Política de sellado de tiempo del Sistema Nacional de Certificación Digital

Dirección de Certificadores de Firma Digital
Ministerio de Ciencia y Tecnología

OID 2.16.188.1.1.1.5
Versión: 1.00
04 de setiembre, 2008


MICIT
Ministerio de
Ciencia y Tecnología

Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
26-10-07	**Consulta pública**	**Comité de Políticas Comité Técnico**	**Lic.Oscar Solís Director DCFD**	**Se presenta la versión de las Políticas de Sellado de Tiempo y se obtiene la aprobación del Director de la DCFD.**
03-12-07	**Borrador**	**Comité de Políticas**	**Lic.Oscar Solís Director DCFD**	**Se incorporan las observaciones de la consulta pública, de acuerdo al edicto publicado el día lunes 19 de noviembre del 2007 en el diario oficial "La Gaceta", número Nº 222**
04-09-08	**1.00**	**Comité de Políticas**	**Lic.Oscar Solís Director DCFD**	**Oficialización y entrada en vigencia de las políticas.**

Índice

1. Introducción

Este documento define las políticas de sellado de tiempo para la emisión del certificado de autoridades de sellado de tiempo (TSA) referenciado en el documento de "Políticas de Certificación del Sistema Nacional de Certificación Digital" del gobierno de Costa Rica.

La autoridad de sellado de tiempo debe implementar las políticas definidas en este documento para poder registrarse ante la Dirección de Certificadores de Firma Digital (DCFD).

En el siguiente gráfico se muestra la ubicación de una autoridad de sellado de tiempo en la jerarquía nacional de certificadores registrados:

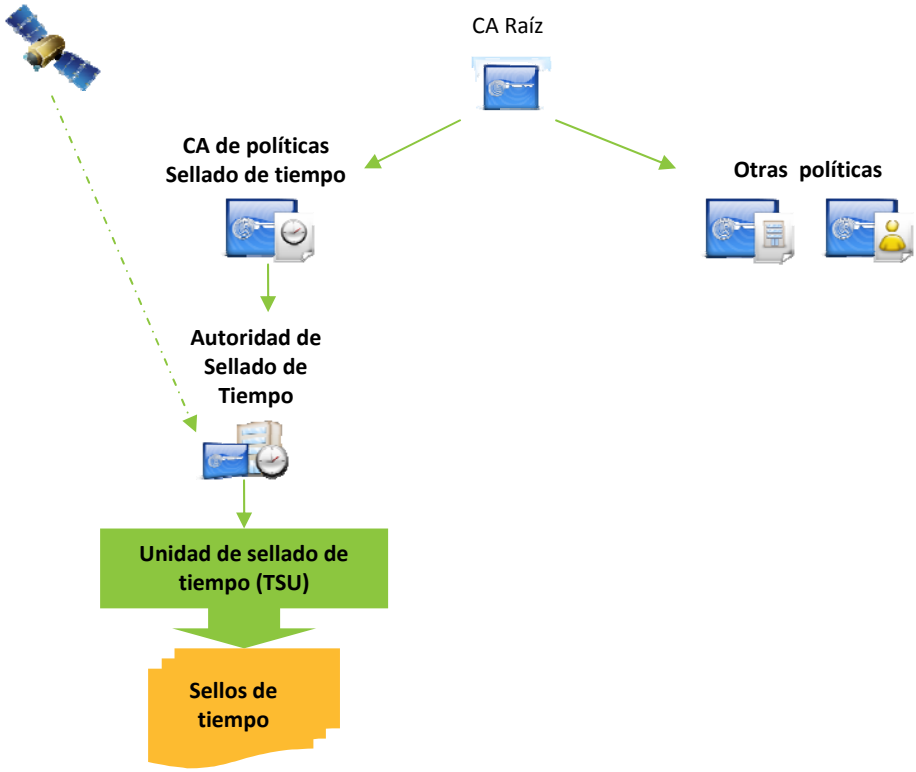

Diagrama N.1: Autoridad de sellado de tiempo del sistema nacional de certificación digital

Adicionalmente, para la implementación de la política de sellado de tiempo se debe cumplir con el protocolo definido por el RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

1.1 Administración de la Política

1.1.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia y Tecnología, dirección: San José, 50 metros Este del Museo Nacional. Apartado Postal: 5589-1000 San José, Costa Rica. Correo Electrónico: informacion@firmadigital.go.cr

1.1.2 Persona de contacto

Jefatura de la Dirección de Certificadores de Firma Digital Director de Certificadores de Firma Digital, Correo Electrónico: informacion@firmadigital.go.cr. Tel. (506) 2248-1515, ext. 115.

2. Resumen

Este CP especifica los requerimientos para una Autoridad de Sellado de Tiempo (TSA), tales como requisitos para la sincronización del tiempo, el sistema de emisión de los sellos de tiempo, y otros requerimientos específicos para el proceso de sellado de tiempo de un documento o dato.

3. Definiciones y abreviaturas

3.1 Definiciones

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

- 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 TSA 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: Objeto de datos 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 token de sellado 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 (por ejemplo: UTC-6 para Costa Rica). 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.

3.2 Abreviaturas

Abreviatura	Descripción
TSA	**Autoridad de Sellado de Tiempo (Time-Stamping Authority)**
TSU	**Unidad de Sellado de Tiempo (Time-Stamping Unit)**
TST	**Token de Sellado de Tiempo (Time-Stamp Token)**
UTC	**Tiempo Universal Coordinado (Universal Time Coordinated)**
TSS	**Servicios de Sellado de Tiempo (Time Stamping Services)**

4. Conceptos Generales

4.1 Servicios de Sellado de Tiempo (TSS)

El servicio de Sellado de Tiempo (TSS) se encarga de recibir la solicitud de sellado de tiempo de un suscriptor, verifica los parámetros de la solicitud y genera el token de sellado de tiempo, de acuerdo a las políticas de estampado de tiempo.

Además, cuenta con mecanismos control para garantizar el acceso a fuentes de tiempo confiables, servicios criptográficos y del sistema de validación.

4.2 Autoridad de Sellado de Tiempo (TSA)

La TSA es la autoridad en la que confían los usuarios de los servicios de sellado de tiempo (suscriptores y partes que confían) para la emisión de los sellos de tiempo. La TSA tiene responsabilidad total en la provisión del servicio de sellado de tiempo que se identifica en la cláusula 4.1.

Una TSA puede operar diferentes TSU, donde cada unidad tiene un par de llaves diferentes. Es decir, una TSA puede tener varios certificados de sellado de tiempo según sean sus necesidades.

El proceso de sellado de tiempo sigue los siguientes pasos:

- El subscriptor del servicio realiza una petición de sellado de tiempo para un dato (hash), y para esto prepara la solicitud de acuerdo con el "*Timestamp Request*" definido en el RFC 3161.
- La autoridad de sellado de tiempo se encarga de:
    - Revisa si la petición está completa y correcta. Si el resultado es positivo, el dato (hash) se envía como entrada a la Unidad de Sellado de Tiempo.
    - Obtiene la hora oficial de una fuente confiable de tiempo
    - Crea un sello de tiempo que asocie el instante de tiempo actual, un número de serie único y el dato (hash) proporcionado para el sellado de tiempo, garantizando el cumplimiento de los requerimientos de esta política.
    - Crea el token de sellado de tiempo que se devolverá al subscriptor del servicio que realizó el pedido. En este momento se genera la firma criptográfica del sello de tiempo.
- El suscriptor recibe el token de sellado de tiempo
- Las partes que confían verifican el sello de tiempo

El proceso de sellado de tiempo se observa en el siguiente diagrama:

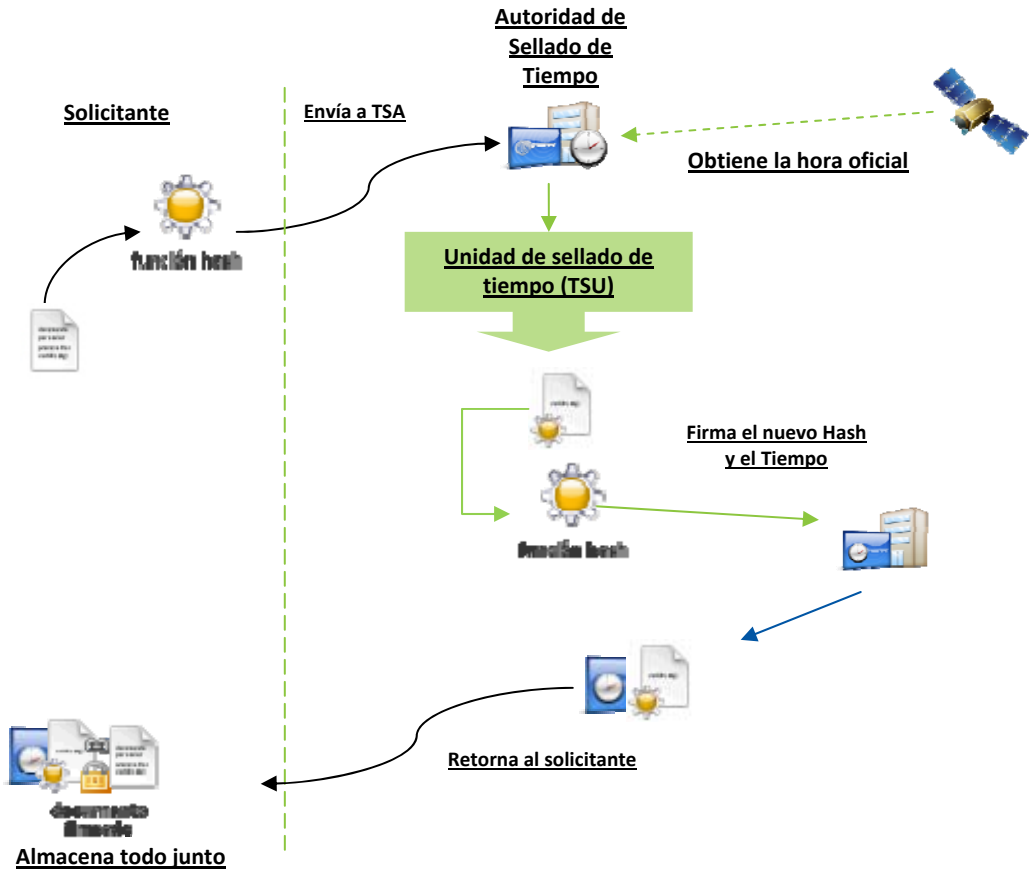

Diagrama N.2: Proceso de sellado de tiempo de una Autoridad de Sellado de Tiempo (TSA)

El proceso de verificación de un sello de tiempo de una parte que confía es mostrado en el siguiente diagrama:

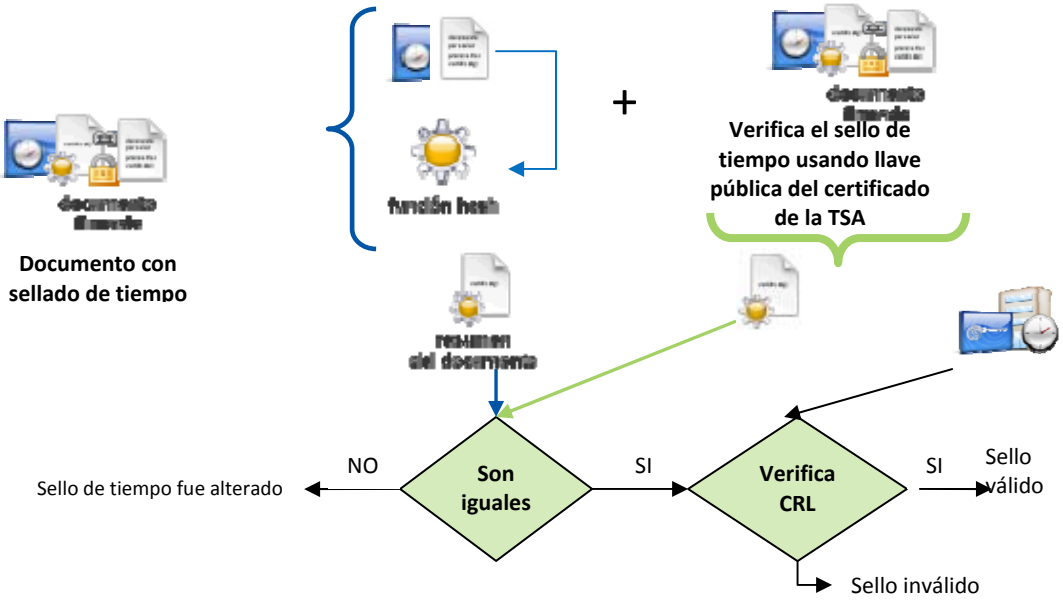

Diagrama N.3: Proceso de verificación de un sello de tiempo

4.3 Suscriptores

Los suscriptores de este servicio son los organismos o entidades finales, que han suscrito el correspondiente acuerdo de suscriptor que les permite acceder a estos servicios de firma electrónica.

4.4 Política de Sellado de Tiempo y la Declaración de prácticas de la TSA

Estos documentos explican los roles relativos a la política de sellado de tiempo. En este caso, cualquier entidad que desea ser una TSA registrada debe probar que su declaración de prácticas de TSA se adhiere a esta política. El cumplimiento de los procedimientos y su adherencia a las políticas debe ser aprobada por la DCFD, posterior al estudio de cumplimiento de la competencia técnica y administrativa realizado por el ECA.

5. Políticas de Sellado de Tiempo

5.1 Resumen

Las políticas definidas para el sellado de tiempo establecen reglas particulares a las definidas en el documento general de Políticas para el Sistema Nacional de Certificación Nacional, y en particular establece el conjunto de reglas utilizadas durante la emisión y el control de los token de sellado de tiempo (TST), y además de regular el nivel de seguridad requerido para la TSA.

5.2 Identificación

De acuerdo con la sección 1.2 Nombre e Identificación del Documento de las Políticas del Sistema Nacional de Certificación, se le asigna el siguiente OID a las políticas del Certificado de TSA:

OID	Descripción
2	**joint-iso-itu-t**
16	**country**
188	**Costa Rica**
1	**Organización**
1	**Dirección de Certificadores de Firma Digital**
1	**Políticas**
1	**Política de certificados para la jerarquía nacional de certificadores registrados**
5	**Política de sellado de tiempo del sistema nacional de certificación digital**

5.3 Comunidad de usuarios y aplicabilidad

Esta política de sellado de tiempo tiene como objetivo cumplir con los requerimientos de las firmas digitales de sellado de tiempo para largos periodos de validez, y por estar dentro de la jerarquía nacional de certificación poseen las características para garantizar no repudio en los procesos que requieran la certificación del tiempo.

5.4 Cumplimiento

La TSA debe implementar los controles y procedimientos identificados en esta política para garantizar la confianza en los sellos de tiempo que emite.

6. Obligaciones y responsabilidades

6.1 Obligaciones de la TSA

6.1.1 General

La TSA que implementa esta política está obligada a:

- Realizar sus operaciones en conformidad con esta política.
- Proteger sus llaves privadas emitidas para cada TSU.
- Emitir sellos de tiempo 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 certificación a los que sirven de soporte.
- Garantizar que puede determinarse con precisión la fecha y la hora a la que se emitió un sello de tiempo.
- Publicar esta política y los documentos relacionados en el sitio Web, garantizando el acceso a la versión actual del documento de políticas de sellado de tiempo y de las políticas del sistema nacional de certificación digital.
- Garantizar que todos los requerimientos de la TSA, incluidos procedimientos, prácticas relativas a la emisión de token y revisión de sistemas están conforme se describe en los documentos operacionales, de procedimiento y técnicos del sistema nacional de certificación digital.

6.1.2 Obligaciones de la TSA hacia sus suscriptores

La TSA debe garantizar el acceso permanente a los servicios de sellado de tiempo que proporciona un tiempo de servicio (uptime) superior al 90%, excluyendo procesos de mantenimiento de sistemas y equipos. Los procesos de mantenimiento técnicos deberán planificarse con la suficiente antelación, tener una duración determinada y avisar a los subscriptores del servicio, utilizando los medios de difusión disponibles.

La TSA debe garantizar los siguientes aspectos:

- Que el tiempo UTC incluido en los sellos de tiempo, asegura una desviación máxima de 500 milisegundos.
- Que los sistemas utilizados en la provisión de estos servicios se ajustan a lo contemplado en la normativa legal.
- Que el valor de tiempo es fiable en cada token de sellado de tiempo emitido.

- Que los sellos de tiempo son firmados usando una llave privada generada exclusivamente para este propósito.
- Que no se emitan sellos de tiempo si el certificado de la TSA está vencido o ha sido revocado.
- Que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo (TSA).

6.2 Obligaciones del suscriptor

En el proceso de obtención de un sello de tiempo, los subscriptores deben verificar la firma electrónica de la TSA y comprobar en la CRL el estado del certificado de la TSA.

6.3 Obligaciones de partes que confían

Las partes que confían deben verificar la firma del sello de tiempo, comprobar el estado del certificado de la TSA y su periodo de validez.

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.

6.4 Responsabilidades

Las responsabilidades generales de la TSA se documentan en la política del Sistema Nacional de Certificación Digital.

En particular la TSA debe responsabilizarse de:

- Emitir los token de sellado de tiempo que pueden identificarse en forma unívoca.
- Mantener el tiempo UTC de los sellos de tiempo dentro del margen de desviación definido en este CP.
- Comunicar al suscriptor las responsabilidades y deberes asumidos con el uso del servicio de sellado de tiempo, en el acuerdo de suscriptor.
- Implementación de los controles requeridos por esta política para emitir los token de sellado de tiempo de acuerdo a este CP.
- Proteger información confidencial o privada.

7. Requerimientos en prácticas de la TSA

7.1 Prácticas y declaraciones de divulgación

7.1.1 Declaración de prácticas de TSA

La TSA que desea registrarse ante la DCFD debe implementar los controles necesarios para garantizar la fiabilidad y confianza del servicio, de acuerdo a las políticas del sistema nacional de certificación digital y de este documento. Estos controles deben especificarse en el documento de la "declaración prácticas de la TSA".

7.1.2 Declaración de divulgación de TSA

Para el caso del sistema nacional de certificación digital, este documento se considera opcional.

7.2 Gestión del Ciclo de vida de las llaves

7.2.1 Generación de la llave de la TSU

La generación de la llave de la Unidad de Sellado de Tiempo asociada a la TSA, debe cumplir con lo especificado en las secciones del documento de política del sistema nacional de certificación digital:

- 5.2 para controles procedimentales, y
- 6.1.1 para la generación del par de llaves

7.2.2 Protección de la llave privada de la TSU

Los niveles de seguridad para la protección de la llave privada deben cumplir con este documento de políticas y las secciones del documento de política del sistema nacional de certificación digital:

- 4.12 de custodia y recuperación de la llave, y
- 6.2.1 de estándares y controles del módulo criptográfico.

7.2.3 Distribución de la llave pública de la TSU

La distribución de la llave pública de la Unidad de Sellado de Tiempo de una TSA debe cumplir lo estipulado en las secciones de la política del sistema nacional de certificación digital:

- 6.1.3 para la entrega de la llave pública al emisor del certificado, y
- 6.1.4 entrega de la llave pública de la CA a las partes que confían.

7.2.4 Re-emisión de llaves de la TSU

La re-emisión de llaves no se implementa como parte del sistema nacional de certificación digital.

7.2.5 Terminación del ciclo de vida de la llave del TSU

La TSA debe asegurarse que las llaves privadas de firma de la Unidad de Sellado de Tiempo no puedan ser utilizadas más allá del periodo de expiración. En particular la TSA debe cumplir con lo estipulado en sección 6.2.10 método de destrucción de la llave privada de la política nacional de certificación digital.

7.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sellado de tiempo

La TSA debe operar los dispositivos criptográficos de acuerdo a las especificaciones de la sección 6.2 para los controles de ingeniería del módulo criptográfico y protección de la llave privada del documento de políticas del sistema nacional de certificación digital.

7.3 Sellado de tiempo

7.3.1 Token de sellado de tiempo

La TSA debe garantizar que los token de sellado de tiempo son emitidos en forma segura y que incluyen la hora oficial de Costa Rica. En particular cada sello de tiempo emitido por la TSA debe incluir:

- El OID de la política de sellado de tiempo de la jerarquía nacional de certificadores registrados.
- Contener un identificador único dentro de la TSA.
- Valores de fecha y hora identificables, mediante los cuales se puede llegar al valor de tiempo UTC.
- El tiempo debe estar sincronizado con el tiempo UTC.
- Una representación (por ejemplo, valor hash) del dato que desea ser sellado, el cual es proveído por el solicitante.
- El identificador de la TSA y de la TSU que lo emite.

Adicionalmente la TSA debe garantizar que:

- Si es imposible la obtención de la exactitud requerida para el tiempo entonces el sello de tiempo no podrá ser emitido.

- El token de sellado de tiempo es firmado por una llave generada exclusivamente para este propósito.

7.3.2 Sincronización de los relojes con UTC

La TSA debe asegurar que su reloj está sincronizado con el tiempo UTC, con una exactitud menor a un segundo, y establecer los controles para:

- La calibración del reloj de la TSU debe ser mantenida dentro de los límites definidos por este CP y por distintos caminos, utilizando como referencia el tiempo UTC para fijar el tiempo oficial.

- El reloj de la TSU debe ser protegido contra amenazas que podrían resultar en el cambio del tiempo fuera de la calibración o por la manipulación física de los sistemas.

- La TSA debe asegura que las diferencias entre el sistema del tiempo de la TSU y el tiempo UTC sean detectadas. El cálculo de tiempo cumple con las recomendaciones de NTP (Network Time Protocol) y de la Oficina de Pesos y Medidas (BIPM = Bureau International des Poids et Mesures).

- La TSA debe asegurar que la sincronización del reloj es mantenida cuando se presenten “segundos intercalares” (leap second) notificados por el organismo apropiado. Dos veces al año, durante el último minuto de los días 30 de junio y 31 de diciembre, se realizan los ajustes automáticos para asegurar que la diferencia acumulada entre UTC y UT1 no excederá a 0.9 segundos antes del próximo ajuste programado. La TSA debe mantener un registro del tiempo exacto (dentro de la exactitud declarada) cuando estos cambios ocurran.

7.4 Gestión de la TSA y operaciones

7.4.1 Gestión de seguridad

Todos los elementos relativos al control de la seguridad se describen en la política del sistema nacional de certificación digital específicamente en la sección 5.2 de controles procedimentales, y de la sección 6.6.2 controles de gestión de seguridad.

7.4.2 Gestión y clasificación de activos

La TSA debe asegurar que su información y otros activos reciban un nivel apropiado de protección. En particular, debe mantener el inventario de todos los activos y quién los tiene asignados de acuerdo al análisis de riesgo efectuado.

7.4.3 Seguridad del personal

Las características del personal son establecidas por la política del sistema nacional de certificación digital, en la sección 5.3 controles de personal. Dentro de los requerimientos de conocimiento del personal se encuentran:

- tecnología de sellado de tiempo.
- tecnología de firma digital.
- mecanismos de calibración o sincronización de los relojes de la TSU con el UTC.
- seguridad de la información y valoración de riesgos.
- procedimientos de seguridad para el personal con roles de confianza.

7.4.4 Seguridad física y ambiental

La descripción de la seguridad física se encuentra documentada en la sección 5.1 de las políticas del sistema nacional de certificación digital.

7.4.5 Gestión de las operaciones

La TSA debe implementar los controles de seguridad definidos por la política del sistema nacional de certificación digital para todas las operaciones de emisión de los token de sellado de tiempo, en particular:

- Auditorias internas al sistema de la TSA.
- Reportes de incidentes y procedimientos de respuesta.
- Monitoreo de las transacciones.

7.4.6 7.4.6 Gestión de acceso a los sistemas

Los controles de acceso a los sistemas son determinados dentro de la política nacional de certificación digital en la sección 6.5 controles de seguridad del computador.

7.4.7 Mantenimiento e implantación de sistemas de confianza

El mantenimiento e implantación de los sistemas de la TSA deben cumplir con las estipulaciones de la política nacional de certificación digital en la sección 6.6.1 controles para el desarrollo de sistemas.

7.4.8 Compromiso de los servicios de TSA

En caso de compromiso de los servicios de sellado de tiempo, se deberá seguir lo estipulado en la sección 5.7 recuperación de desastre y compromiso de la política del sistema nacional de certificación digital.

7.4.9 Terminación de una TSA

La TSA debe garantizar el mínimo impacto en caso de un cese de actividades. En particular, debe cumplir con los aspectos que una CA requiere para el cese de funciones y que están documentados como parte de la política del sistema nacional de certificación digital, en la sección 5.8 terminación de una CA o RA.

7.4.10 Cumplimiento de requerimientos legales

Sin estipulaciones.

7.4.11 Registro de información concerniente a las operaciones del servicio de sellado de tiempo

La TSA debe incorporar los mecanismos para la creación y control de las bitácoras de auditoría, con los eventos que han sido derivados de su operación, los cuales deben estar de acuerdo a la sección 5.4 procedimientos de bitácora de auditoría del documento de políticas del sistema nacional de certificación.

La TSA debe asegurar que toda la información relevante concerniente a los Tokens de Sellado de Tiempo (TST) son almacenados por el período de tiempo apropiado, en particular para:

- Operaciones de la TSA:
    - Los datos y eventos específicos a ser registrados en bitácoras deben ser documentados por la TSA;
    - La confidencialidad y la integridad de los registros actuales y los archivados relativos a la operación de servicios de la TSA deben ser mantenidos;
    - Los registros concernientes a la operación de servicios de la TSA debe estar almacenados completa y confidencialmente;
    - Los registros concernientes a la operación de servicios de la TSA debe estar disponible si fueron almacenados para el propósito de evidencias de pruebas de la correcta operación de los servicios de la TSA con el objetivo de actos jurídicos;
    - El tiempo preciso de eventos de sincronización del reloj deben ser registrados;

- Los registros concernientes a los servicios de la TSA deben estar retenidos por el período de tiempo posterior al vencimiento del certificado de la TSA para proveer la evidencia legal necesaria;

- Los eventos deben ser registrados al sistema de manera que no puedan ser fácilmente eliminados o destruidos dentro del período de tiempo que están obligados a ser retenidos; y

- Cualquier información grabada acerca de Suscriptores deben ser mantenida confidencial excepto cuando un contrato del Subscriber permita su publicación.

- Gestión de la llave de la TSA

  - los registros concernientes a todos los eventos referentes al ciclo de vida de las llaves de la TSA deben ser puestos en bitácora; y

  - los registros concernientes a todos los eventos del ciclo de vida de los certificados de la TSA deben ser puestos en bitácora.

- Sincronización de los relojes

  - Los registros concernientes a todos los eventos de sincronización del reloj de la TSA para asignar el UTC deben ser puestos en la bitácora. Esto incluirá la información concerniente a la sincronización o calibración normal de relojes usados en el estampado de tiempo ; y

  - los registros concernientes a todos los eventos relacionados para la detección de pérdida de sincronización deben ser puestos en bitácora.

7.5 Organización

Las autoridades de sellado de tiempo se encuentran incluidas dentro de la jerarquía nacional de certificadores registrados, bajo una política particular de sellado de tiempo, y se adhieren a las políticas dictadas por la Dirección de Certificadores de Firma Digital (DCFD).