Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

OID: 2.16.484.101.10.316.2.5.1.3.1.1.2

Versión 1.3

Tabla de Contenidos

1. Administración de la Documentación

I. Manejo de Versiones

El presente documento será considerado válido y con vigencia siempre que los cambios hayan sido autorizados y aprobados por los responsables definidos en la siguiente sección

El presente documento deberá ser revisado dos veces al año, lo cual no implica una actualización del mismo.

II. Control de Versiones

El manejo de versiones para la documentación sigue el cumplimiento de políticas definidas para la asignación de un número de versión, de acuerdo a:

Se incrementa un número entero cuando

- Un cambio o mejora grande ocurre en la documentación.
- Un conjunto de características, que han sido planeadas, han sido implementadas.
- La estructura del documento cambia.
- Si el contenido del documento cambia en un 40% será necesario incrementar el número de versión con un número entero.

Se incrementa con un decimal sobre la versión del documento cuando

Se incrementa para distinguir múltiples liberaciones de la actualización de la documentación.
Este número indica mejoras o cambios menores en el contenido de la documentación.
Si el contenido del documento cambia en un porcentaje menor al 40%, será necesario incrementar el número de versión con un número decimal.

VERSIÓN	FECHA DE	CAMBIO EN EL DOCUMENTO
1.0	13-JUNIO-2011	DOCUMENTO INICIAL

1.1	**13-SEPTIEMBRE-2011**	**MODIFICACIONES POR PREVENTORIO DE SECRETARIA DE ECONOMÍA**
1.2	**8-NOVIEMBRE-2011**	**ADECUACIONES POR REQUERIMIENTO DE INFORMACIÓN DE SECRETARIA DE ECONOMÍA**
1.3	**OCTUBRE 2020**	**ACTUALIZACION DEL CENTRO DE DATOS ALTERNO DE TULTITLAN A TULTITLAN** **ACTUALIZACION DE ESPECIFICACIÓN DE NOM 151 SCFI 2002 A NOM 151 SCFI 2016** **ADICION DE CALENDARIO DE REVISION DEL DOCUMENTO** **ACTUALIZACION DEL APARTADO 5 DE REFERENCIAS**

III. Lista de Distribución

Las copias en papel, medio magnético y electrónico de este documento están almacenadas en las siguientes localidades.

LOCALIDAD	DIRECCIÓN	RESPONSABLE	MEDIO DE ALMACENAMIENTO
CDMX	INSURGENTES SUR 2375	OLGA GARCIA	MAGNETICO Y PAPEL
CDMX	INTERLOMAS	MOISES BAUTISTA	MAGNETICO Y PAPEL

IV. Calendario de Revisiones del Documento

El documento se revisará al menos una vez al año para verificar que el contenido sea aplicable y funcional a la Infraestructura de Clave Pública, lo que no implica una actualización del mismo.

FECHAS PROGRAMADAS DE FUTURAS REVISIONES
01/02/2020
01/02/2021
01/02/2022
01/02/2023

2. Introducción

SeguriData Privada S.A. de C.V. está acreditada para el servicio de Expedición de certificados de FEA, y está en proceso para las acreditaciones de los servicios de Expedición de Constancias de Conservación de mensajes de datos de acuerdo a NOM-151-SCFI-2016 y de Expedición de Sellos Digitales de Tiempo, ante la Secretaria de Economía.

Este documento contiene las políticas que regirán el funcionamiento y operación para el servicio de Expedición de Sellos Digitales de Tiempo, basados en el uso de Criptografía de clave pública, Certificados Digitales y fuentes de tiempo confiables.

3. Objetivo

El documento de políticas para el Servicio de Expedición de Sellos Digitales de Tiempo, tiene el objetivo de presentar las reglas a seguir en los procesos de operación y administración del servicio de Expedición de Sellos Digitales de Tiempo.

4. Alcance

El documento de políticas para el servicio de Expedición de Sellos Digitales de Tiempo, define las obligaciones y responsabilidades necesarias para las prácticas de operación y administración de la Autoridad de Sellos Digitales de Tiempo, para que los Clientes tengan seguridad en la operación del servicio de Expedición de Sellos Digitales de Tiempo.

5. Referencias

La estructura de esta Política está basada en lo dispuesto por:

- Articulo 102 incisos A, Reformas al Código de Comercio. (publicado(a) en el Diario Oficial de la Federación el DOF 07-04-2016).
- Reglamento del Código de comercio en materia de Prestadores de Servicios de Certificación, publicado en el Diario oficial de la federación el DOF-19-07-2004
- Reglas generales a las que deben sujetarse los Prestadores de Servicios de Certificación , en su TITULO SEXTO referido a la Emisión de Sellos Digitales de Tiempo, publicado en el Diario oficial de la federación el DOF-14-05-2018
- RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

6. Definiciones y Conceptos

TÉRMINO	DEFINICIÓN
Secretaria de Economía	Es un órgano de la Administración Pública Federal Centralizada que coordina y actúa como Autoridad Certificadora y Registradora, respecto de los Prestadores de Servicios de Certificación, entre otros
Centro nacional de Metrología (CENAM)	Es el organismo descentralizado de la administración Pública federal, con personalidad jurídica y patrimonio propio, que tiene como función, entre otras, sincronizar el Tiempo UTC con el servidor TSA de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.
UTC	Tiempo Universal Coordinado Escala de Tiempo según lo definido en la recomendación TF.460-5 de ITU-R
USDT	Unidad de Sellos Digitales de Tiempo Sistema de hardware y de software que es administrado como una unidad y tiene una sola clave privada activa exclusiva para firmar los Sellos Digitales de Tiempo
SELLO DIGITAL DE TIEMPO	Sello Digital de Tiempo Es el mensaje de datos que vincula una representación de datos a una fecha y hora en particular, estableciendo así evidencia de que existió el dato.
Solicitante	Es la persona física o moral que inicia el trámite para obtener un Sello Digital de Tiempo.
Cliente - Suscriptor	A las personas físicas o morales que requieren los servicios proporcionados por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. y que han aceptado explícitamente sus términos y condiciones, definidos en el contrato para la prestación del servicio.
Segundo Intercalar	Es una corrección de un segundo necesario para mantener sincronizados los calendarios civiles basados en reloj atómico (UTC) con la escala de Tiempo basada en la rotación de la tierra
RFC 3161	(Request For Comments). Que establece el protocolo referente a la expedición de Sellos Digitales de Tiempo.
RFC 3628	(Request For Comments). Que define los requerimientos para establecer una política de Sellos Digitales de Tiempo para una Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.
Servidor TSA	Es el servidor de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., el cual se integra de una tarjeta PSI nShield 500e F3, software Time Stamping Option pack y el manejador de base de datos SQL Server 2005. En el documento lo llamaremos servidor TSA aunque este descrito por cada componente.
TSS –TSMC -TSM	TSS: Time Stamping Service

TÉRMINO	DEFINICIÓN
	TSMC: Time Source Master Clock TSM: Time Stamping Master
TAC	Una vez que se empieza a ajustar el TSS con TSMC (Se puede tardar un par de minutos) al momento de que ya se haya ajustado lo más cercano posible al tiempo del TSMC, entonces el emite un Certificado de Tiempo (TAC), esto quiere decir, que el tiempo de TSS es correcto conforme al tiempo de TSM
DRIFT	Se configura para determinar el rango de tiempo (segundos) que puede estar desfasado con el TSMC.
SECURITY WORLD	Entorno creado por Thales para el control sobre los procedimientos y protocolos que se requieren para crear, gestionar, distribuir y, en caso de desastre, recuperar claves, es decir, maneja la seguridad del ciclo de vida de las claves criptográficas.
SEE	Motor de ejecución segura (SEE, Secure Execution Engine). El motor de ejecución segura (SEE) es una función disponible en algunos módulos de seguridad del hardware de Thales la cual permite que el código de la aplicación que se ejecuta este dentro de los límites de seguridad del módulo.
Parte que confía	La persona que, siendo o no el Destinatario, actúa sobre la base de prestación del servicio de expedición de sellos digitales de tiempo
Firma electrónica avanzada	Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos: **I.** Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante; **II.** Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante; **III.** Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y **IV.** Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

7 Identificación de la Política para la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

Nombre del documento	Política para la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.
Versión del documento	1.3
Autor	SeguriData Privada S.A. de C.V.
Estado del documento	En operación
Fecha de emisión	8/noviembre /2011
Fecha de inicio de uso	30/enero/2012
Fecha de expiración	No es aplicable
Identificador de Objeto – OID (Object Identifier)	2.16.484.101.10.316.2.5.1.3.1.1.2
Localización (URL) de la Política para el servicio de Expedición de Sellos Digitales de Tiempo	https://psc.seguridata.com/docs/doc22.pdf
Declaración de Prácticas asociada a la Política para la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.	Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

La Política está dirigida a cumplir los requerimientos establecidos por la Secretaría de Economía, para brindar el servicio de Expedición de Sellos Digitales de Tiempo que se ofrece como Prestador de Servicios de Certificación.

El servicio de Sellos Digitales de Tiempo, está disponible para personas físicas y morales que requieran incorporar en sus procesos y/o servicios un Sello Digital de Tiempo y que estén de acuerdo en sujetarse a los términos y condiciones establecidos por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., en el contrato para la prestación del servicio.

8 Administración del Documento de Políticas para el Servicio de Expedición de Sellos Digitales de Tiempo

Responsable de la Administración de la Política	
Nombre	SeguriData Privada S.A. de C.V.
Correo electrónico	autoridad-sello@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.
Teléfono	(55) 3098-0700
Fax	(55) 3098-0702
Responsable de la administración del documento	Oficial de Seguridad oficial.seguridad@seguridata.com Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.

Persona de Contacto	
Nombre	Oficial de Seguridad
Correo electrónico	oficial.seguridad@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.

8.1 Determinación de Cambios a la presente Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

No aplica

9 Participantes en la Expedición de Sellos Digitales de Tiempo

La representación esquemática de los componentes involucrados en la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. Es la que se muestra en la figura 1.

En el nivel superior de la figura, se ubica la Autoridad Certificadora raíz y núcleo de confianza perteneciente a la Secretaría de Economía.

El segundo nivel corresponde a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, con el que se firmaran los Sellos Digitales de Tiempo expedidos

Figura 1

9.1 Autoridad Certificadora SeguriData

Es la entidad acreditada por la Secretaría de Economía para ofrecer el servicio de Expedición de Certificados Digitales a las personas y entidades que lo requieran

9.2 Secretaria de Economía

Es un órgano de la Administración Pública Federal Centralizada que coordina y actúa como Autoridad Certificadora y Registradora, respecto de los Prestadores de Servicios de Certificación, entre otros.

9.3 Centro Nacional de Metrología (CENAM)

Es el organismo descentralizado de la administración Pública federal, con personalidad jurídica y patrimonio propio, que tiene como función, entre otras, ofrecer el servicio de sincronía, a servicios relacionados con el tiempo, como por ejemplo, a equipos selladores digitales de tiempo.

9.4 Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

Autoridad acreditada por la Secretaría de Economía para emitir Sellos Digitales de Tiempo.

9.5 Clientes-Suscriptores

A las personas físicas o morales que requieren los servicios proporcionados por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. y que han aceptado explícitamente sus términos y condiciones, definidos en el contrato para la prestación del servicio.

9.6 Profesional Jurídico auxiliado por el Agente Certificador

El profesional jurídico y el Agente Certificador del servicio de emisión de certificados digitales, se ubican en las oficinas de SeguriData Privada S.A. de C.V. en Insurgentes Sur 2375 Piso 3, Colonia Tizapán, Delegación Álvaro Obregón, en México, Distrito Federal.

La misión y responsabilidad del profesional jurídico, es realizar las funciones de asistencia a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. en los procedimientos y trámites relacionados con los clientes para su identificación, garantizando con esto la correcta validación de la identidad de los solicitantes de los Sellos Digitales de Tiempo, delegando y auxiliándose del o los Agentes Certificadores del Servicio de emisión de certificados digitales.

Se define al Agente Certificador como apoyo al Profesional Jurídico, en los casos en que este último no se encuentre en las oficinas de SeguriData Privada S.A. de C.V., por causas de fuerza mayor, en el momento en que un cliente realice el trámite de contratación del Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. Sin embargo, el profesional Jurídico en primera instancia es el responsable de la identificación.

En un inicio el Agente Certificador será el actual del servicio de Expedición de certificados digitales, sin dejar de contemplar a los agentes certificadores que en un futuro se puedan dar de alta ante dicha Secretaria.

10 Política para el Servicio de Expedición de Sellos Digitales de Tiempo

El objetivo del sello digital de tiempo es dar certeza de la fecha y hora en que se origina una transacción, dicha fecha y hora es asignada por un emisor confiable como lo es el CENAM, y es firmado por una autoridad acreditada por Secretaria de Economía.

El propósito del sello digital de tiempo es contar con un registro de la fecha y hora en que se efectúa una transacción

La Política que se define, establece las reglas, obligaciones y responsabilidades para el servicio de Expedición de Sellos Digitales de Tiempo aplicables a los requerimientos técnicos de la organización y a los procedimientos relacionados con dicho servicio, complementándose con la Declaración de Prácticas para el Servicio de Expedición de Sellos Digitales de Tiempo donde se establecen los procedimientos operativos, y la forma en que se mantiene la exactitud del reloj, sincronizado con el CENAM, detallando términos y condiciones de operación definidos en el contrato para la prestación del servicio, así como el cumplimiento de lo establecido en la presente Política.

Se asegura el Servicio de Expedición de Sellos Digitales de Tiempo, emitiendo Sellos Digitales de Tiempo con una exactitud de ±1 mili segundo de tiempo con respecto a la fuente confiable de tiempo UTC y no emitirá Sellos Digitales de Tiempo fuera de este parámetro definido.

Se asegura que el Servicio de Expedición de Sellos Digitales de Tiempo cumple con el estándar internacional internet X.509 Public Key Infraestructure Time Stamp y los RFC 3161 y 3628, de acuerdo a lo mencionado en el anexo, del proveedor Thales, del servidor TSA.

Por otra parte se cumple con los mecanismos de seguridad para la no suplantación de Sellos Digitales de Tiempo, y la Trazabilidad de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., cumpliendo con:

a) Los de servicio de Expedición de Sellos Digitales de Tiempo usando SHA-256
b) Generación de reporte mensual de Sellos Digitales de Tiempo estampillado por otro PSC
c) Suspensión de Servicio de Expedición de Sellos Digitales de Tiempo por de sincronía de reloj con CENAM
d) Almacenamiento de Log cifrados para ser enviados a Secretaria de Economía

10.1 Obligaciones y Responsabilidades

10.1.1 Obligaciones de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

- La Autoridad de Sellos Digitales de Tiempo debe asegurar que todos los requerimientos de la Declaración de Prácticas están implementados de acuerdo a lo establecido en la presente Política.

- La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. debe proporcionar todos sus servicios en forma consistente y como lo establece en su Declaración de Prácticas.

- La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. debe atender las solicitudes de servicio de acuerdo a los términos y condiciones establecidas en el contrato suscrito por ambas partes, incluyendo los niveles de servicio, la disponibilidad y la exactitud de su servicio.

- La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. debe verificar la identidad de los solicitantes del servicio de Sellos Digitales de Tiempo de acuerdo a lo establecido en la Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V...

- Proporcionar a los clientes la información necesaria sobre los términos y condiciones respecto al uso del Servicio de expedición de Sellos Digitales de Tiempo, a través del contrato que firman ambas partes.

- La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., para dar exactitud en el servicio, debe utilizar fuentes confiables de tiempo oficial para garantizar una desviación del tiempo de más menos 1 mili segundo.

- Debe contar con la Infraestructura necesaria que brinde disponibilidad y acceso permanente al servicio de expedición de Sellos Digitales de Tiempo.

- La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. se compromete a guardar y cumplir estrictamente con la seguridad y confidencialidad de la información de los clientes, garantizando dicho cumplimiento por parte del personal que interviene en el servicio; de acuerdo a la fracción II del inciso A del artículo 102, fracción V y VII del artículo 104 del Código de Comercio, y último párrafo de la fracción III del Artículo 5, fracción VII y VIII del artículo 27 del reglamento del Código de Comercio en materia de Prestadores de Servicio.

10.1.2 Obligaciones del Cliente

- El Cliente debe resguardar la IP mediante la cual solicita el Servicio de Expedición de Sellos Digitales de Tiempo

- Validar que el Certificado Digital de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., se encuentre vigente y no este revocado.

- Verificar a través de la clave pública del Certificado Digital de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., que la firma contenida en el Sello Digital de Tiempo corresponda a dicha Autoridad

- El Cliente debe revisar que el sello digital de tiempo que recibe de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. ha sido correctamente firmado.

- Verificar que el certificado de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. no esté revocado

10.1.3 Obligaciones del Profesional Jurídico y su auxiliar Agente Certificador

La Autoridad de Sellos Digitales de Tiempo SeguriData Privada S.A. de C.V. asigno Al Profesional jurídico y como su auxiliar al agente certificador, y debe realizar sus funciones y obligaciones conforme a:

- Debe realizar la comprobación de datos de los clientes para la expedición de Sellos Digitales de Tiempo, tomando como base las copias de documentos entregados cotejados contra los originales
- Mantener bajo resguardo en un sitio seguro en una gaveta bajo llave, toda la documentación relacionada con el servicio de Expedición de Sellos Digitales de Tiempo
- Someterse a las auditorías periódicas que se establezcan y en su caso cumplir con los requerimientos y recomendaciones que de ellas deriven.
- Seguir una política de privacidad conforme a la Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData privada S.A. de C.V.

10.1.4 Obligaciones de Partes que confían

- Comprobar que el sello digital de tiempo sea correcto y que la clave privada utilizada para firmar el sello de tiempo no ha sido comprometida hasta el momento de la verificación
- Tener en cuenta las limitaciones en el uso del sello digital de tiempo indicadas en la presente política de la Autoridad de sellos digitales de tiempo de SeguriData Privada S.A. de C.V.

10.2 Responsabilidad de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La responsabilidad está limitada exclusivamente a proveer el servicio de Sellos Digitales de Tiempo de SeguriData privada SA de CV de acuerdo a lo establecido en la Presente Política y su Declaración de Prácticas.

La Autoridad de Sellos Digitales de Tiempo de SeguriData privada SA de CV no será responsable de manera enunciativa más no limitativa en los siguientes casos:

- Por cualquier tipo de daños y/o perjuicios que sufran sus clientes, siempre que éstos deriven de la indebida utilización del Servicio.

- Por cualquier tipo de daños y/o perjuicios que sufran sus clientes, siempre que estos deriven del incumplimiento de las obligaciones de la autoridad.

- Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los clientes de Sellos Digitales de Tiempo, realicen del Servicio, sin que estas hayan sido confirmadas expresamente por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

- Por los daños y/o perjuicios que se causen, si el cliente entrega datos y/o documentos falsos, para la obtención del servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

- Por la interrupción o alteración temporal del servicio por causas ajenas a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, como pueden ser de manera enunciativa más no limitativa, condiciones climatológicas adversas, sismos, inundaciones, fallas en la energía eléctrica, fuego, actos vandálicos, huelgas, cualquier otro motivo que afecte sus instalaciones o limiten la libertad en las comunicaciones.

10.3 Responsabilidad del Cliente-Suscriptor

- Resguardar la IP definida para el servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV
- Guardar los Sellos Digitales de Tiempo y administrar su correlación con los mensajes de datos para los cuales fueron solicitados los Sellos Digitales de Tiempo.

10.4 Responsabilidad del Profesional Jurídico y su auxiliar Agente certificador

- Proporcionar el servicio para la contratación del servicio de Expedición de Sellos Digitales de Tiempo

10.5 Responsabilidad de Partes que confían

- Guardar los Sellos Digitales de Tiempo y administrar su correlación con los mensajes de datos para los cuales fueron solicitados los Sellos Digitales de Tiempo.

11 Requerimientos de Control de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe implementar los controles para alcanzar los siguientes requerimientos:

- Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

Debe contener los requerimientos técnicos, de organización y de procedimiento, que en conjunto brindan la confiabilidad necesaria para proporcionar el servicio de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y se encuentren vinculados a esta Política.

- Debe llevar a cabo un Análisis de Riesgo para evaluar los activos del negocio y las amenazas a que están expuestos, para determinar los controles de seguridad y procedimientos de operación necesarios, definidos en el Plan de Continuidad y Recuperación ante desastres para el servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

- Debe contar con una Declaración de Prácticas, que establezca los procedimientos para cubrir todos los requisitos técnicos, de organización y de procedimiento identificados en esta política.

- La Declaración de Práctica de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe identificar las obligaciones de todas las organizaciones externas que dan soporte a dicha autoridad, incluyendo las políticas y las prácticas aplicables.

- Debe poner a disposición de los Clientes su Declaración de Prácticas, y cualquier otra documentación relevante, que sea necesaria para evaluar el cumplimiento de la política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

- Debe publicar y hacer accesible a todos los Clientes, los términos y condiciones que se especifican en el contrato, del servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, mediante publicación en su sitio de Internet http://psc.seguridata.com/sellosdigitales

- Debe contar con la aprobación de la Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV por los roles involucrados, oficial de Seguridad y profesional jurídico, y posteriormente asegurar que se implementen de manera correcta.

- La Publicación de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe especificar al menos lo siguiente:

A) La información para contactar a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV
B) La Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV aplicable
C) Incluir un algoritmo de Hash el cual puede ser usado para representar los datos que serán sellados digitalmente.
D) El tiempo de vida esperado de la firma usada para firmar los Sellos Digitales de Tiempo de SeguriData Privada SA de CV
E) La precisión de la fecha y hora en el sello digital de tiempo con respecto al UTC
F) La limitación en el uso del servicio de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

- Las obligaciones del Cliente

- El período del tiempo en que la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV de SeguriData privada, conservará los registros e información operativa (Punto 15.9 Auditoria de procedimientos de registro).

- El marco legal aplicable, incluyendo cualquier requisito legal para los servicios de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

- Los limites de responsabilidad de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

- Procedimientos para atender quejas y dar solución a conflictos.

- La referencia de que la Secretaría de Economía revisa el cumplimiento de esta política y Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV durante la solicitud de acreditación y posteriormente, cuando sea acreditado, hará las evaluaciones del cumplimiento de las mismas.

- Establecer que la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV cuenta con una arquitectura redundante y un DRP para asegurar el servicio

11.1 Política de Alta Disponibilidad del Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

La arquitectura definida incluye dos Sites, uno como principal ubicado en Interlomas y el otro como DRP ubicado en Tultitlan, con lo cual se asegura la alta disponibilidad del servicio, aunado a la redundancia que se tiene en el site de Interlomas con los dispositivos de seguridad HSM donde reside la llave de la autoridad de Sellos digitales de tiempo de SeguriData Privada S.A. de C.V.

De manera general y como introducción a la Arquitectura definida, se tienen dos Sites para el servicio de Expedición de Sellos Digitales de Tiempo, uno identificado como Site principal que se encuentra en Interlomas, el cual maneja la operación principal de la *TSA*; de manera general la *TSA* esta implementada por un *TSS* (servidor de sellado de tiempo) que esta puesto como un dispositivo dedicado(*Appliance*), en su interior se tiene un módulo HSM FIPS 140-2 nivel 3, (tarjeta PCI *nShield F3 500e*), el software *Time Stamping Option pack* y el manejador de base de datos SQL Server 2005;el dispositivo dedicado está ubicado en el rack identificado para PSC. Este *TSS* cumple con el estándar IETF X.509 RFC 3161 para la emisión de estampillas de tiempo.

El otro "site" identificado como Sitio alterno que se encuentra en Tultitlan, tiene la *TSA* implementada por un *TSS* (servidor de sellado de tiempo) que esta puesto como un dispositivo dedicado (*Appliance*), en su interior se tiene un módulo HSM FIPS 140-2 nivel 3, (tarjeta PCI *nShield 500e F3*), el software *Time Stamping Option pack* y el manejador de base de datos SQL Server 2005; el dispositivo dedicado está ubicado en el rack identificado para PSC. Este *TSS* cumple con el estándar IETF X.509 RFC 3161 para la emisión de estampillas de tiempo, es un equipo físico ubicado en el rack identificado para PSC.

El detalle se muestra en el Documento técnico y de Riesgos Jurídicos para el Servicio de Expedición de Sellos Digitales de Tiempo.

12 Ciclo de Vida de la Administración de Claves

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV para emitir Sellos Digitales de Tiempo usa una clave pública y una clave privada, dichas claves tienen un ciclo de vida comprendido desde la generación, protección, resguardo y distribución, y vigencia.

12.1 Generación de Claves de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar que cualquier clave criptográfica esté generada bajo circunstancias controladas.

La generación de las claves de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV deben ser generadas en un ambiente físicamente seguro, por personal con roles de confianza.

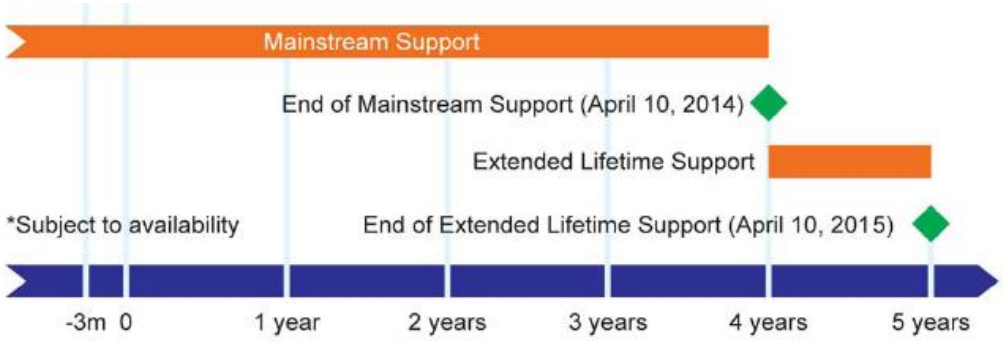
La generación de las claves de firma de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe llevarse a cabo dentro de un módulo de seguridad de hardware criptográfico que cumpla con los requerimientos identificados en FIPS 140-2 nivel 3, como lo es el servidor TSA con su componente tarjeta PCI nShield 500 eF3.

El algoritmo de la generación de las claves de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, la longitud de la clave resultante y el algoritmo usado para firmar los Sellos Digitales de Tiempo se define de acuerdo a los estándares de la industria, con una longitud de 2048 bits.

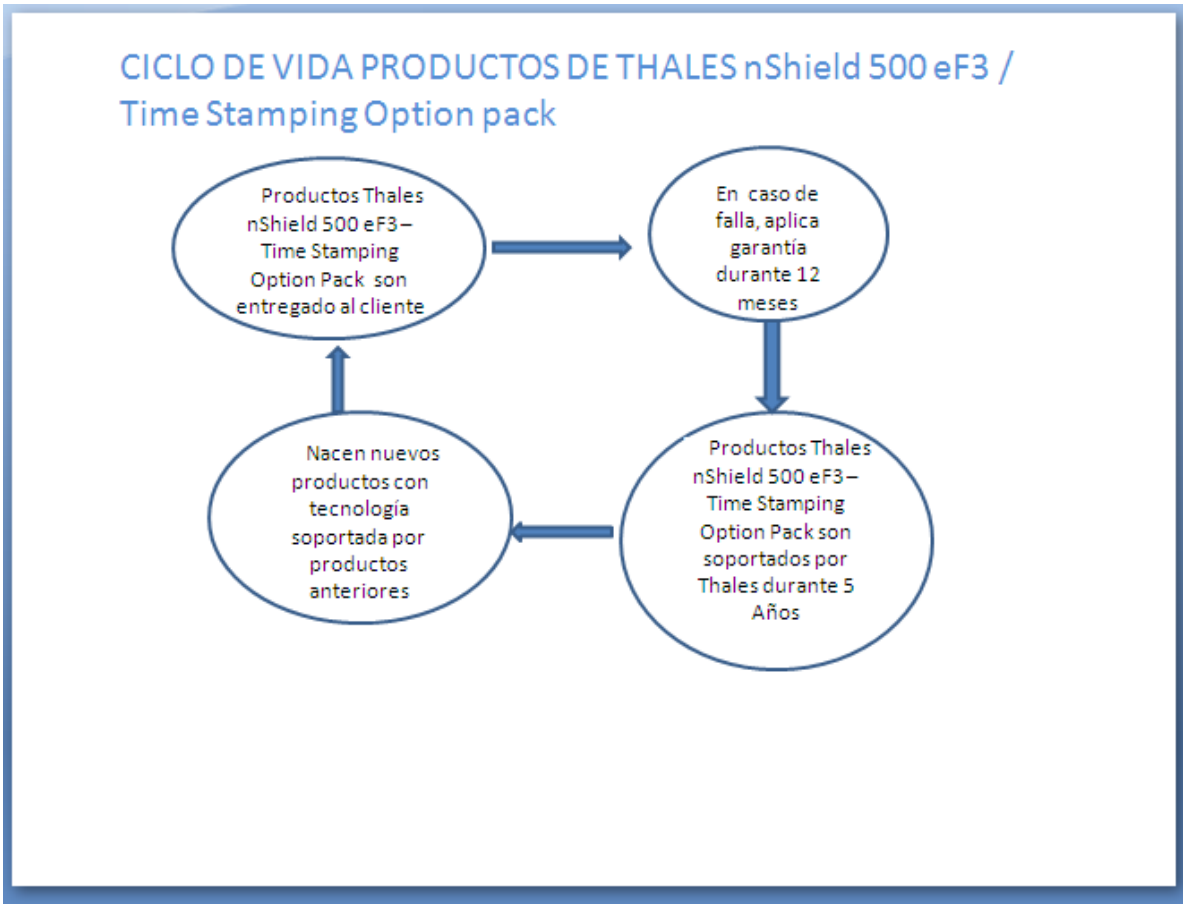
12.1.1 Ciclo de Vida productos Thales – Servidor TSA

Thales garantiza que sus productos funcionarán sustancialmente. Dicha garantía es válida por un período de doce (12) meses a partir de la fecha de entrega en el caso de hardware. En caso de que la funcionalidad del producto sea materialmente deteriorada en virtud de los defectos de fabricación, THALES se obliga a reparar o reemplazar el producto afectado de forma inmediata 1 semana como máximo.

El ciclo de vida de los productos se da en función del siguiente esquema de soporte



El ciclo de vida de los productos está en función del soporte de 5 años a partir de su lanzamiento, asegurando la compatibilidad con los nuevos modelos, para el caso del servidor TSA y de sus partes Tarjeta PSI nShield e 500F3 y software Time Stamping Option pack, su ciclo de vida es al año 2015, con la garantía de que su funcionamiento se continúa soportando hacia los nuevos modelos.



El enfoque de mantenimiento para futuras versiones de este producto garantiza la continuidad del negocio para los clientes existentes.

Ofrece la continuidad del negocio, escalabilidad y administración remota, que permite a las organizaciones implementar de manera fiable pensando en el futuro.

12.2 Generación, Protección y resguardo de la Clave Privada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe asegurar que se mantenga en todo momento la confidencialidad e integridad de su clave privada, el PSC SeguriData genera la llave privada y el requerimiento que será enviado a la Secretaria de

Economía para que esta a su vez expida el certificado de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

La clave privada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe mantenerse y usarse dentro de un módulo criptográfico que cumpla con los requerimientos de estándar FIPS 140-2 nivel 3

El módulo criptográfico se debe mantener en instalaciones físicamente seguras y el acceso debe estar protegido por mecanismos de control de acceso.

La clave privada que sea respaldada, debe ser almacenada y recuperada solamente por personal con roles de confianza, en un ambiente físicamente seguro.

El personal autorizado para llevar a cabo estas funciones debe cumplir con las actividades establecidas por las Prácticas de la Autoridad de Sellado Digital de tiempo de SeguriData Privada.

La copia de respaldo de la clave privada debe ser protegida para asegurar su confidencialidad e integridad.

12.3 Distribución de las Claves Públicas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar que la integridad y la autenticidad de la clave de verificación de firma de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV se mantiene segura durante su distribución.

El Certificado Digital de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV se debe publicar en el sitio Web de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y de la Secretaría de Economía, para que los clientes puedan verificar la integridad y la autenticidad de los Sellos Digitales de Tiempo que emita la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe tener implementadas políticas y controles de seguridad lógica.

12.4 Renovación de la Clave Criptográfica de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

El Certificado de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, no debe ser utilizado más allá del período de tiempo que el algoritmo de firma y la longitud de la clave elegida se reconozca que siguen siendo confiables para emitir Sellos Digitales de Tiempo.

En cualquiera de estas condiciones se debe proceder a emitir nuevas claves de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV e incorporarlas al ambiente productivo en el Servidor TSA y darlas a conocer en el Sitio WEB y al CENAM para la sincronía de relojes.

SeguriData Privada SA de CV no recomienda ni aplica renovación de claves.

12.5 Fin del Ciclo de Vida de las Claves de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar que sus claves privadas no puedan ser utilizadas después de su expiración o vigencia.

Se asegura que nuevas claves entren en operación cuando las claves de la Autoridad de Sellos Digitales de Tiempo SeguriData Privada SA de CV expiren

Se asegura la Expedición de nuevas claves antes de que las que estén en su momento operando y por expirar, o cuando se vea comprometida su confidencialidad.

El servidor TSA que expide los Sellos Digitales de Tiempo, debe rechazar cualquier intento de Expedición de Sello Digital de Tiempo, si el certificado de la Autoridad de Sello Digitales de Tiempo de SeguriData Privada SA de CV, ha vencido.

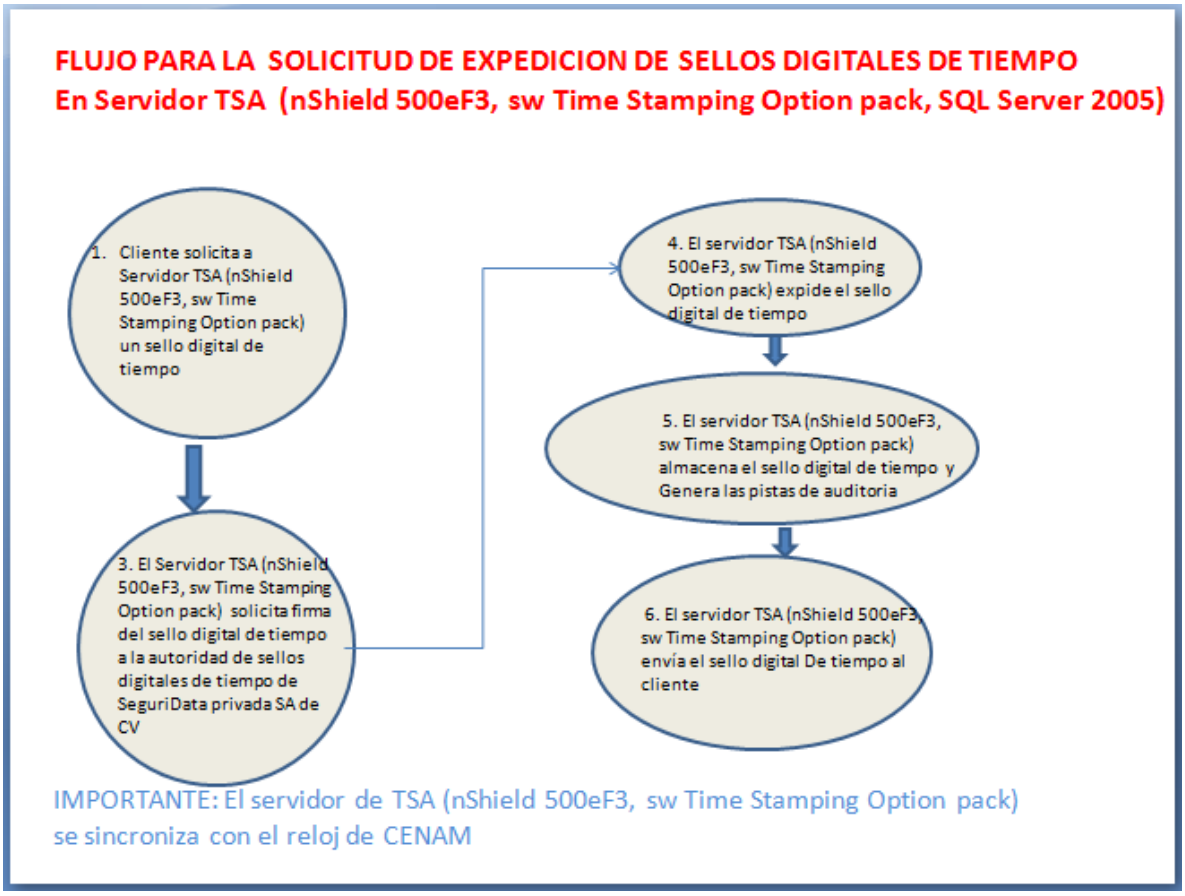
12.6 Ciclo de Vida del Módulo Criptográfico - Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. debe garantizar la seguridad del hardware criptográfico para la administración, almacenamiento y uso de su clave privada, que se encuentra en el Servidor TSA que incluye un modulo HSM FIPS 140-2 nivel 3. Como parte de la administración del ciclo de vida de los dispositivos criptográficos.

La Infraestructura de la Autoridad de Sellos Digitales de Tiempo que conforman la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, utiliza el hardware criptográfico servidor TSA que incluye tarjeta PCI NShield 500 eF3, software Time Stamping Option pack, y manejador de base de datos SQL Server 2005, para la expedición y firmado de Sellos Digitales de Tiempo.

El hardware criptográfico que firma los Sellos Digitales de Tiempo debe estar funcionando correctamente y bajo condiciones que garanticen la integridad de la clave privada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

A continuación el flujo de operación de la expedición de Sellos Digitales de Tiempo, usando el Servidor TSA.



12.6.1 Política de Mantenimiento

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe tener un contrato establecido con el proveedor de los equipos de hardware criptográfico, servidor TSA, que

contemple soporte en línea (Web), y mantenimiento correctivo que incluya la reparación o cambio en caso de falla de algún componente.

13 Sellos Digitales de Tiempo - Generalidades

Los Sellos Digitales de Tiempo vinculan mensajes de datos con una fecha y hora en particular, para establecer evidencia de que dichos mensajes de datos existieron.

Los Sellos Digitales de Tiempo permiten contar con una evidencia que permita validar la existencia e integridad de mensajes de datos a partir de la fecha y hora contenidos en un Sello Digital de Tiempo.

13.1 Uso y Límites de Uso de Sellos Digitales de Tiempo

Los Sellos Digitales de Tiempo son interoperables con el servidor TSA que incluye un modulo HSM FIPS 140-2 nivel 3, que cumple con lo establecido por la Secretaría de Economía, el estándar internacional Internet X.509 “Public Key Infrestructure Time Stamp” y con los RFC3628 y RFC3161.

Su ámbito de aplicación se extiende a todos los sectores que desean incorporar a sus procesos un Sello Digital de Tiempo.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV expide Sellos Digitales de Tiempo para uso, principalmente, en operaciones de actos mercantiles con apego a lo establecido en el Código de Comercio, leyes aplicables, circulares y demás disposiciones que permitan su uso, sin perjuicio de poderlos expedir en actos de cualquier otra naturaleza en los procesos en los que se desee incorporar un sello digital de tiempo.

13.2 Información en los Sellos Digitales de Tiempo

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar que los Sellos Digitales de Tiempo sean emitidos a través de un proceso seguro y que contengan la fecha y hora correctas.

Cada Sello digital de tiempo debe tener un identificador único (número de folio). Y de acuerdo al RFC 3161 el campo de tiempo se conforma de: YYYYMMDDhhmmssZ

YYYY indica el año, MM indica el mes, DD indica el día, hh la hora, mm los minutos, ss los segundos, Z un terminador.

El terminador es un sinónimo de UTC.

Los valores de tiempo que la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV utilizada en los Sellos Digitales de Tiempo debe ser rastreable hasta al menos uno de los valores de tiempo real provisto por el Sistema de Sincronización de Tiempo del CENAM; entidad reconocida para proveer la hora oficial en México.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe contar con la evidencia de la rastreabilidad a través de un TAC (TimeAttribute Certificate) que se obtiene por la sincronización del tiempo con el CENAM.

El tiempo incluido en el sello digital de tiempo debe estar sincronizado con el UTC dentro de la exactitud definida en la presente Política.

El Sello Digital de Tiempo debe incluir una representación (Ej. valor de hash) del dato que se sellará digitalmente tal cual fue proporcionado por el Cliente.

El Sello Digital de Tiempo debe ser firmado usando una clave generada exclusivamente para este propósito.

La información contenida en los Sellos Digitales de Tiempo es:

- Identificador de la política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV
- Hash correspondiente al mensaje de datos para el cual se solicito el Sello Digital de Tiempo.
- Tiempo YYYYMMDDhhmmssZ
- Número de folio
- Datos generales de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV
- Firma electrónica avanzada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

13.2.1 Vigencia de los Sellos Digitales de Tiempo

La vigencia de los Sellos Digitales de Tiempo no está limitada, es decir se mantienen por siempre.

a) Las claves de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV con las cuales se expidan los Sellos Digitales de Tiempo no deben ser comprometidas.
b) El algoritmo hash contenido en los Sellos Digitales de Tiempo debe ser reconocido como un algoritmo que no presenta ataques conocidos.
c) El algoritmo de firma y longitud de la clave empleada por la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV para firmar los Sellos Digitales de Tiempo no deben ser vulnerables a ataques criptográficos.

13.3 Sincronización del Reloj con el UTC

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurarse que el reloj que utiliza para el servicio de sello digital de tiempo esté sincronizado con el reloj del CENAM, dentro de la exactitud declarada, de acuerdo a:

a) La calibración de los relojes de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV debe mantenerse de tal forma que no se desvíen de la exactitud de tiempo declarada.

b) Los relojes de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV deben ser protegidos contra amenazas que podrían dar lugar a un cambio no detectado que los desvié de su calibración.

c) La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar, que si el tiempo que debe indicarse en los Sellos Digitales de Tiempo varía o se desvía de la sincronización con el UTC provisto por el CENAM, éste será detectado y continuara la emisión de sellos de tiempo de acuerdo a la vigencia del último TAC definido, una vez finalizada dicha vigencia dejara de expedir Sellos Digitales de Tiempo hasta que re-sincronice su reloj con el UTC provisto por el CENAM o por la Secretaría de Economía y se obtenga un nuevo TAC. La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe mantener evidencia de rastreabilidad de la sincronización de tiempo entre sus unidades de sellado digital de tiempo y la fuente de tiempo oficial del CENAM, esto se realiza a través del protocolo del servidor de TSA.

d) La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe asegurar que la sincronización del reloj se mantenga cuando ocurra un segundo intercalar, cuando éste sea notificado por un organismo autorizado. El segundo intercalar ocurrirá en el último minuto de la última hora del día, siempre y cuando el segundo intercalar esté programado para ocurrir. Un registro de sello digital de tiempo debe mantener el tiempo exacto (dentro de la exactitud declarada) cuando ocurra este cambio.

13.4 Política de Deshecho – Limitantes

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe:

Rechazar las peticiones de Expedición de Sellos Digitales de Tiempo, cuando el Certificado de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV este revocada o haya vencido.

Asegurar que después de la desincorporación de las claves de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV , estas no puedan ser accedidas ni usadas para ningún propósito diferente al menos que se requiera para aclaración de alguna controversia.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV a partir del servidor TSA no debe expedir el Sello Digital de Tiempo, si se detecta que el reloj de tiempo varia o se desvía de la sincronización con la precisión establecida con respecto al UTC provisto por el CENAM.

13.5 Grado de Fiabilidad de los Mecanismos y Dispositivos utilizados

Los puntos importantes para asegurar la fiabilidad de los mecanismos de Sellado digital de tiempo son:

1. La seguridad que se da al acceso a la autoridad de sello digital de tiempo de PSC SeguriData

2. La seguridad que se da al software cliente que es solicitante de estampillas de tiempo

3. La confianza que se tiene en los algoritmos utilizados tanto para la digestión de los mensajes como para la generación de las Firmas Electrónicas Avanzadas de los Sellos Digitales de tiempo

4. La exactitud de la fuente de tiempo

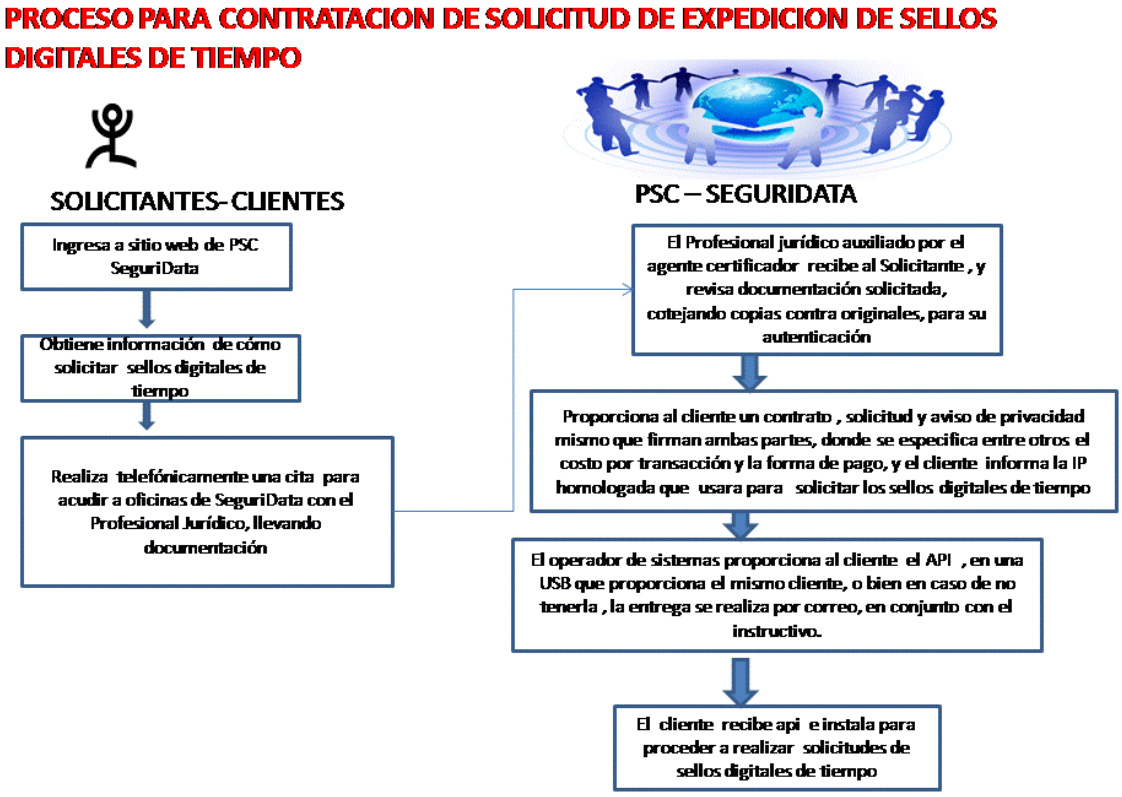
5. La seguridad que se tiene al obtener la información de la fuente de tiempo

6. La disponibilidad que se tiene de la fuente de tiempo

13.5.1 Seguridad en el acceso a la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, se encuentra almacenada y custodiada en el servidor de TSA que incluye un modulo HSM FIPS 140-2 nivel 3 (tarjeta PSI nShield 500e F3), ésta nunca abandona el hardware en claro. Incluso, si el hardware fuera manipulado y se abriera, las llaves se eliminarían automáticamente en dicho intento.

14 Proceso para la prestación del servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.



Los pasos a seguir por el solicitante para contratar el Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV son:

- El solicitante realiza cita telefónica para acudir a oficinas de SeguriData, al menos con 2 días de anticipación.
- Profesional Jurídico o Agente Certificador recibe solicitud de servicio donde indica la IP a través de la cual realizara la solicitud de Sellos Digitales de Tiempo y documentación presentada por el Solicitante.
- Profesional Jurídico o Agente Certificador realiza el cotejo de documentos originales contra las copias presentadas por el Solicitante, para su autenticación.
- Profesional Jurídico o Agente Certificador formaliza la contratación del servicio con la firma del contrato y la firma del convenio de confidencialidad
- Profesional Jurídico o Agente Certificador entrega el API en una USB que el cliente proporciona.
- Profesional Jurídico o Agente Certificador apoya en la configuración del API

- URL para la comunicación con el sellador (protocolo http usando TSP que cumple RFC 3161)
- Certificado de la autoridad de sellado de tiempo
- Nombre del documento que se desea sellar
- Nombre del archivo donde quedara el sello digital de tiempo

- Profesional Jurídico o Agente Certificador brinda soporte al solicitante durante el proceso de Expedición de Sello digital de tiempo.

14.1 Autenticación de la Identidad de un Individuo

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. recaba una serie de documentos para realizar una correcta verificación de la identidad del solicitante del Sellado de tiempo digital, esto bajo consentimiento explícito y conforme a lo que señala la Política de Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, el solicitante deberá acudir con el profesional Jurídico o Agente certificador a las oficinas de SeguriData. El trámite es personal e intransferible por lo que el interesado deberá presentarse en las instalaciones para realizarlo.

Los documentos se deben presentar en original y copia

- Personas Físicas:
  - Identificación Oficial de uno de los siguientes documentos:
    - Credencial para votar emitida por el Instituto Federal Electoral (IFE).
    - Pasaporte vigente emitido por la Secretaría de Relaciones Exteriores (SRE)
    - Cédula profesional
    - Para extranjeros, pasaporte vigente y la documentación que acredite su estancia legal en el país.
  - Documento oficial en el cual conste la nacionalidad, fecha y lugar de nacimiento del solicitante:
    - Acta de nacimiento.
    - Cédula Única de Registro de Población.
    - Carta de naturalización.
  - Comprobante de Domicilio:
    - Servicio de energía eléctrica.
    - Servicio telefónico (excepto telefonía celular).
    - Servicio de agua potable.
    - Impuesto predial.
    - Estados de cuenta bancarios.

Para el solicitante extranjero con residencia en el país, se consideran los mismos documentos.

- Personas Morales, representadas a través de una persona física.

- Instrumento público mediante el cual se acredite la legal constitución de la Persona Moral (Ejemplo: Acta Constitutiva que contenga los datos de inscripción del Registro Público de Comercio, Publicación en el Diario Oficial o su equivalente).
- Instrumento público en el cual consten las facultades otorgadas al representante legal.
- Registro Federal de Contribuyentes de la Persona Moral.
- Comprobante de Domicilio de la Persona Moral.

Adicionalmente el Representante Legal deberá cumplir con los requisitos y presentar la documentación establecida para una Persona Física

En caso de que la identificación oficial del solicitante no contemple su domicilio o no sea el actual, deberá presentar un comprobante de domicilio que esté a su nombre.

Si la identificación oficial del solicitante contempla su domicilio actual, el comprobante de domicilio puede estar a su nombre o al de un tercero.

El comprobante de servicio de energía eléctrica, el comprobante de servicio telefónico y los estados de cuenta bancaria no deberán tener antigüedad mayor a cuatro meses. El comprobante de servicio de agua potable y el comprobante de impuesto predial no deberán tener antigüedad mayor a un año.

La verificación de la identidad del solicitante (Personas Físicas y Morales) la realiza el profesional jurídico auxiliado del agente certificador, observando que correspondan los rasgos fisionómicos del solicitante respecto a documentación presentada que cuente con sus datos y fotografía.

14.2 Procedimiento para la atención a solicitantes del Servicio de Expedición de Sellos Digitales de Tiempo

La atención se realiza a través del Profesional jurídico o su agente certificador, quien es personal de SeguriData Privada SA de CV.

El solicitante del servicio de Sellos Digital de Tiempo debe:

1. Llenar el formato “Solicitud de servicio de expedición de Sellos Digitales de Tiempo” (Anexo 1) el cual se encuentra disponible en el sitio de Internet http://psc.seguridata.com/sellosdigitales

Consideraciones para el llenado del formato:

Persona Física:

- Nombre completo del Solicitante iniciando por el Nombre(s), Apellido Paterno y Apellido Materno.

- Domicilio particular del Solicitante, indicando la calle, número exterior y en su caso, número interior y la colonia.
- IP desde donde solicitara la expedición de Sellos Digitales de Tiempo

Persona Moral:

- Denominación o razón social, tal y como se establece en el instrumento público mediante el cual acredite su legal constitución (Ejemplo: Acta Constitutiva)
- Datos de la Escritura Pública o datos de la publicación en el Diario Oficial de la Federación, en la que conste su constitución.
- Registro Federal de Contribuyentes de la persona moral.
- Nombre del representante legal.
- Datos de la Escritura Pública en la que consten sus facultades como representante legal.
- Domicilio de la persona moral, indicando la calle, número exterior y en su caso, número interior, Delegación o municipio, Ciudad, Estado y código postal.
- IP desde donde solicitara la expedición de Sellos Digitales de Tiempo

2. Entregar al profesional Jurídico o agente certificador la solicitud del servicio debidamente requisitada y firmada de manera autógrafa por el Solicitante.

3. Entregar original y copia de la documentación requerida para acreditar la identidad y personalidad del solicitante.

4. Establecer una relación jurídica con la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV SeguriData a través de la firma del contrato para la prestación del servicio de expedición de Sellos Digitales de Tiempo.

5. Establecer convenio de confidencialidad a través de la firma del aviso de privacidad por parte del cliente.

14.2.1 Otorgamiento del Servicio

Para el otorgamiento del servicio el personal responsable de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y el Cliente desempeña las actividades siguientes:

El profesional Jurídico o el auxiliar agente certificador realizan lo siguiente:

Es responsable de formalizar la firma del contrato con Personas Físicas o Morales para establecer la relación de prestación del servicio de expedición de Sellos Digitales de Tiempo, para lo cual realiza lo siguiente:

a) Recibir solicitud de servicio y verificar la documentación presentada por el Solicitante.
b) Realizar el cotejo de documentos originales contra las copias presentadas por el Solicitante
c) Verifica la identidad del solicitante (Personas Físicas y Morales) observando correspondan los rasgos fisionómicos del solicitante respecto a documentación presentada que cuente con sus datos y fotografía, como se establece en el documento de Declaración de Practicas.
d) Formalizar la contratación del servicio con la firma del contrato, y la firma del aviso de privacidad.
e) Es responsable de tramitar el alta del cliente en el sistema de Sellos Digitales de Tiempo y las pruebas para la incorporación del Cliente al servicio, mediante el bloqueo de acceso por IP que se validan en el firewall.
f) Entrega en la USB que el cliente presenta la aplicación API
g) Brinda soporte al usuario para comprobar la funcionalidad para la expedición del Sello Digital de Tiempo

El Cliente debe realizar lo siguiente:

a) Configurar su ambiente operativo de acuerdo a lo indicado por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, API entregada en la USB propiedad del cliente.
b) Realizar las pruebas de funcionalidad para la expedición de Sello Digital de Tiempo

15 Administración de la Autoridad de Sellos de Tiempo de SeguriData Privada

15.1 Administración de la Seguridad

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. usará sistemas confiables y los productos serán protegidos contra alteraciones, esto se asegura por las características de la tarjeta PSI nShield 500eF3 al manejar el concepto SEE y el software asociado Time Stamping Option Pack, el detalle se explica en el Documento Técnico y de Riesgos Jurídicos para el Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

La seguridad en el acceso entre el cliente (API) y el Servicio de Expedición de Sellos Digitales de Tiempo tanto para la solicitud del sello digital de tiempo como para la entrega del mismo se da por:

- La validación que se realiza de la IP proporcionada por el cliente durante la contratación del servicio, la cual está registrada asociada al cliente que realiza la solicitud. El servicio valida que la IP corresponda al MAC address que se relaciono con la IP dada de alta, si ambos datos coinciden, se proporciona el servicio y se acepta la solicitud.

La entrega se realiza a través de la misma vía hacia la IP que solicito el sello digital de Los mecanismos de seguridad para el Time Stamping Option Pack, se dan a través del manejo de un usuario y password, el cual tiene permisos para la configuración e instalación del mismo.

Los datos de configuración son almacenados de manera segura en la base de datos y únicamente el administrador de la base de datos tiene acceso a los mismos, sin la posibilidad de modificarlos.

Las medidas de protección del depósito público (repositorio de información), de los sellos digitales de tiempo y de la información privada que se obtiene durante la contratación del servicio, por parte del cliente, se da en la base de datos mediante el uso de un usuario y contraseña.

Por otra parte la seguridad de acceso al modulo HSM nShield 500 eF3, para la llave privada de la autoridad de sellos digitales de tiempo, se explica en el documento técnico y de riesgos jurídicos para el servicio de expedición de sellos digitales de tiempo, y la no modificación de la hora y fecha en el reloj de tiempo que se encuentra en dicho modulo, se explica en el documento de Procedimiento de Seguridad Eliminar posibilidad de modificación de Reloj de Tiempo.

Estos controles son congruentes con lo descrito en el documento Plan de Seguridad de Sistemas.

15.2 Controles de Seguridad Física

SeguriData Privada S.A. de C.V. gestiona y pone en práctica controles de seguridad apropiados para restringir el acceso al hardware y al software utilizado en relación con la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

SeguriData Privada S.A. de C.V. asegurará que el acceso físico a servicios críticos es controlado y que se tiene el análisis y la reducción de los riesgos físicos de sus activos.

Se ponen en práctica controles para evitar la pérdida, el robo, el daño o el compromiso de activos y la interrupción de la operación de la Infraestructura de la Autoridad de Sellos digitales de tiempo. También existen perímetros de seguridad claramente definidos.

Se ponen en marcha controles de seguridad físicos y ambientales para proteger los recursos en los que está alojada la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., aplicando controles de acceso físico, controles de protección y recuperación ante desastres, controles de seguridad contra incendios e inundaciones y, controles de fallos en las instalaciones, suministros de energía, telecomunicaciones y, aire acondicionado, entre otros

15.2.1 Ubicación y Construcción

La ubicación de los servicios de la Infraestructura de la Autoridad de Sellos digitales de tiempo está en un centro de datos ambientalmente segura, ubicada en Interlomas como centro principal de operación, y un centro de datos alterno ubicado en Tultitlan. Dichos centros de datos cumplen con las normas ISO siguientes:

- NMX-CC-9001-IMNC-2000/ISO 9001:2000, para los procesos de Administración de Cambios, Administración de Incidentes y Administración de las Configuraciones.
- ISO/IEC 20000-1:2005, para la administración de sistemas de Tecnologías de la Información.
- ISO/IEC 27001:2005, para la administración de sistemas de Tecnologías de la Información.

Todos los equipos relacionado con la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. cumplen con un conjunto de principios de seguridad mínimos que permiten proporcionar un servicio a prueba de fallos conforme al documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.1.doc, entregado a la Secretaría de Economía con motivo de la acreditación como Prestador de Servicios de Certificación, para el servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

15.2.2 Acceso Físico

El personal autorizado (roles de: oficial de seguridad, profesional jurídico, operador de sistemas, administrador de sistemas, administrador de base de datos, administrador de redes y, personal que realiza auditorias), para acceder a las áreas seguras donde está la Autoridad de sellado digital de tiempo, ya sea en el centro de datos principal o alterno, no podrá quedarse sólo, en los centros de datos, sin la supervisión de personal autorizado, y únicamente para realizar labores de actualización, mantenimiento, o auditoria. En la administración de la Autoridad de sellado digital de

tiempo se protegen datos sensitivos contra accesos no autorizados o modificaciones por red, la Autoridad de sellado digital de tiempo asegura que el acceso a la información y a las funciones de las aplicaciones del sistema están restringidos de acuerdo a la Política de Seguridad Física del Sitio de Interlomas y Tultitlan, incluyendo la separación de funciones de administración y operación.

El procedimiento para el Acceso Físico al Site Principal ubicado en Interlomas es:

El personal autorizado por parte de SeguriData debe enviar un correo electrónico a NEXO solicitando el acceso de los visitantes, informando el motivo de la visita y el tiempo que permanecerán en las instalaciones, así como las áreas a las que se tendrá acceso, al menos con 24 hrs de anticipación

Si el visitante ingresa con auto, debe solicitarse la autorización para el estacionamiento, limitado a las políticas de espacio que en ese momento se tengan, la notificación debe ser vía correo electrónico por la persona autorizada por parte de SeguriData, con 24 horas de anticipación.

El visitante no podrá ingresar solo a las instalaciones den centro de datos, debe hacerlo forzosamente con personal autorizado por parte del centro de datos.
Todo equipo de cómputo debe quedar registrado, anotando la marca y el número de serie
Queda prohibido introducir cajas de cartón, plástico y cualquier tipo de material flamable, al centro de datos.

El cliente es responsable de llevarse todo el empaque de sus equipos que ingresan por la bodega

El cliente es responsable de avisar a NEXO para que el custodio de la llave de SeguriData, abra la jaula o rack correspondiente.

El procedimiento para el Acceso Físico al Site alterno ubicado en Tultitlan es:

Si el visitante ingresa en auto, accede por el área de estacionamiento, donde el guardia solicita su nombre y la persona que visita, una vez que el guardia revisa si está en la lista de accesos, solicita su identificación y asigna el numero de cajón que le corresponde, en caso contrario no se permite el acceso.

En la recepción, se solicita identificación y se anotan los datos en una bitácora electrónica, se toma una foto y se registra huella del dedo índice de la mano derecha, con esto se genera un gafete (etiqueta adherible).
En caso de traer equipo de cómputo el guardia de seguridad anota en una bitácora los datos del equipo a ingresar, número de serie, y marca

A continuación el custodio de los visitantes, abre la puerta de cristal blindado, con una tarjeta de proximidad

Al pasar esta puerta se encuentra un arco sensor de metales y un guardia, el cual solicita al visitante o cliente se registre en la bitácora (nombre, fecha, hora de entrada, hora de salida, persona que guía al visitante, motivo de visita y firma), previa revisión de su autorización

El siguiente control es un control mediante huella digital y PIN, mediante el cual se abre una puerta de metal

Una vez que se accedió al centro de datos, se tiene un pasillo que conduce a otras puertas más, una de cristal y otra de malla de alambre las cuales abren con tarjetas de proximidad.
Continúan con una puerta adicional que abre con tarjetas de proximidad y conducen a los racks de SeguriData.

15.2.3 Energía Eléctrica y Aire acondicionado

El área segura de operaciones se encuentra conectada a una fuente de energía estándar. Los componentes críticos de la Infraestructura de la Autoridad de Sellos digitales de tiempo se encuentran conectados a la fuente de energía ininterrumpida (UPS). Para prevenir la interrupción del servicio en caso de interrupciones del suministro eléctrico, se cuenta con plantas de emergencia de generación de energía eléctrica y cuatro tanques de combustible para la misma, de 600, 1000, 1500, y 6000 litros, que aseguran la continuidad en el servicio.

Se cuenta con unidades de aire acondicionado de precisión de 5, 10, 20 y 30 toneladas.

15.2.4 Riesgos por Inundaciones

La ubicación donde se encuentran los servicios de la Infraestructura de la Autoridad de Sellos digitales de tiempo proporciona protección contra las inundaciones, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.0.doc.

15.2.5 Prevención de Incendios y Protección

La ubicación donde se encuentran los servicios de la Infraestructura de la Autoridad de Sellos digitales de tiempo proporciona protección contra incendios, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.0.doc.

15.3 Almacenamiento de Medios

Todos los medios de comunicación magnéticos que contienen la información de la Infraestructura de la Autoridad de Sellos digitales de tiempo, incluyendo medios de comunicación de respaldos, son almacenados en gabinetes bajo llave bajo el resguardo del Centro de Datos con acceso

exclusivo para el administrador de base de datos, el operador de sistemas y el administrador de sistemas, cumpliendo con la seguridad descrita tanto para el site de Interlomas como Tultitlan.

Se conservan todos los registros de los usuarios y de la Autoridad de Sello digital de tiempo, protegiéndolos contra destrucción y falsificación de acuerdo a la Política de Seguridad de la Información.

15.4 Destrucción de Documentos

Los documentos en papel y aquellos medios que contengan elementos sensibles de la Infraestructura de la Autoridad de Sellos digitales de tiempo o información comercialmente sensible o confidencial serán eliminados, solo en caso de que la autoridad de Sello digital de tiempo de SeguriData Privada SA de CV deje de existir, y será bajo las siguientes condiciones:

- Para información en medios magnéticos:
    - Destrucción completa del mecanismo.
    - El empleo de una herramienta aprobada para limpiar o sobrescribir medios magnéticos.
- Para información en material impreso

  Trituración.

15.5 Copias de Seguridad

Se utilizarán elementos de almacenamiento en sitios externos para el resguardo y la retención de las copias de seguridad pertenecientes a la información relacionada con la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., el software de reserva y datos relacionados con elementos críticos especificados en la Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

El almacenamiento en sitio externo se tiene en el Site alterno ubicado en Tultitlan:

- Está disponible al personal autorizado 24 horas por día, 365 días del año con el fin de recuperar el software y datos;
- El lugar cuenta con los niveles apropiados de seguridad física.

Esto se detalla en el documento: PSC-SEGURIDATA-POLITICASDESEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.1.doc

15.6 Procedimientos de Control

SeguriData Privada S.A. de C.V. asegura que los procedimientos administrativos relacionados con el personal y exigencias procesales, mecanismos de seguridad físicos y tecnológicos, se mantienen conforme a esta Declaración de Prácticas de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, la Política de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y otros documentos operacionales relevantes.

SeguriData Privada S.A. de C.V. asegura que sus sistemas son seguros y se gestionan correctamente, con un riesgo mínimo de fallo. Los perjuicios, incidentes de seguridad y mal funcionamiento serán reducidos al mínimo mediante el uso de sistemas de información de incidentes y procedimientos de respuesta.

SeguriData Privada S.A. de C.V. actuará de una manera oportuna y coordinada para responder rápidamente a los incidentes que puedan surgir.

El administrador de sistemas y el operador de sistemas de la autoridad de sello digital de tiempo, deben proporcionar información de los riesgos de la seguridad presentados durante la operación, al oficial de seguridad, como responsable de la Política de Seguridad de Información, mediante el registro de los eventos en la Bitácora definida.

15.7 Roles de Confianza

A fin y efecto de asegurar quien tiene acceso a qué parte del sistema, las responsabilidades se han diferido en varios roles y usuarios para asegurar que las personas actúan dentro de los límites de sus responsabilidades y dentro de la política de seguridad indicada.

Dicha diversificación se ha logrado creando roles separados con sus respectivas cuentas de usuario y certificados digitales, con límites establecidos de acuerdo a las funciones de cada rol.

Los roles implican las responsabilidades siguientes:

- **Oficial de Seguridad**: Responsable de administrar las prácticas de seguridad.
- **Administrador del Sistema**: Autorizado para instalar, configurar y mantener sistemas.

- **Operador del Sistema**: Responsable de gestionar el funcionamiento diario de los sistemas. Autorizados para gestionar el sistema de copias de seguridad y recuperación ante fallos;
- **Profesional Jurídico**: Autorizados para ver y mantener archivos y registros de auditoría del sistema.
- **Administrador de Base de datos.** Encargado de administrar la base de datos
- **Administrador de redes.** Encargado de la administración de las comunicaciones y redes.

Los roles relevantes del personal serán formalmente designados por el profesional jurídico y profesional informático, apoyados por el oficial de seguridad, asignados de manera formal mediante una reunión, y no podrán ejercerlos hasta que esto suceda.

Los procedimientos serán establecidos y puestos en práctica para todas las funciones que afecten a la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

15.7.1 Número de Personas Requeridas por Tarea

El número de personas requeridas por tarea es:

Tarea	Personas requeridas
Contratación del servicio – entrega de api –validación y resguardo de información	Profesional jurídico auxiliado por Agente certificador
Generación de Llaves de la autoridad se sello digital de tiempo	Administrador de sistemas Oficial de seguridad
Administración de la base de datos	Administrador de base de datos
Administrar las comunicaciones	Administrador de redes
Revisar procesos de auditoria y seguridad	Oficial de seguridad

Se llevarán a cabo prácticas para asegurar que una persona que actúa sola no pueda alterar las medidas de seguridad. Para asegurar mejor la integridad de los equipos donde opera la Infraestructura de la Autoridad de Sellos Digitales de Tiempo, se aplicarán esfuerzos para identificar a un individuo distinto para cada rol de confianza, de acuerdo a la tabla siguiente:

Rol original	Reemplazo temporal de rol
Oficial de seguridad	Profesional Informático
Administrador de redes	Oficial de seguridad
Administrador de base de datos	Administrador de redes
Administrador de sistemas	Operador de Sistemas
Operador de sistemas	Administrador de Sistemas

15.7.2 Identificación y Autenticación para cada Función

Las personas que realizan las funciones relevantes están sometidas a una seguridad apropiada definida de acuerdo al rol que desempeñen como usuario y password para administradores de bases de datos, usuario y password para la administración, usuario y password para el acceso al servidor TSA.

15.7.3 Funciones que Requieren Separación de Deberes

Las funciones que implican la administración de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV son separadas y asignadas a los roles comentados en los puntos 15.7 y 15.7.1

Todas las funciones que implican el mantenimiento de registros de auditoría son separadas y asignadas a los roles comentados en los puntos 15.7 y 15.7.1

El personal (tanto temporal como permanente) tiene descripciones de trabajo definidas desde el punto de vista de separación de deberes y privilegios de acceso, determinando la sensibilidad de la posición con base en los deberes y niveles de acceso, los antecedentes, preparación y conocimientos del empleado, diferenciando funciones generales y específicas.

Para ello las descripciones de trabajo incluyen habilidades y requisitos de experiencia.

15.8 Controles de Seguridad Personales

Se realizan estudios e investigaciones sobre todas las personas seleccionadas para llevar a cabo un rol de confianza, de acuerdo a lo marcado en el procedimiento de selección y contratación en el documento PSC-SEGURIDATA-PROCEDIMIENTOSELECC-CONTRA- RH-VERSION1.0.doc, para asegurar su integridad, antes de iniciar sus funciones.

Sin restricción, SeguriData Privada S.A. de C.V. no será responsable de la conducta de un empleado más allá de sus deberes y sobre el que SeguriData Privada S.A. de C.V. carece de control, como los actos de espionaje, el sabotaje, la conducta criminal, o la mala fe.

SeguriData Privada S.A. de C.V. asegurará que las prácticas sobre el personal y la contratación del mismo, garanticen la validez de las operaciones realizadas dentro de la Infraestructura de la Autoridad de Sellos digitales de tiempo de SeguriData Privada S.A. de C.V.

15.8.1 Requerimientos de Calificación, Experiencia, Calidad y Formación

SeguriData Privada S.A. de C.V. empleará personal que posea los conocimientos, experiencia y calificación necesaria para poder prestar los servicios que sean apropiados a su puesto de trabajo.

El personal directivo empleado poseerá conocimientos en tecnología de Sellos Digitales de Tiempo, firma electrónica avanzada, así como en procedimientos de seguridad para el personal y experiencia en seguridad de la información y prevención de riesgos.

15.8.2 Procedimiento de Comprobación

Los procedimientos de comprobación incluyen, aunque no limitadamente, la comprobación y la confirmación de:

- Empleo anterior
- Referencias profesionales
- Referencias personales
- Formación académica
- Antecedentes penales
- Estatus e historial financiero y crediticio

SeguriData Privada S.A. de C.V. utilizará técnicas de investigación disponibles permitidas por la ley que proporcionen información similar.

SeguriData Privada S.A. de C.V. proveerá a su personal de formación interna y externa para mantener los niveles apropiados y requeridos de competencia para realizar su trabajo con el más alto nivel de calidad.

En caso de realización de cualquier tipo de acción no autorizada, se impondrá la sanción correspondiente, marcadas en el plan de continuidad del negocio y recuperación ante desastres, en función de la falta cometida, que va desde 3 llamadas de atención, hasta el despido.

15.8.3 Requisitos de Personal Externo

SeguriData Privada S.A. de C.V. no apoya el empleo de personal externo para la realización de funciones relevantes.

15.8.4 Documentación Suministrada al Personal

SeguriData Privada S.A. de C.V. proporciona a su personal todos los materiales de formación necesarios para realizar sus funciones de trabajo y sus tareas, manejando los casos de reemplazo de roles en caso de alguna ausencia en caso de enfermedad, u otro evento de acuerdo a lo definido en el Análisis y Evaluación de manejo de riesgos

15.9 Auditoría de Procedimientos de Registro

En este subcomponente se describe el registro de eventos y la auditoría de sistemas, implementados con el fin de mantener un entorno seguro

Todos los actos relacionados con la expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV son registrados. Esto incluye todos los datos de configuración usados en el proceso.

Los tipos de datos registrados incluyen, pero sin carácter limitativo:

- Todos los datos incluidos en cada proceso de expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV serán registrados en la base de datos, para tener una referencia futura en caso de que su uso fuera necesario.

- Toda la documentación presentada para la solicitud de expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV en conjunto con la propia solicitud, contrato y aviso de confidencialidad firmados por el cliente, los cuales se encuentran en un sitio seguro de manera física almacenados en gavetas bajo llave

15.9.1 Frecuencia de Registro

Comprobaciones de los registros son realizadas y contrastadas de manera semanal. Mediante el proceso de generación de reporte de auditoria, mientras que el registro de las transacciones es diario en función de su ocurrencia.

Las transacciones son conservadas en la base de datos durante al menos 5 (cinco) años para posibles comprobaciones de auditoría, y al menos 5 (cinco) años para la información de los Sellos Digitales de Tiempo.

Las transacciones serán almacenadas al menos 5 (cinco) años después de que la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV cese sus operaciones.

15.9.2 Protección de los Registros de Auditoria

Los datos recogidos en la auditoria son revisados con regularidad para evitar cualquier tentativa de violar la integridad de cualquier elemento de la Infraestructura de la Autoridad de de Sellos digitales de tiempo.

Solo el Oficial de Seguridad de la Infraestructura de la Autoridad de de Sellos digitales de tiempo y Auditores pueden ver los registros de auditoría en su totalidad. SeguriData Privada S.A. de C.V. decidirá si algún registro de auditoría en particular tiene que ser visto por un tercero y lo pondrá a su disposición.

SeguriData Privada S.A. de C.V. realiza un respaldo de la base de datos que contiene las transacciones descritas, el cual se efectúa diariamente, de acuerdo a lo definido en las Políticas de Respaldo definidas en este documento en la sección 16.1.1.

15.9.3 Notificación al Individuo que Genera un Suceso

Cuando se registra un suceso, al emitir el reporte de auditoria y recibir problemas en la integridad de los datos, el oficial de seguridad que revisa dicho reporte, notifica al administrador de base de datos para que proceda a restaurar la base de datos con el respaldo correspondiente, de manera que no es necesario notificar del suceso, ya que no afecta a los clientes.

Lo anterior, está definido en el documento de Análisis y Evaluación de manejo de riesgos para la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

15.9.4 Evaluación de Riesgos e Identificación de Vulnerabilidades

Se llevarán a cabo evaluaciones de riesgo relativas al Servicio de Sellos Digitales de Tiempo, amenazas corrientes e identificación de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de Sellos Digitales de Tiempo , incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de riesgos e identificación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la Infraestructura de Sellos Digitales de Tiempo, así como determinar un índice de riesgo en base a la existencia de protecciones y prácticas de control. Gracias a ello la dirección podrá llevar a cabo decisiones informadas, determinando como proporcionar un ambiente seguro en el que el riesgo se reduzca a un nivel y a un costo de gestión aceptables para dirección, clientes, y accionistas.

SeguriData Privada S.A. de C.V. realizará una evaluación de riesgo para evaluar los riesgos de seguridad y determinará las exigencias y procedimientos operacionales necesarios.

SeguriData Privada S.A. de C.V. mantendrá un inventario de todos los activos de la información y asignará una clasificación a las exigencias de protección de tales activos, compatible con el análisis de riesgo efectuado.

Lo anterior, está definido en el documento de Análisis y Evaluación de manejo de riesgos para la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

16 Base de datos Utilizada.

Se utiliza Microsoft SQL Server 2005 como base de datos para la Autoridad de sello digital de tiempo, dentro de la cual se cuenta con las tablas de estampas de tiempo, recibos criptográficos, bloques de recibos criptográficos, con la información necesaria para los sellos de tiempo digital.

El acceso a las bases de datos se realiza mediante la autenticación de un usuario y password, lo que asegura que no puede ser manipulada, es decir borrados o alterados los sellos digitales de tiempo emitidos, además de contar con las pistas de auditoria, las cuales tienen un recibo criptográfico, mediante el cual se reconstruyen las transacciones para asegurar lo anterior

Se maneja el log del manejador de base de datos, el cual es revisado durante el día por el administrador de base de datos, para detectar cualquier tipo de anomalía en la operación o accesos no autorizados.

La base de datos incluye las tablas de:

a. Estampas de tiempo: contiene los datos relacionados con el sello digital de tiempo como: secuencia, emisor, fecha-hora de la solicitud digestión, sello digital de tiempo, fecha y hora de emisión, solicitante.

b. Bloques de recibos criptográficos: contiene parte de las pistas de auditoria como los recibos criptográficos (contienen todos los datos de emisión del sello digital que se tienen en la tabla de estampa de tiempo de manera criptográfica), fecha y hora y el bloque al que corresponden

c. Recibos criptográficos: contiene parte de las pistas de auditoria para la reconstrucción de los sellos digitales de tiempo, fecha, hora, y secuencia del sello digital de tiempo relacionado con su recibo criptográfico (contienen todos los datos de emisión del sello digital que se tienen en la tabla de estampa de tiempo de manera criptográfica).

El concepto de recibo criptográfico que contiene los datos del sello digital emitido, aseguran que no se pueda agregar ningún sello digital de tiempo que no tenga dicho recibo, por lo que no se pueden agregar registros falsos a la base de datos.

La base de datos de sellos digitales de tiempo no podrá ser accedida por ningún sistema que no sea el de Sellos digitales de tiempo (Time Stamping Option pack) por la seguridad del mismo al acceder únicamente a los elementos de NShield 500e F3, Time Stamping Option Pack y manejador de base de datos, explicada a detalle en el Documento Técnico y de Riesgos Jurídicos para el Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

La privacidad de datos cumplirá con las disposiciones de la Ley federal de Protección de Datos Personales en Posesión de Particulares, considerando:

- Observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en dicha Ley.

Con base a:

- La privacidad de los datos personales
- La confidencialidad de la información
- Las medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, esto se detallo en la sección de seguridad física y en esta sección de Base de datos, así como en la de Procedimiento para registro de auditoria.

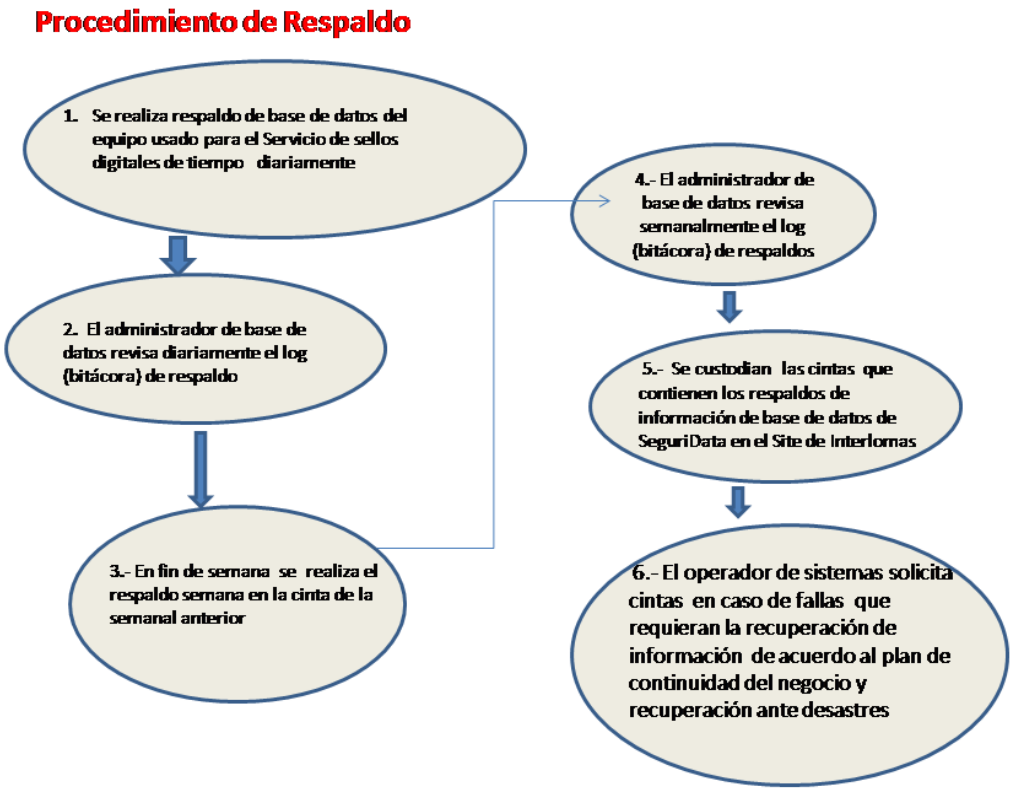
16.1 Respaldo de base de datos

Para llevar a cabo los respaldos se manejara una infraestructura de almacenamiento en cinta de StorageTek a la cual se accede mediante herramientas especializadas, para ejecución y administración de respaldos de VERITAS / LEGATO con la suite de productos de Netbackup / Networker.

El esquema de respaldos a ejecutar sobre la base de datos es:

- El administrador de la base de datos realiza un respaldo de la base de datos a un archivo indicando en que carpeta se guarda para que este archivo cerrado se guarde en cinta.
- Se entregan 2 cintas. Una es la que se utiliza y reescribe diariamente en un respaldo incremental y la otra se resguarda en la cintoteca del centro de datos de Tultitlan site alterno como DRP donde se tiene un respaldo mensual, y se reutilizara cada mes

El esquema de respaldo a ejecutar sobre los archivos cerrados es de un respaldo completo los domingos y respaldos diarios incrementales con un histórico de una semana.



16.1.1 Política de Respaldos

La política contempla la ejecución de un respaldo completo cada 8 días y un respaldo incremental diario entre cada uno de los respaldos completos.

El servicio de respaldo tanto para el Site de Interlomas – principal como el de Tultitlan – alterno, incluye:

- Respaldo completo semanal después de las 20:00 hrs los sábados
- Respaldo diario incremental después de las 20:00hrs
- Respaldo histórico de un mes , último día del mes después de las 20:00 hrs
- Resguardo histórico por mes, en instalaciones de siete de Tultitlan alterno

Se conservara una bitácora de los respaldos efectuados, marcando el servidor, la fecha de respaldo, el tipo de respaldo, la hora de respaldo y el log de la información respaldada

17 Procedimiento para registro de Auditoria

El procedimiento se define de acuerdo a los eventos listados en los puntos anteriores, a partir del servidor TSA cuyos componentes son tarjeta PSI nShield 500e F3, software Time Stamping Option Pack y su relación con el manejador de base de datos SQL Server 2005.

El servidor TSA se audita a través de los log (Bitácoras), que son archivos de texto, con la Firma Electrónica Avanzada de los mismos, usando un certificado para este fin, el cual se emitirá desde la auto certificación, siendo el responsable el administrador de sistemas. Se contempla que el log se firme electrónicamente de manera automática, diariamente por cada transacción registrada, teniendo la fecha y hora.

El monitoreo y revisión de los log se realiza diariamente, y los procesos de auditoria y de inicio de Servidor TSA y manejador de Base de datos, con que operan los Sellos Digitales de Tiempo, se realiza de manera automática, por lo que ante cualquier caída de los mismos, se asegura que al arrancar de nuevo estos procesos se activan de manera automática.

Los datos que se registran en la base de datos para los Sellos Digitales de Tiempo, se efectúan en 3 tablas que son de Estampas de tiempo, Recibos criptográficos y Bloques de recibos criptográficos; donde se obtienen datos de número de secuencia, fecha, emisor, Sello Digital de Tiempo.

Y para el caso de documentación física se establece con relación al resguardo en un sitio seguro en una gaveta asegurada con llave.

Aunado a lo anterior se manejan las pistas de auditoria, las cuales se generan en paralelo a la emisión del sello digital de tiempo y son almacenadas en la base de datos.

La base de datos incluye las tablas de:

- Estampas de tiempo: contiene los datos relacionados con el sello digital de tiempo como: secuencia, emisor, fecha-hora, digestión, sello digital de tiempo.
- Bloques de recibos criptográficos: contiene parte de las pistas de auditoria como los recibos criptográficos, los fecha hora y el bloque al que corresponden

- Recibos criptográficos: contiene parte de las pistas de auditoria para la reconstrucción de los sellos digitales de tiempo, fecha, hora, y secuencia del sello digital de tiempo relacionado con su recibo criptográfico.

Las pistas de auditoria se generan en paralelo al sello digital de tiempo, grabándose en las tablas de bloques de recibos criptográficos la fecha y hora de emisión del sello y el recibo criptográfico correspondiente que contiene el sello digital de tiempo generado, por otro lado se registra dicho recibo criptográfico en la tabla de recibos criptográficos donde se tiene la secuencia del sello digital de tiempo generado, con ambas tablas se regeneran las transacciones realizadas y registradas en la tabla de estampas de tiempo comparando contra las pistas cada sello digital de tiempo emitido y en caso de alguna diferencia, las pistas detectan el problema y se reporta en el log de la base de datos.

Considerando que se toman las medidas necesarias de acuerdo a lo descrito en los documentos de Plan de seguridad física, plan de seguridad de sistemas, y plan de continuidad del negocio y recuperación ante desastres; que los registros de eventos podrían ser parte de las pruebas que el solicitante de un sello digital de tiempo ofrezca en caso de presentarse una contingencia de refutación en la prestación del servicio.

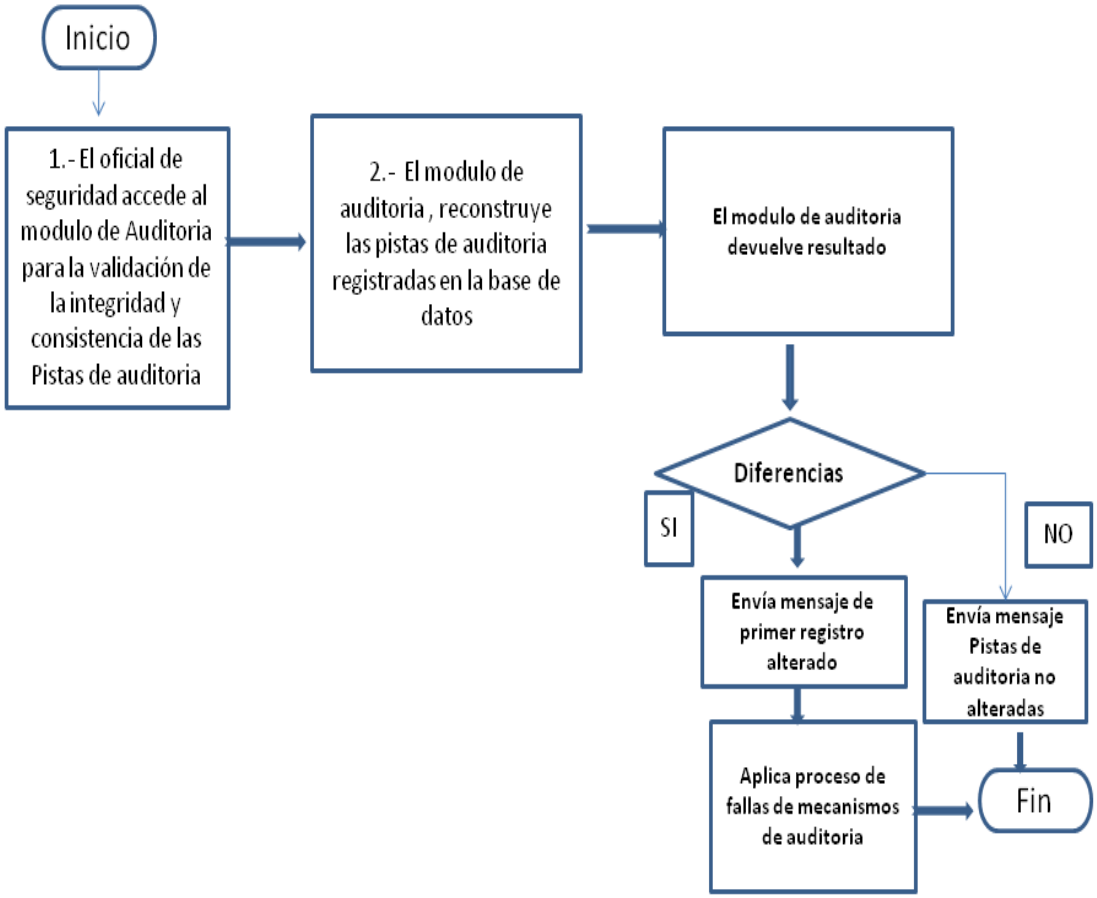
Se guardan los logs de la tarjeta PSI nShield 500e F3 como modulo HSM que contiene el reloj integrado así como el del software Time Stamping Option Pack, y aunados estos dos elementos, se tienen las evidencias logs de la sincronía de tiempo.

Todos los logs generados son respaldados bajo las mismas condiciones que las bases de datos, es decir de manera diaria, semanal y mensual.

A continuación se muestra el procedimiento de registro de auditoria

PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS

Validación de las Pistas de Auditoria



17.1 Archivo de Registros

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. sea registrada durante un período de tiempo de al menos 5 años, en particular con el objetivo de disponer de pruebas, relativas a los Sellos Digitales de Tiempo, que se puedan utilizar en procedimientos judiciales

17.2 Tipos de Registros Archivados

SeguriData Privada S.A. de C.V. archiva y hace disponible bajo petición autorizada, la documentación relacionada con este documento. Para cada sello digital de tiempo. Estos registros incluirán toda la documentación relevante en posesión de SeguriData Privada S.A. de C.V. incluyendo:

- Registros de auditoría. (Información de las pistas de auditoria almacenadas en la base de datos de los Sellos Digitales de Tiempo)
- La solicitud de la expedición del Sello Digital de Tiempo, contratos firmados por clientes (almacenados físicamente en un sitio seguro en gaveta cerrada con llave)
- Contenido de los Sellos Digitales de Tiempo. (almacenada en la base de datos)

17.3 Período de Retención de Archivos

Los archivos de SeguriData Privada S.A. de C.V. serán conservados y protegidos contra la modificación o destrucción durante un plazo de al menos 10 (diez) años, de acuerdo a lo marcado en el artículo 49 del Código de Comercio.

Los registros de Sellos Digitales de Tiempo serán mantenidos por siempre para proporcionar las pruebas necesarias para sustentar la información, en caso se algún proceso legal.

17.3.1 Protección de Archivo

Los archivos serán conservados y protegidos contra la modificación o destrucción. Sólo el Oficial de Seguridad de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., puede ver la totalidad de los archivos. El contenido de los archivos no será revelado, salvo que la legislación lo exija. SeguriData Privada S.A. de C.V. puede decidir liberar los registros de transacciones individuales a petición de cualquiera de las entidades vinculadas en la transacción o sus representantes autorizados.

Los archivos serán registrados de modo que no puedan ser suprimidos o destruidos durante el período de conservación necesario.

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. es registrada durante un período apropiado de tiempo, en particular con el objetivo de disponer de pruebas, relativas a los Sellos Digitales de Tiempo, que se puedan utilizar en procedimientos judiciales.

17.3.2 Procedimientos de Archivo de Reserva

Se aplicarán procedimientos de reserva adecuados, para que en caso de pérdida o destrucción de archivos primarios haya un juego completo de copias de reserva fácilmente disponible, a través de los respaldos de la base de datos que se realizan diariamente y la replicación de la base de datos que de realiza en línea, hacia el Site de Tultitlan como DRP.

17.3.3 Exigencias para el Sellado de Tiempo de los Registros

Todos los acontecimientos registrados dentro del Servicio de Expedición de Sellos Digitales de Tiempo, incluyen la fecha y la hora en el que el acontecimiento ocurrió. Esta fecha y hora se sincronizan con la fecha y hora del CENAM.

17.3.4 Sistema de Registro de Archivos (Interno o Externo)

El sistema de registro de archivos de SeguriData Privada S.A. de C.V. es interno.

17.4 Recuperación ante Desastres y la Revelación de Claves

SeguriData Privada S.A. de C.V. dispone de procedimientos para la recuperación después de desastres. El objetivo de estos es restaurar las actividades esenciales con la mayor rapidez posible cuando los sistemas y/o operaciones se han visto considerablemente afectados por incendios, huelgas, terremotos, inundaciones, etc.

SeguriData Privada S.A. de C.V. posee un Plan de Continuidad del negocio y Recuperación ante desastres apropiados, que asegura la continuación inmediata de los servicios en caso de una emergencia inesperada. SeguriData Privada S.A. de C.V. considera su Plan de Continuidad del negocio y Recuperación ante desastres como propio, y susceptible de contener información sensible o confidencial. En consecuencia su contenido no es públicamente disponible, pero si entregado a Secretaria de Economía como parte de la acreditación en el Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

SeguriData Privada S.A. de C.V. posee un plan frente a la revelación de claves apropiado que detalla sus actividades en caso de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV. Tales proyectos incluyen procedimientos para:

- Notificación inmediata a todos los clientes de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

En caso de revelación de claves de la Autoridad de Sellos digitales de Tiempo de SeguriData Privada S.A. de C.V. se compromete al menos a:

- Informar de la revelación de claves a todos los clientes, a la Secretaria de Economía, y otras entidades con las que tenga acuerdos u otro tipo de relaciones establecidas.

Lo anterior está definido en el documento PSC-SEGURIDATA-ANALISISYEVALUACION-DE-RIESGOSYAMENAZAS-SELLOS-DIGITALESDETIEMPOV1.0.doc y en el PSC-SEGURIDATA-PLANCONTINUIDADNEGOCIOYRECUPERACIONANTEDESASTRE-SELLOS-DIGITALESDETIEMPOV1.0.doc

17.5 Procedimientos de Revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de sello digital de tiempo

En caso de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de sello digital de tiempo, el certificado será revocado, de acuerdo a los procesos señalados en el Plan de Continuidad del Negocio y Recuperación ante Desastres.

17.6 Procedimiento de Continuidad del Negocio tras un Desastre

El Plan de Continuidad del Negocio de SeguriData Privada S.A. de C.V. es estrictamente confidencial y contiene:

- Procedimiento de resolución de incidentes y revelación de claves.
- Gestión de Recursos Informáticos, Software, y/o Datos Corrompidos.
- Capacidad de continuidad del negocio y procedimientos después de un desastre.

SeguriData Privada S.A. de C.V. asegurará en caso de un desastre, incluyendo la revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, que las operaciones serán restauradas cuanto antes.

El Plan de Continuidad del Negocio (o el Plan de Recuperación ante Desastres del servicio de Expedición de sellos Digitales de Tiempo de SeguriData privada SA de CV) tratará como un desastre la revelación o sospecha de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de Sellos Digitales de Tiempo de SeguriData privada SA de CV.

17.7 Terminación de la Autoridad de Sello digital de tiempo

17.7.1 Suspensión Temporal

Este escenario se presenta cuando la Secretaria de Economía sancione a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, con la suspensión temporal por incumplir con alguna de las "reglas generales a las que deberá sujetarse un Prestador de Servicios de Certificación".

Durante el periodo de tiempo definido por la Secretaría de Economía la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV dejará de expedir Sellos Digitales de Tiempo y continuará proporcionando los servicios de consulta de información para no afectar la operación de los clientes.

En caso de una suspensión temporal se realizaran las siguientes actividades:

- Informar mediante el sitio WEB de la Suspensión temporal.
- Tratar de restablecer el servicio a la brevedad.

Anunciar mediante el Sitio WEB, cuando se tenga fecha de restablecimiento del servicio
.

17.7.2 Terminación Definitiva

Si fuera necesario liquidar el servicio de la Autoridad de Sello digital de tiempo, el impacto de la liquidación será reducido al mínimo posible.

SeguriData Privada S.A. de C.V. define la política a seguir en caso de terminación total o parcial de su operación en cuanto a la Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV. La política al menos considera:

- Asegurar que cualquier interrupción causada por la terminación de la Autoridad de sello digital de tiempo, es reducida al mínimo.
- Asegurar que los archivos de registro de la Autoridad de sello digital de tiempo, son conservados.
- Asegurar que la terminación se notifica puntualmente a los clientes, y otras partes relevantes en la Infraestructura de la Autoridad de Sellos digitales de tiempo.
- Se hará disponible al público la información de las razones de la terminación del servicio, a través de la página WEB.

- Notificar al gobierno competente y a los órganos de certificación relevantes, la terminación de operaciones, de acuerdo con la legislación vigente.

- SeguriData Privada tomará medidas para revocar el certificado que utiliza para brindar el servicio de expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

SeguriData Privada S.A. de C.V. asegurará que las interrupciones potenciales a clientes, son reducidas al mínimo como consecuencia del cese de servicios de la Autoridad de sello digital de tiempo y asegura el mantenimiento de los registros necesarios para proporcionar pruebas de cara a un posible procedimiento judicial.

Antes de que la Autoridad de sello digital de tiempo, cese sus servicios ejecutará los siguientes procedimientos:

- Informará a todos los clientes, con las que mantenga acuerdos u otro tipo de relaciones vinculantes sobre el cese de los servicios, terminando la autorización de todos los subcontratistas que actúan en apoyo de la autoridad de sellos digitales de tiempo de SeguriData Privada S.A. de C.V. de cualquier función relacionada al servicio de expedición de Sellos digitales de tiempo.

- Realizará las gestiones necesarias para transferir a un tercero que puede ser otro PSC autorizado o en su caso a la Secretaria de Economía, la obligación de mantener la información y archivos de registro de sucesos durante el período respectivo de tiempo pactado con el cliente.

Las gestiones a realizar con la Secretaria de Economía u otro PSC acreditado en el servicio son:

1) Solicitar al PSC o Secretaria de Economía la aceptación de la transferencia explicando los motivos de la suspensión definitiva del servicio por parte de SeguriData privada SA de CV

2) Obtener la aprobación del PSC o Secretaria de Economía para la transferencia de información, responsabilidades y obligaciones

3) La transferencia de realizara en un dispositivo magnético, con la base de datos actualizada hasta el día de la suspensión definitiva de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, en conjunto con el reporte de lo que se está transfiriendo, ya sea a otro PSC o a la Secretaria de Economía.

El certificado digital de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV se transfiere también en un dispositivo magnético y únicamente para la reconstrucción de las pistas de auditoria no para seguir con la firma de los sellos digitales de tiempo, ya que la clave privada de la autoridad es destruida.

4) Jurídicamente SeguriData Privada SA de CV redactara un escrito detallando la transferencia que se realiza, y los activos que se entregan, cediendo la responsabilidad y obligaciones al PSC o la Secretaria de Economía a la que se realiza dicha transferencia.

Lo anterior adicional a:

- Destruirá o impedirá el uso de sus Datos de Creación de Firma Electrónica avanzada.

El procedimiento para realizar esto, es usando el KEY SAFE de la tarjeta HSM nShield e500F3, donde se listan las llaves resguardadas y se tiene la opción de Discard key, previa identificación del usuario y password valido para esta acción.

Se establece en la Declaración de prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV las provisiones hechas para el cese del servicio. Esto incluirá:

- La notificación a las entidades afectadas.
- Se informa al cliente que se cuenta con un seguro de responsabilidad civil y fianza para cubrir los requerimientos de suspensión en caso de que la autoridad de sellos digitales de tiempo de SeguriData Privada SA de CV este en bancarrota o por otras razones que puedan cubrir costos.

Se asegura que los registros de la operación del servicio de Expedición de Sellos Digitales de Tiempo están disponibles siempre que sean requeridos para proveer evidencia de la operación correcta de dicho servicio, en algún proceso legal. Esto se asegura porque los registros se tienen en la base de datos SQL Server 2005 la cual será respaldada en medios magnéticos seguros (cintas) y resguardad en la caja fuerte de SeguriData y no son eliminados hasta 10 anos después del cese de operaciones de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

17.7.3 Clasificación y Administración de Activos

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV mantiene un inventario de todos los activos consistentes con el análisis y evaluación de riesgos del Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV.

18 Privacidad y Seguridad

Limitantes y Restricciones en el Uso de información

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, debe tomar las medidas técnicas y operativas apropiadas para mitigar el riesgo de procesamiento no autorizado o ilegal de datos personales y de la pérdida o destrucción accidental, o daño, de datos personales de sus clientes.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV utilizará la información proporcionada por el Cliente en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos al servicio de expedición de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, salvo autorización expresa del propio Cliente o por requerimiento de autoridad competente.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, utilizará los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el Cliente y/o usuario, para lo cual deberá informar de las medidas de protección y confidencialidad.

Los Sellos Digitales de Tiempo expedidos por la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., están sujetos únicamente a lo que la presente Política de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV y la Declaración de Prácticas de la autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, establecen.

18.1 Limitación de Responsabilidad

Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos directos o indirectos.

18.1.1 Exclusión de Responsabilidad

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. no asume ninguna responsabilidad cuando se encuentre ante cualquiera de estas circunstancias:

- Si el sello digital de tiempo bajo el control del reclamante ha sido comprometido por mala conservación, falta de confidencialidad, falta de protección contra el acceso, la revelación, el descubrimiento o el uso no autorizado del par de llaves o de cualquier contraseña o datos de activación adicionales para controlar el acceso.

- Si el sello digital bajo el control del reclamante fuera emitido como consecuencia de cualquier falsedad o falsificación de los hechos proporcionados por el cliente para la expedición del sello digital de tiempo.

- Si el sello digital de tiempo bajo el control del reclamante ha sido modificado o cambiado de cualquier modo o usado incumpliendo los términos de esta Política de Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV, de la Declaración de Prácticas de la autoridad de sello digital de tiempo o del contrato con el cliente.

- Si el sello digital de tiempo bajo el control del reclamante fue emitido infringiendo la normatividad aplicable.

- Si se ha desarrollado hardware, software, o algoritmos matemáticos, que conviertan en insegura la criptografía de clave pública, siempre que la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV de SeguriData Privada S.A. de C.V. haga uso de prácticas comercialmente razonables para protegerse contra incumplimientos en la seguridad que sean resultado de tal hardware, software, o algoritmos.

- El fallo de uno o más sistemas informáticos, de infraestructura de las comunicaciones, de procesamiento o resguardo de la información, o de cualquier sub-componente de los sistemas precedentes, que no esté bajo el control exclusivo de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. y/o sus subcontratistas o proveedores de servicio, siempre que SeguriData Privada S.A. de C.V. use métodos comercialmente razonables de protección contra tales perturbaciones.

- Uno o más de los acontecimientos siguientes: Un desastre natural (incluyendo sin restricción, inundación, terremoto, u otra causa natural o meteorológica relacionada); huelga; guerra, insurrección u hostilidades militares abiertas; legislación adversa o acción gubernamental, prohibición, embargo, o boicot; revueltas o perturbaciones civiles; incendio o explosión; epidemia catastrófica; embargo o restricción comercial; cualquier falta de disponibilidad de las telecomunicaciones o integridad, y cualquier acontecimiento o circunstancia fuera del control de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V.

- Por el uso indebido de la información contenida en el Sello digital de tiempo.

18.2 Responsabilidades Económicas

18.2.1 Indemnización por Parte de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

Estipulado en la sección 14.9 de la Declaración de Prácticas de Autoridad de sellado digital de tiempo.

18.2.2 Indemnización por Parte de los Clientes

Al grado permitido por la Declaración de Prácticas de la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV aplicables a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V., los clientes indemnizarán a la Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. por:

- Omisión de revelar un hecho destacado en la solicitud de Sellos Digitales de Tiempo, si la omisión fue realizada negligentemente o con la intención de engañar a una persona o al Profesional Jurídico o agente certificador.
- Mal uso de la IP registrada para la solicitud de expedición de Sellos digitales de tiempo, en el uso de un sistema de confianza, o en la toma de las precauciones necesarias para prevenir el compromiso, pérdida, entrega, modificación o uso no autorizado.
- El uso de parte del cliente de un nombre (incluyendo sin limitación un nombre común, nombre de dominio, IP o correo electrónico) que infrinja los derechos de propiedad intelectual de un tercero, obligándose a sacarlo en paz y a salvo de cualquier reclamación en su contra.

19 Publicación y Responsabilidades de Repositorio

19.1 Actualización de la Política de Autoridad de Sellos Digitales de Tiempo de SeguriData Privada SA de CV

La versión autorizada de este documento de Política de Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. está en todo momento disponible al público en general en la página http://psc.seguridata.com/sellosdigitales.

19.2 Repositorios

SeguriData Privada S.A. de C.V. es responsable de administrar el repositorio de Sellos Digitales de Tiempo.

La Autoridad de Sellos Digitales de Tiempo de SeguriData Privada S.A. de C.V. no mantiene copias de los Datos de Creación de Firma electrónica avanzada.

19.2.1 Disponibilidad del Servicio

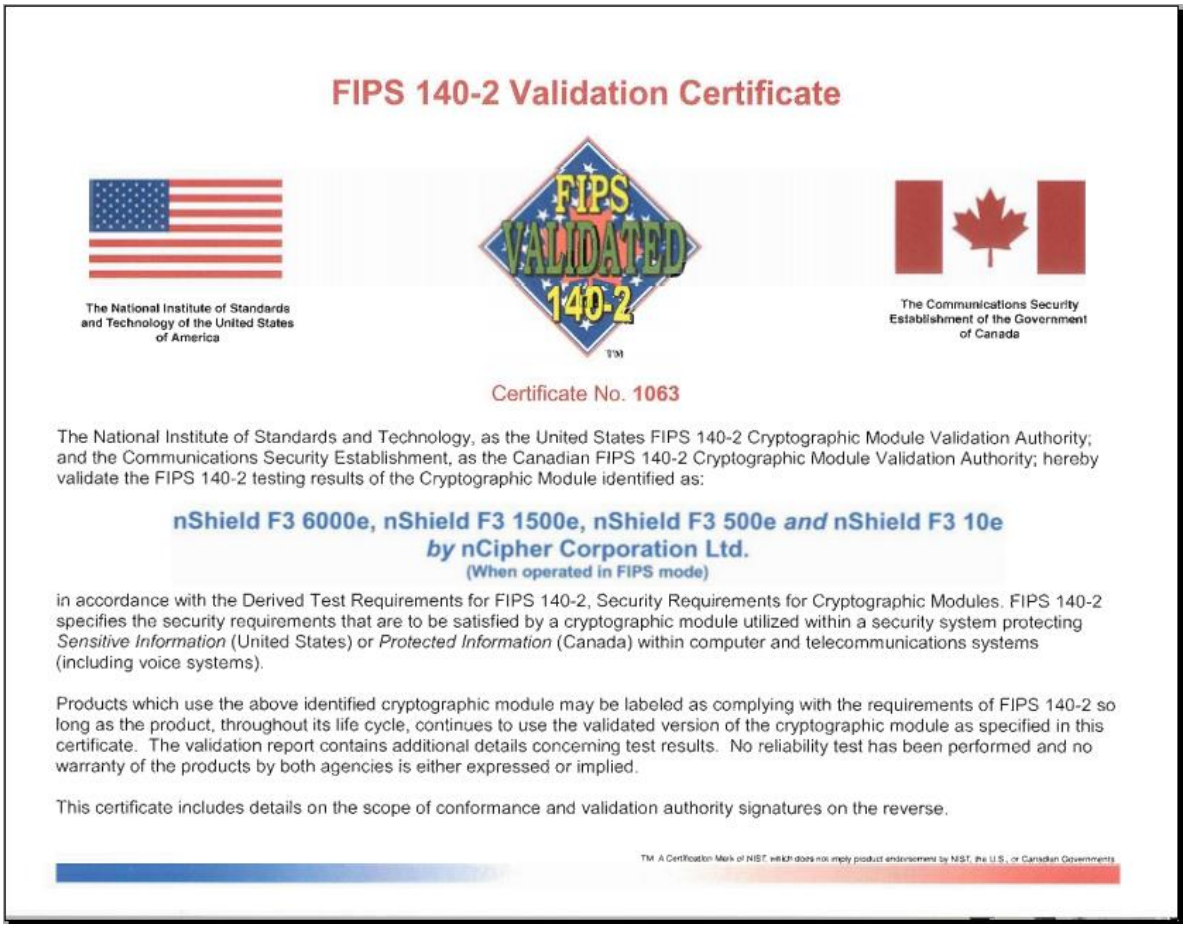
El servicio de consulta y expedición de los Sellos Digitales de Tiempo de SeguriData Privada SA de CV, está disponible 24 horas por día, 7 días por semana, los 365 días del año.

20 Anexos

20.1 Anexo 1 Cumpliendo por parte de Thales del RFC 3161

La ubicación del documento para el cumplimiento de FIPS 140 se puede descargar de:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1063.pdf



FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 1063

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

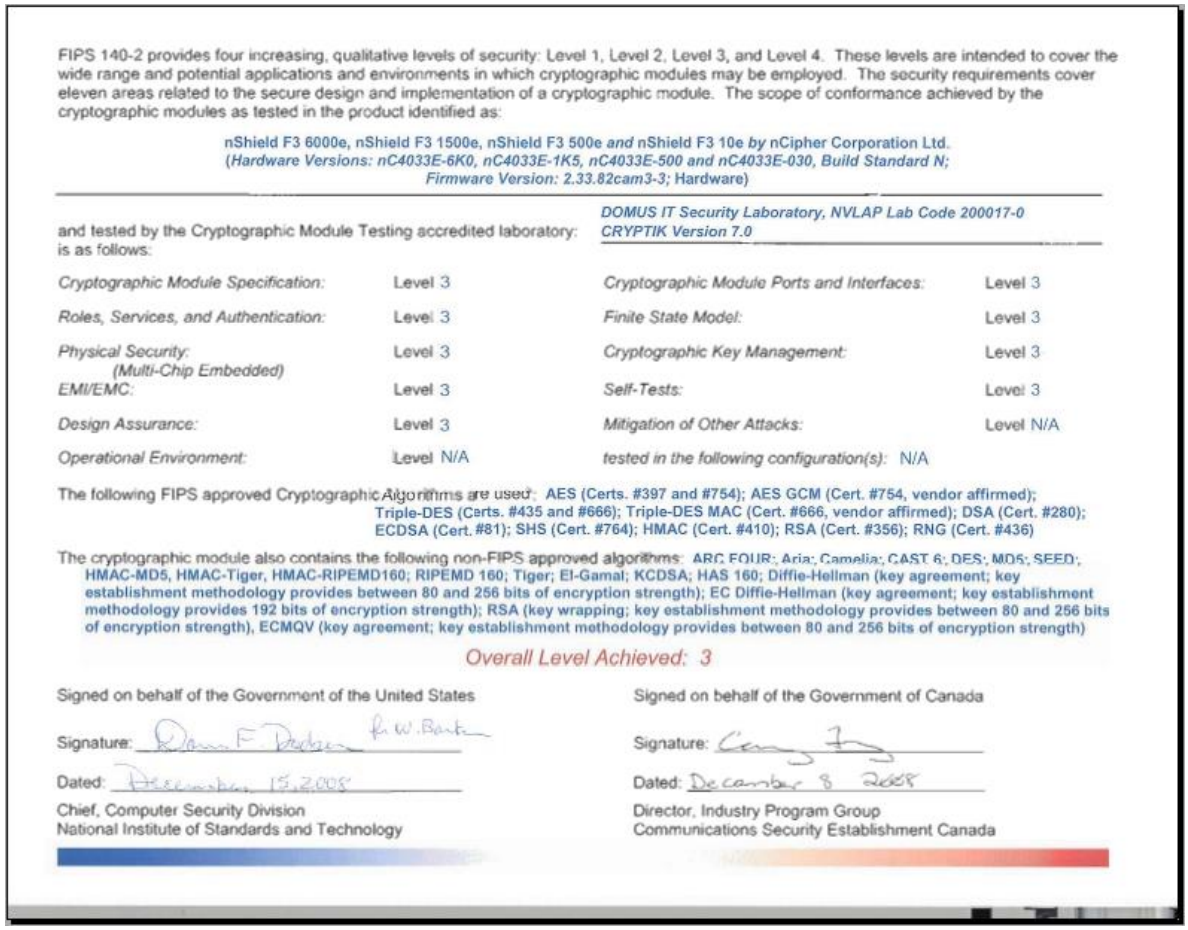
nShield F3 6000e, nShield F3 1500e, nShield F3 500e *and* nShield F3 10e
***by* nCipher Corporation Ltd.**
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments



FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

nShield F3 6000e, nShield F3 1500e, nShield F3 500e *and* nShield F3 10e *by* nCipher Corporation Ltd.
(Hardware Versions: nC4033E-6K0, nC4033E-1K5, nC4033E-500 and nC4033E-030, Build Standard N;
Firmware Version: 2.33.82cam3-3; Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: *DOMUS IT Security Laboratory, NVLAP Lab Code 200017-0*
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 3	*Cryptographic Module Ports and Interfaces:*	Level 3
Roles, Services, and Authentication:	Level 3	*Finite State Model:*	Level 3
Physical Security: *(Multi-Chip Embedded)*	Level 3	*Cryptographic Key Management:*	Level 3
EMI/EMC:	Level 3	*Self-Tests:*	Level 3
Design Assurance:	Level 3	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level N/A	*tested in the following configuration(s):*	N/A

The following FIPS approved Cryptographic Algorithms are used: AES (Certs. #397 and #754); AES GCM (Cert. #754, vendor affirmed); Triple-DES (Certs. #435 and #666); Triple-DES MAC (Cert. #666, vendor affirmed); DSA (Cert. #280); ECDSA (Cert. #81); SHS (Cert. #764); HMAC (Cert. #410); RSA (Cert. #356); RNG (Cert. #436)

The cryptographic module also contains the following non-FIPS approved algorithms: ARC FOUR; Aria; Camelia; CAST 6; DES; MD5; SEED; HMAC-MD5, HMAC-Tiger, HMAC-RIPEMD160; RIPEMD 160; Tiger; El-Gamal; KCDSA; HAS 160; Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides 192 bits of encryption strength); RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength), ECMQV (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)

Overall Level Achieved: 3

Signed on behalf of the Government of the United States

Signature: _____

Dated: December 15, 2005

Chief, Computer Security Division
National Institute of Standards and Technology

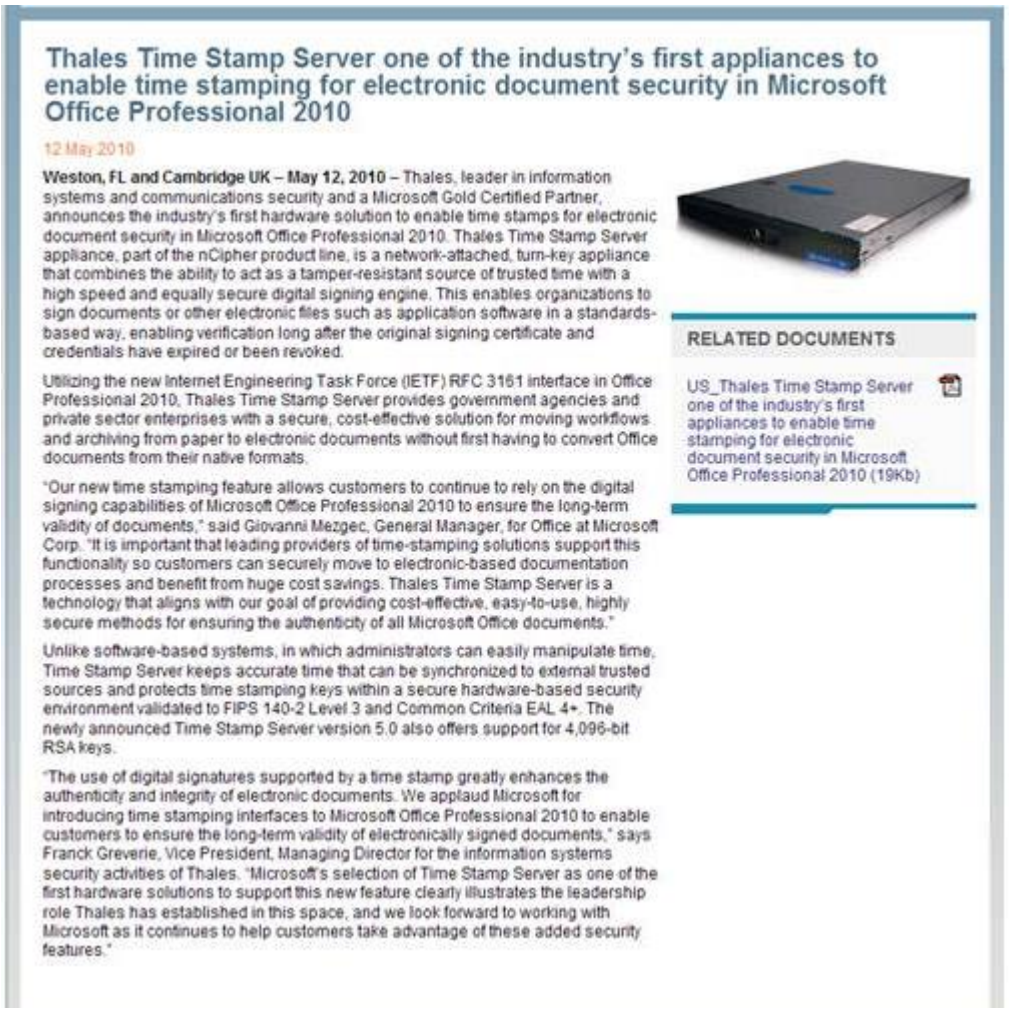
Signed on behalf of the Government of Canada

Signature: _____

Dated: December 8 2005

Director, Industry Program Group
Communications Security Establishment Canada

http://www.thalesgroup.com/Pages/PressRelease.aspx?id=12868



Thales Time Stamp Server one of the industry's first appliances to enable time stamping for electronic document security in Microsoft Office Professional 2010

12 May 2010

Weston, FL and Cambridge UK – May 12, 2010 – Thales, leader in information systems and communications security and a Microsoft Gold Certified Partner, announces the industry's first hardware solution to enable time stamps for electronic document security in Microsoft Office Professional 2010. Thales Time Stamp Server appliance, part of the nCipher product line, is a network-attached, turn-key appliance that combines the ability to act as a tamper-resistant source of trusted time with a high speed and equally secure digital signing engine. This enables organizations to sign documents or other electronic files such as application software in a standards-based way, enabling verification long after the original signing certificate and credentials have expired or been revoked.

Utilizing the new Internet Engineering Task Force (IETF) RFC 3161 interface in Office Professional 2010, Thales Time Stamp Server provides government agencies and private sector enterprises with a secure, cost-effective solution for moving workflows and archiving from paper to electronic documents without first having to convert Office documents from their native formats.

"Our new time stamping feature allows customers to continue to rely on the digital signing capabilities of Microsoft Office Professional 2010 to ensure the long-term validity of documents," said Giovanni Mezgec, General Manager, for Office at Microsoft Corp. "It is important that leading providers of time-stamping solutions support this functionality so customers can securely move to electronic-based documentation processes and benefit from huge cost savings. Thales Time Stamp Server is a technology that aligns with our goal of providing cost-effective, easy-to-use, highly secure methods for ensuring the authenticity of all Microsoft Office documents."

Unlike software-based systems, in which administrators can easily manipulate time, Time Stamp Server keeps accurate time that can be synchronized to external trusted sources and protects time stamping keys within a secure hardware-based security environment validated to FIPS 140-2 Level 3 and Common Criteria EAL 4+. The newly announced Time Stamp Server version 5.0 also offers support for 4,096-bit RSA keys.

"The use of digital signatures supported by a time stamp greatly enhances the authenticity and integrity of electronic documents. We applaud Microsoft for introducing time stamping interfaces to Microsoft Office Professional 2010 to enable customers to ensure the long-term validity of electronically signed documents," says Franck Greverie, Vice President, Managing Director for the information systems security activities of Thales. "Microsoft's selection of Time Stamp Server as one of the first hardware solutions to support this new feature clearly illustrates the leadership role Thales has established in this space, and we look forward to working with Microsoft as it continues to help customers take advantage of these added security features."

RELATED DOCUMENTS

US_Thales Time Stamp Server one of the industry's first appliances to enable time stamping for electronic document security in Microsoft Office Professional 2010 (19Kb)