis de riesgos y teniendo en cuenta las medidas de seguridad físicas y otras no técnicas.

c. El algoritmo de generación de clave de la TSU, la longitud de la clave de firma y el algoritmo de firma usado para firmar los tokens de sello de tiempo deben ser reconocidos por cualquier organismo nacional de supervisión o concordar con el actual estado del arte, como apto para los fines de los tokens de sello de tiempo emitidos por la TSA.

10.2.2 Protección de la clave privada de la TSU

La TSA debe asegurar que la clave privada de la TSU se mantiene confidencial y mantiene su integridad.

En particular:

a. La clave privada de firma de la TSU será conservada y usada dentro de un módulo criptográfico cual:

   - Cumple los requerimientos identificados en FIPS 140-1 level 3 or superior; o
   - Cumplir con los requerimientos identificados en CEN Workshop Agreement 14167-2 [CWA 14167-2]; o
   - Es un sistema confiable que es asegurado a EAL4 o superior de acuerdo a la ISO 15408, o equivalente criterio de seguridad. Este será un objetivo de seguridad o perfil de protección que cumple los requerimientos de este documento, basado sobre análisis de riesgos y tomando en cuenta medidas de seguridad física y otras no técnicas. Backup de la clave privada de la TSU está en desuso para evitar minimizar los riesgos de compromiso de la clave.

b. Si la clave privada de la TSU es respaldada, esta debe ser copiada, almacenada y recuperada sólo por personal en los puestos de confianza, usando un control dual en un ambiente físicamente seguro (ver 10.4.4). El personal autorizado a llevar esta función debe ser limitado a aquellos requeridos para hacerlo las prácticas de la TSA.

c. Cualquier copia de backup de la clave privada de firma de la TSU debe estar protegida para asegurar su confidencialidad por un módulo criptográfico antes de ser almacenada fuera del dispositivo.

10.2.3 Distribución de la clave pública de la TSA

La TSA debe asegurar que la integridad y autenticidad de la firma de la TSU, verificando las claves (pública) y cualquier parámetro asociado que sea mantenido durante su distribución a las terceras partes confiantes.

En particular:

a. La verificación de las claves (pública) de la TSU debe estar disponible a las terceras partes confiantes dentro del certificado de clave pública, por ejemplo, el certificado de las TSU's puede ser emitido por una autoridad de certificación operado por la misma organización que la TSA, o emitida por otra autoridad.
b. La verificación de la firma de los certificados de clave pública de las TSUs debe ser emitida por una autoridad de certificación operada bajo una política la cual provea un nivel de seguridad equivalente o mayor que esta política de sellado de tiempo.

10.2.4 Reemisión de la llave de TSA

Por motivo de seguridad y evitar el repudio a un certificado, IDOK como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo a las políticas y prácticas que rigen la operación de su CA. Sin embargo, la llave privada de la TSU será reemplazada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

Las claves privadas caducadas se almacenan por un periodo no inferior a 10 años, siendo IDOK la ejecutora del procedimiento y la responsable de esta decisión. Las claves públicas se almacenan por un periodo adicional no inferior a 15 años, para permitir la verificación de sellos de tiempo emitidos con dichas claves.

10.2.5 Revocación y suspensión de certificados

La CA se asegurará de que los certificados se revoquen de manera oportuna en función de las solicitudes de revocación de certificados validadas y autorizadas.
En particular:

10.2.5.1 Gestión de revocación

a) La CA deberá documentar como parte de su declaración de prácticas de certificación los procedimientos para revocación de certificados que incluyen:

   I. quién puede presentar informes y solicitudes de revocación;
   II. cómo pueden presentarse;
   III. cualquier requisito para la confirmación posterior de informes y solicitudes de revocación, por ejemplo, es posible que se requiera una confirmación del suscriptor si un tercero informa un compromiso;
   IV. si los certificados pueden suspenderse y por qué motivos;
   V. el mecanismo utilizado para distribuir información sobre el estado de revocación;
   VI. la demora máxima entre la recepción de una solicitud o informe de revocación y el cambio al estado de revocación, información disponible para todas las partes que confían.

b) Solicitudes e informes relacionados con la revocación, por ejemplo, debido al compromiso de la clave privada del sujeto, muerte del sujeto, terminación inesperada del acuerdo o funciones comerciales de un suscriptor o sujeto, violación de obligaciones contractuales, se tramitarán a su recepción.

c) Las solicitudes e informes relacionados con la revocación se autenticarán, comprobando que proceden de una fuente autorizada.
   Dichos informes y solicitudes se confirmarán según lo requieran las prácticas de la CA.

d) El estado de revocación de un certificado puede establecerse en "suspendido" mientras se confirma la revocación. La CA se asegurará de que un certificado no se mantenga suspendido durante más tiempo del necesario para confirmar su estado (el soporte para la suspensión de certificados es opcional).

e) El sujeto, y en su caso el suscriptor, de un certificado revocado o suspendido, será informado del cambio de estado del certificado.

f) Cuando se utilicen listas de revocación de certificados (CRL) que incluyan cualquier variante, por ejemplo, Delta CRL, estas se deberán publicar.

g) Cuando las listas de revocación de certificados (CRL), incluidas las variantes, Delta CRL, se utilizan como únicos medios para proporcionar información sobre el estado de la revocación:

I. cada CRL indicará una hora para la próxima emisión de CRL programada; y
II. se puede publicar una nueva CRL antes de la hora indicada para la próxima emisión de CRL;
III. la CRL deberá estar firmada por la autoridad de certificación o una autoridad designada por la CA. Para maximizar la interoperabilidad, se recomienda que la CA emita Listas de revocación de certificados como se define en la Recomendación UIT-T X.509 [9].

10.2.5.2 Estado de revocación

La información sobre el estado de la revocación estará disponible según se especifica en la Práctica de certificación de la CA.

La información sobre el estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. Ante una indisponibilidad del sistema, servicio u otros factores que no están bajo el control de la CA, la CA hará todo lo posible para garantizar que este servicio de información no esté disponible por más tiempo que el período de tiempo máximo indicado en la declaración de prácticas de certificación. La información sobre el estado de revocación puede proporcionarse, por ejemplo, mediante el servicio de estado de certificados en línea o mediante la distribución de CRL a través de un repositorio.

h) Se protegerá la integridad y autenticidad de la información de estado.
i) Si la CA está emitiendo un certificado al público, la información sobre el estado de la revocación estará disponible pública e internacionalmente.
j) La información sobre el estado de la revocación incluirá información sobre el estado de los certificados al menos hasta que expire.

10.2.6 Fin del ciclo de vida de la TSU

La TSA debe asegurarse que la clave privada de la TSU no sea usada luego del fin de su ciclo de vida. En particular:

a. Procedimientos operacionales o técnicos deben asegurar que la nueva clave es colocada en su lugar cuando la clave de la TSU expira.
b. La clave privada de la TSU, o cualquier parte incluyendo copias deben ser destruidas tal que la clave privada no puede ser recuperada.
c. El sistema de generación de token de sellado de tiempo debe rechazar cualquier intento de emitir tokens si la clave privada de firma ha expirado

10.2.7 Administración del ciclo de vida del módulo criptográfico usado para firmar Sellos de tiempo.

La TSA velará por la seguridad de su hardware de seguridad a lo largo de su ciclo de vida.

En particular la TSA velará porque:

a. El hardware criptográfico para firma de tokens de sellos de tiempo no ha sido manipulado/alterado durante su traslado.
b. El hardware criptográfico para firma de tokens de sellos de tiempo no ha sido manipulado/alterado mientras estaba almacenado.
c. Instalación, activación y duplicación de la clave de firma de la TSU en el hardware criptográfico debe ser realizado sólo por personal con roles adecuados de confianza, usando controles duales en un ambiente físicamente seguro.
d. El hardware criptográfico para firma de tokens de sellos de tiempo está funcionando correctamente; y
e. La clave privada de firma de la TSU (almacenada en el módulo criptográfico) es eliminada cuando el módulo es retirado.

10.3 SELLO DE TIEMPO

10.3.1. Token de Sello de Tiempo

La TSA debe asegurar que los tokens de sello de tiempo son emitidos de forma segura e incluye un tiempo correcto.

En particular:

a. El token de sellado de tiempo debe incluir un identificador para la política de sellado de tiempo;

b. Cada token de sello de tiempo debe tener un identificador único;

c. Los valores de tiempo que la TSU use en los tokens de sello de tiempo deben ser trazable al menos uno de los valores de tiempo real distribuido por un laboratorio UTC.

d. El tiempo incluido en los tokens de sello de tiempo deben estar sincronizados con UTC dentro de la precisión definida en esta política y, si está presente, dentro de la precisión definida en el propio token de sello de tiempo.

e. Si se detecta que el proveedor de hora de los sellos de tiempo, comienza estar fuera de la precisión establecida el token de sello de tiempo no debe ser emitido.

f. El token de sello de tiempo debe incluir una representación (ej. valor hash) de dato que es time-stamped, cómo es proporcionado por el solicitante;

g. El token de sellado de tiempo debe ser firmado usando una clave generada exclusivamente para este propósito. Un protocolo para un token de sello de tiempo es definido en la RFC 3631 y el perfil en TS 101 861 [TS 101861]. En el caso de un número de solicitantes en aproximadamente el mismo tiempo, el orden del tiempo dentro de la precisión del reloj de la TSU no es mandatorio.

h. El token de sello de tiempo debe incluir:
   - donde aplique, un identificador para el país en el cual la TSA está establecida;
   - un identificador para la TSA;
   - un identificador para la unidad que emite el sello de tiempo.

10.3.2. Sincronización de Reloj con UTC

La TSA debe asegurar que su reloj está sincronizado con UTC, dentro de la precisión declarada.

En particular:

a. La calibración del reloj de la TSU debe ser mantenido de tal forma que el reloj no tenga una desviación mayor a la precisión declarada.

b. Los relojes de la TSU deben estar protegidos contra amenazas que pudieran resultar en un cambio indetectable al reloj externo del cual toma su calibración. Amenazas pueden incluir manipulación por personal no autorizado, interferencias de radio o eléctricas.

c. La TSA debe asegurar que, si el tiempo que debería ser indicado en el token de sello de tiempo se desvía o salta fuera de la sincronización con UTC, esto será detectado. Es obligatorio informar a las terceras partes ante el suceso de tales eventos.

d. La TSA debe asegurar que la sincronización del reloj es mantenida cuando un segundo intercalar (leap second) ocurre, según lo notificado por el órgano

competente. El cambio para tener en cuenta este segundo intercalar ocurre durante los últimos minutos del día, cuando un segundo intercalar es programado que ocurra "https://es.wikipedia.org/wiki/Segundo_intercalar". Se debe mantener un registro del tiempo exacto (dentro de la declaración de precisión) cuando este cambio ocurre. Un segundo intercalar es un ajuste a UTC por saltar o agregar un segundo extra sobre el último segundo de un mes UTC. La primera preferencia es dada al mes de diciembre y junio, y la segunda preferencia es dada al mes de marzo y septiembre.

10.4 OPERACIÓN Y GESTION DE LA TSA

10.4.1. Gestión de la Seguridad

La TSA asegura que los procedimientos administrativos y de gestión aplicados son adecuados y corresponde a las mejores prácticas reconocidas.

En particular:

TSA General

a. La TSA mantiene responsabilidad absoluta sobre el servicio de sellado de tiempo, dentro del alcance de esta política de sellado de tiempo, "aun cuando existan funciones tercerizadas". Las responsabilidades de estas terceras partes serán claramente definidas por la TSA y se realizarán acuerdos para asegurar que las terceras partes estén obligados a implementar todos los controles requeridos por la TSA. La TSA mantiene responsabilidad por la divulgación de las prácticas relevantes a todas las partes.

b. La gerencia de la TSA debe proveer dirección sobre la seguridad de la información, a través de un foro de alto nivel que sea responsable de definir la política de seguridad de la TSA. La TSA debe asegurar la comunicación de esta política a todos los empleados que están implicados en ella.

c. La infraestructura necesaria para manejar la seguridad de la información dentro de la TSA debe ser mantenida continuamente. Cualquier cambio que impacte sobre el nivel de seguridad provisto, será aprobado por el forum ejecutivo de la TSA.

d. Los controles de seguridad y los procedimientos operativos, para las instalaciones de la TSA, sistemas y activos de información, que proveen el servicio de sellado de tiempo, deben estar documentados, implementados y mantenidos. La presente documentación, comúnmente llamada política o manual de seguridad, debe identificar todos los objetivos relevantes, objetos y potenciales amenazas relacionadas al servicio y las salvaguardas requeridas para evitar o limitar los efectos de aquellas amenazas, consistente con el Análisis de Riesgo requerido. Este debe describir las reglas, directivas y procedimientos al respecto, de cómo el servicio especificado y las garantías de seguridad asociadas son garantizadas, en adicional a la política sobre incidentes y desastres.

e. La TSA debe asegurar que la seguridad de la información es mantenida cuando la responsabilidad de las funciones de la TSA sea tercerizada por otras organizaciones o entidades.

10.4.2. Gestion y clasificación de Activos

La TSA debe asegurar que su información y otros activos, reciben un apropiado nivel de protección.

En particular:

- La TSA debe mantener un inventario de todos los activos y debe asignar una clasificación, para los requisitos de protección de aquellos activos, el cual debe ser consistente con el Análisis de Riesgos.

10.4.3. Seguridad del Personal

La TSA asegura que el personal y las prácticas de contratación, mejora y respalda la fiabilidad de las operaciones de la TSA.

En particular (TSA general):

a. La TSA debe emplear personal que posea conocimiento experto, experiencia y calificaciones necesarias para los servicios ofrecidos, según sea apropiado para el puesto de trabajo. El personal de la TSA debe ser capaz de cumplir todos los requerimientos de "conocimiento experto", experiencia y calificaciones mediante capacitación formal y credenciales, experiencia actual, o una combinación de las dos. Personal empleado por

la TSA incluye al personal individual contractualmente comprometido en realizar funciones de soporte en los servicios de la TSA. El personal quien está involucrado en el monitoreo de los servicios de la TSA, no necesita ser personal de la misma.

b. La responsabilidad de los roles de seguridad, como se especifica en la política de seguridad de la TSA, debe estar documentada en la descripción de puestos. Los puestos de confianza, sobre los cuales las operaciones de seguridad de la TSA dependen, deben ser claramente identificados.

c. Personal de la TSA (temporal y permanente) debe tener una descripción de puesto definido desde el punto de vista de la separación de tareas y privilegios mínimos, determinado la sensibilidad de la posición sobre la tarea y niveles de acceso, investigación de antecedentes, formación y sensibilización de los empleados. Cuando sea apropiado, se debe diferenciar entre funciones generales y funciones específicas de la TSA. Este debe incluir requerimientos de experiencia y conocimientos.

d. El personal debe ejercitar los procesos/procedimientos administrativos y de gestión que están alineados con los procedimientos de la gestión de la seguridad de la información (ver ISO/IEC 17799 [ISO 17799] para más información)

   Los siguientes controles deben ser aplicados a la gestión del sellado de tiempo:

e. Deberá emplearse personal Directivo que posea:
   - Conocimiento en tecnología de sellado de tiempo; y
   - Conocimiento en tecnología de firma digital; y
   - Conocimiento en mecanismos de calibración o sincronización de los relojes de la TSI con UTC, y familiarizado con procedimientos de seguridad para el personal con responsabilidad en seguridad; y
   - experiencia con seguridad de la información y análisis de riesgos.

f. Todo el personal de la TSA en cargos de confianza debe estar libres de conflictos de interés que puedan perjudicar la imparcialidad de las operaciones de la TSA.

g. los puestos de confianza incluyen cargos que involucran las siguientes responsabilidades:

   - Oficiales de Seguridad: responsabilidad global por la gestión de la implementación de las prácticas de seguridad.

- Administradores de Sistemas: autorizados a instalar, configurar y mantener la fidelidad de los sistemas de la TSA.
- Operadores de Sistema: responsables de las operaciones básicas de los sistemas de la TSA día a día. Autorizados a realizar backup y recovery.
- Auditores de Sistemas: Autorizados a ver archivos y logs de auditoría de los sistemas de la TSA.

h. El personal de la TSA debe ser formalmente designado en los roles de confianza por altos directivos responsables de la seguridad.

i. No deben ser designados los puestos de confianza o directivos, a personas quienes ya son conocidos por tener condenas por delitos graves u otros delitos que afecte su idoneidad para el cargo. El personal no debe tener acceso a los puestos de confianza hasta que todos los chequeos necesarios sean terminados. En algunos países no es posible que la TSA obtenga la información del pasado delictivo sin la colaboración del candidato al puesto.

10.4.4. Seguridad física y del entorno

La TSA debe asegurar que el acceso físico a los servicios críticos es controlado y el riesgo a los activos físicos es minimizado.

En particular (general):

a. Para ambos, la provisión de sellos de tiempo y la gestión de los sellos de tiempo:

- Acceso físico a las instalaciones con el servicio de sellado de tiempo deben ser limitada a personas debidamente autorizadas;
- Controles deben ser implementados para evitar pérdidas, daño o compromiso de los activos e interrupciones a las actividades del negocio; y
- Los controles deben ser implementados para evitar, compromiso o robo de información, y de procesamiento de información.

b. Controles de acceso deben ser aplicados a los módulos de seguridad para cumplir los requisitos de seguridad de los módulos criptográficos como se define en la sección 10.

c. Los siguientes controles adicionales deben ser aplicados a la gestión de los sellos de tiempo:

- La gestión de las instalaciones de sellado de tiempo debe ser operadas en un ambiente el cual este protegido físicamente el servicio del compromiso, a través de acceso no autorizado a los sistemas o datos.
- La protección física se logra a través de la creación de perímetros claramente definidos (barreras físicas) en torno a la gestión del sellado de tiempo. Cualquier de las instalaciones compartidas con otra organización, debe estar fuera de este perímetro.
- Los controles de seguridad física y del entorno deben ser implementados para proteger las instalaciones que resguardan los recursos de los sistemas, los sistemas en sí, y las instalaciones para soportar sus operaciones. La política de seguridad física y del entorno para los sistemas de la TSA, concernientes con la administración del sellado de tiempo, debe ser dirigida como mínimo al control de acceso, protección contra desastres naturales, seguridad contra los factores de incendio, fallas de equipamiento de soporte (energía, telecomunicaciones), colapso de la estructura, pérdidas en las cañerías, protección contra robo, allanamientos y recuperación ante desastres.
- Los controles deben ser implementados para proteger el equipamiento, información, y que el software/medios relacionados al servicio de sellado de tiempo sea llevado fuera del sitio sin autorización, ver ISO/IEC 17799 [ISO 17799] para obtener orientación sobre seguridad física y ambiental. Otras funciones pueden ser soportadas dentro de la misma área de seguridad, siempre que el acceso sea limitado a personal autorizado.

10.4.5. Gestión de la Operaciones

La TSA debe asegurar que los sistemas componentes de la TSA son seguros y correctamente operados, con un riesgo mínimo de falla:

En particular (general):

a. La integridad de los sistemas componentes de la TSA y la información deben ser protegida contra virus, software malicioso o no autorizado.

b. Procedimientos de reporte y respuesta a incidentes deben ser empleados de tal manera que el daño causado por incidente de seguridad y el mal funcionamiento sean minimizados.

c. Medios (usb/cd) usados en los sistemas de confianza de la TSA deben ser manejados de forma segura para protegerlo de daños, robo, acceso no autorizado y obsolescencia. Todo miembro del personal con responsabilidades directivas es responsable por la planificación y la implementación efectiva de la política de sellado de tiempo y prácticas asociadas como se documenta en la declaración de prácticas de la TSA.

d. Los procedimientos deben ser establecidos e implementados por todos los roles administrativos y de confianza que impactan sobre la provisión del servicio de sellado de tiempo.

Manejo de medios y Seguridad

e. Todos los medios deben ser manejados de forma segura en concordancia con los requisitos del esquema de clasificación de información. Los medios conteniendo datos sensitivos deben ser eliminados de forma segura cuando ya no se necesite.

Planificación del Sistema

f. La demanda de capacidad debe ser monitoreada y las proyecciones a futuro de requerimientos de capacidad hechas para asegurar adecuado poder de procesamiento y almacenamiento.

Reporte y Respuesta a Incidentes

g. La TSA debe actuar de manera oportuna y coordinada en orden de responder rápidamente a incidentes y limitar el impacto de las brechas de seguridad. Todo incidente debe ser reportado tan pronto como sea posible después de ocurrido.

Los controles siguientes deben ser aplicados a la gestión del sellado de tiempo:

Procedimientos de Operaciones y Responsabilidades

h. Las operaciones de seguridad de la TSA deben estar separadas de otras operaciones. Operaciones de seguridad de la TSA incluyen las siguientes responsabilidades:

- Procedimientos operacionales y responsabilidades.
- planificación de sistemas de seguridad y aceptación.
- protección de software malicioso;

- Servicio de limpieza;
- administración de redes;
- monitoreo activo de auditorías, análisis de eventos y seguimiento;
- manejo de medios y seguridad;
- intercambio de datos y software.

Estas operaciones deben ser manejadas por personal de confianza, pero, puede de momento ser realizadas por no especialistas, personal de operaciones (bajo supervisión), como se define en la apropiada política de seguridad, y documentos de roles y responsabilidades.

10.4.6. Administración del sistema de control de acceso

La TSA debe asegurar que el acceso a los sistemas es limitado a un número reducido y autorizado de personas.

En particular (general):

a. Los controles (ej. firewalls) deben ser implementados para proteger los dominios internos de acceso no autorizado, incluyendo acceso por los suscriptores y las terceras partes confiantes. Los Firewalls deben ser también configurados para inhibir todos los protocolos y accesos no requeridos para la operación de la TSA.

b. La TSA deberá garantizar una administración efectiva de usuarios (esto incluye operadores, administradores y auditores) acceso para mantener la seguridad de los sistemas, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o remoción de accesos.

c. La TSA debe asegurar el acceso a la información y que las funciones de las aplicaciones están restringidas de acuerdo con la política de control de acceso, y que la TSA provee de controles de seguridad suficientes tomando en consideración los roles definidos por las prácticas, incluyendo la separación de funciones de administración y operación.

d. Todo el personal de TSA debe ser identificado y autenticado antes de usar aplicaciones críticas relacionadas con el servicio de Sello de Tiempo.

e. El personal de TSA debe ser responsable de todas sus actividades, por ejemplo, registrando todo el detalle de las actividades por medio de un log.

Los siguientes controles deben ser aplicados a la gestión del servicio de Sello de Tiempo:

f. La TSA debe asegurar que los componentes de red (Routers, Firewalls, IPS, WiFi) están en un lugar físico seguro y que sus configuraciones son auditadas en forma periódica según lo definido en las políticas de seguridad.

g. Se debe realizar un monitoreo permanente de las alarmas para detectar, registrar y reaccionar en forma rápida ante un acceso no autorizado. Se puede usar, por ejemplo, un sistema de detección de intrusos (IDS), monitoreo de control de acceso y sistemas de alarmas.

10.4.7. Implementación y mantenimiento de sistemas confiables

La TSA utilizará sistemas y productos confiables que estén protegidos contra la modificación. El análisis de riesgo llevado a cabo en los servicios de la TSA debe identificar sus servicios críticos que requieren sistemas confiables y los niveles de aseguramiento requeridos.

En particular:

a. Se llevará a cabo un análisis de los requisitos de seguridad en la etapa de diseño y especificación de requisitos de cualquier sistema/proyecto de desarrollo emprendido por la TSA o en nombre de la TSA para garantizar que la seguridad está incorporada en los sistemas de TI.

b. Se aplicarán procedimientos de control de cambios para las liberaciones, modificaciones y correcciones de software de emergencia de cualquier sistema operativo.

10.4.8. Compromiso de los servicios de la TSA

La TSA se asegurará en el caso de eventos que afecten la seguridad de los servicios de la TSA, incluido el compromiso de la llave privada de TSU o pérdida de calibración detectada, que la información relevante es puesta a disposición de los suscriptores y usuarios de confianza.

En particular:

a. El plan de recuperación de desastres de la TSA deberá abordar el compromiso o sospecha de compromiso de las claves de firma privadas de TSU o pérdida de calibración de un reloj TSU, que puede haber afectado la marca de time-stamp que han sido emitidas

b. En el caso de un compromiso, o sospecha de compromiso o pérdida de calibración, la CST pondrá a disposición de todos los suscriptores y partes de confianza una descripción del compromiso ocurrido.

c. En el caso de compromiso con la operación de una TSU (por ejemplo, la clave de la TSU se ve comprometida), sospecha de pérdida o compromiso de la calibración del TSU, no se emitirán time-stamp tokens hasta que se tomen medidas para recuperar la operación comprometida.

d. En caso de mayor compromiso de la operación de la TSA o pérdida de calibración, siempre que sea posible, la CST pondrá a disposición toda la información de los suscriptores y partes confiables para identificar las time-stamp tokens que pueden haber sido afectados, a menos que esto infrinja la privacidad de los usuarios de TSA o la seguridad de los servicios TSA.

e. En caso de compromiso o sospecha de compromiso de la llave privada de la TSA, se debe revocar el certificado de la TSA. En caso de que la clave privada se vea comprometida, una auditoría del rastro de todas las fichas generadas por la CST puede proporcionar un medio para distinguir entre tokens retroactivos genuinos y falsos. Dos tokens de sello de tiempo de dos TSA diferentes pueden ser otra forma de resolver esta situación.

10.4.9. Cese de la TSA

La TSA garantizará que las posibles interrupciones de los suscriptores y las partes confiantes se minimizan como resultado del cese de los servicios de sellado de tiempo de TSA, y en particular, aseguran la continuidad y mantenimiento de la información requerida para verificar la corrección de time-stamp tokens.

En particular:

a. Antes de que la TSA termine sus servicios de sellado de tiempo, como mínimo se ejecutarán los siguientes procedimientos:

- La TSA pondrá a disposición de todos los suscriptores y confiando información de las partes concerniente a su terminación;
- La TSA dará por terminada la autorización de todos los subcontratistas para actuar en nombre de la TSA en el desempeño de cualquier función relacionada con el proceso de emisión de fichas de sello de tiempo;
- La TSA transferirá las obligaciones a una parte confiable para mantener el registro de eventos y los archivos de auditoría necesarios para demostrar el funcionamiento correcto de la TSA durante un período razonable;
- La TSA mantendrá o transferirá a una parte confiable sus obligaciones de poner a disposición su clave pública o sus certificados a las partes confiables durante un período razonable;
- Las claves privadas de la TSU, incluidas las copias de seguridad, se destruirán de tal manera que las claves privadas no puedan recuperarse.

b. La TSA deberá tener un acuerdo para cubrir los costos para cumplir con estos requisitos mínimos en caso de que la TSA se declare en bancarrota o por otros motivos no pueda cubrir los costos por sí misma.

c. La TSA deberá indicar en sus prácticas las disposiciones hechas para la terminación del servicio. Esto incluirá:

    - Notificación de las entidades afectadas;
    - Transferencia de las obligaciones de la TSA a otras partes.

d. La TSA deberá tomar medidas para que los certificados de la TSU sean revocados.

10.4.10. Cumplimiento de los requisitos legales

La TSA debe garantizar cumplimiento con los requerimientos legales.

En particular:

a. La TSA debe garantizar que los requerimientos de Directivas Europeas de protección de datos [Dir 95/46/EC], se cumple mediante legislación nacional.

b. Se adoptarán las medidas técnicas y organizativas adecuadas contra el tratamiento no autorizado o ilegal de los datos personales y contra la pérdida accidental o la destrucción o daño a datos personales.

c. La información aportada por los usuarios a la TSA será completamente protegida de divulgación menos con su consentimiento o por orden judicial u otro requisito legal.

10.4.11. Registro de Información de las operaciones del Servicio de Sellado de Tiempo

La TSA se asegurará de que toda la información pertinente sobre el funcionamiento de los servicios de sellado de tiempo se registra durante un período definido de tiempo, en particular para el propósito de proporcionar evidencia de los efectos de los procedimientos legales.

En particular:

a. Los eventos y datos específicos que se van a registrar serán documentados por la TSA.

b. La confidencialidad y la integridad de los registros actuales y archivados referente a la operación de los servicios de sellado de tiempo serán mantenidos.

c. Los registros relativos a la gestión de servicios de sellado de tiempo deberán archivarse por completo y de forma confidencial de acuerdo con prácticas comerciales de divulgación.

d. Los registros relativos a la gestión de servicios de sellado de tiempo, deberán estar disponibles, si se requiere, para los fines de proporcionar evidencia de la operación correcta de los servicios de sellado de tiempo a los efectos de los procedimientos judiciales.

e. Se debe registrar la hora exacta de eventos significativos del entorno de la TSA, de la gestión de claves y sincronización de reloj.

f. Los registros relativos a los servicios de sellado de tiempo, se mantendrán por un período de tiempo, después de la expiración de la validez de la clave de firma de la TSU, según corresponda. Para proporcionar evidencia legal necesaria y según lo notificado en la declaración de divulgación de la TSA.

g. Los eventos serán registrados de un modo que no pueden ser fácilmente borrados o destruidos, excepto si se transfieren de forma fiable a medios de largo plazo, dentro del

período de tiempo que se requiere que sean mantenidos. Estos pueden ser resguardados, por ejemplo, mediante el uso de medios de sólo escritura, un registro de cada medio extraíble utilizado y la utilización de copias de seguridad fuera del sitio.

h. Cualquier información registrada sobre los suscriptores será confidencial, excepto cuando el acuerdo es obtenido por publicaciones del suscriptor.

Administración de la clave de la TSU

i. Los registros relativos a todos los eventos relacionados con el ciclo de vida de las claves TSU serán registrados.

j. Los registros relativos a todos los eventos relacionados con el ciclo de vida de los certificados TSU (en su caso) serán registrados.

Sincronización del Reloj

k. Los registros relativos a todos los eventos relacionados con la sincronización del reloj de una TSU a UTC serán registrados. Esto incluirá información relativa a la recalibración o la sincronización de los relojes normales utilizar en sellado de tiempo.

l. Se registrará los registros relativos a todos los eventos relacionados con la detección de pérdida de sincronización.

10.5 ORGANIZACIÓN

La TSA se asegurará de que su organización es confiable.

En particular, que:

a. Políticas y procedimientos bajo los cuales opera la TSA deberán ser no discriminatorios.

b. La TSA hará que sus servicios sean accesibles para todos los solicitantes cuyas actividades están comprendidas en su ámbito declarado de funcionamiento y que se comprometen a cumplir con sus obligaciones según lo especificado en la declaración de divulgación de la TSA.

c. La TSA es una persona jurídica de acuerdo a la legislación nacional.

d. La TSA tiene un sistema o sistemas de gestión de seguridad de la calidad y la información adecuada para los servicios de sellado de tiempo que está proporcionando.

e. La TSA cuenta con mecanismos adecuados para asumir las responsabilidades derivadas de sus operaciones y / o actividades.

f. Tiene la estabilidad financiera y los recursos necesarios para operar en conformidad con esta política. Esto incluye los requisitos para la terminación de la TSA. Se emplea un número suficiente de personal que tiene la educación necesaria, formación, conocimientos técnicos y experiencia relacionada al tipo, variedad y volumen de trabajo necesario para proporcionar el servicio de sellado de tiempo.

   El personal empleado por una TSA incluye personal individual contractualmente comprometidos al desempeñar funciones de apoyo a los servicios de la TSA de sellado de tiempo. El personal que pueda estar involucrado solamente en el seguimiento de los servicios de la TSA no tiene que ser el personal de TSA.

g. Se cuenta con políticas y procedimientos para la resolución de quejas y disputas recibidas de los clientes o de otras partes de la provisión de los servicios de sellado de tiempo o cualquier otro asunto relacionado.

h. Tiene un acuerdo debidamente documentado y relación contractual en el lugar donde el aprovisionamiento de los servicios implica subcontratación, tercerización u otros acuerdos de terceros.

11. Consideraciones de Seguridad

Al verificar tokens de sello de tiempo es necesario para el verificador asegurarse que el certificado de la TSU es confiable y no está revocado.

Esto significa que la seguridad, depende de la seguridad de la CA que ha emitido el certificado de la TSU, tanto para la emisión del certificado y proporcionar información precisa del estado de revocación de dicho certificado.

Cuando un sello de tiempo es verificado como válido en un punto dado del tiempo, esto no quiere decir que necesariamente permanecerá válido después. Cada vez, que un token de sello de tiempo se verifica durante el período de validez del certificado de TSU, este debe ser verificado nuevamente contra la información de estado de revocación más reciente, ya que, en caso de compromiso de una clave privada de la TSU, todos los tokens de sello de tiempo generadas por esta TSU pierden su validez.

En la aplicación de sellado de tiempo en aplicaciones, consideraciones de seguridad también deben ser tomadas en las aplicaciones. En particular, cuando la aplicación de sellos de tiempo, es preciso asegurar que la integridad de los datos se mantiene antes de aplicar el sello de tiempo.

El solicitante debe realmente asegurarse que el valor hash incluido en el token de sello de tiempo coincide con el hash de los datos.

12. Auditorías

Los procedimientos y frecuencia de las Auditorías de la Entidad Acreditadora dependiente del Ministerio de Economía están regidos por las guías de acreditación y a lo informado en la página web www.entidadacreditadora.gob.cl.

13. Administración y Modificaciones

IDOK podrá hacer cambios en sus procedimientos manteniendo siempre los estándares exigidos y justificables desde un punto de vista Técnico, Comercial y/o Jurídico, las veces que estime conveniente y debidamente publicado.

14. Publicación de Modificaciones

Todo cambio en la CP o CPS o cualquier política que involucre directamente la operación de los certificados será informada por los canales adecuados a todos sus suscriptores y solicitantes en un período no superior a 10 días hábiles desde la aplicación de los cambios.
Luego del comunicado, y si no se recibe ninguna declaración por escrito de suscriptores o solicitantes en contra de lo comunicado, las modificaciones se declararán como aceptadas por la comunidad de usuarios.