Política de Autoridad de Constancias de Conservación de Mensajes de datos de acuerdo a la NOM 151-SCFI-2016

OID: 2.16.484.101.10.316.2.5.1.2.2.1.2

Versión 1.2
Noviembre, 2019

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-JULIO-2011	DOCUMENTO INICIAL
1.1	2-SEPTIEMBRE-2011	ADECUACIONES POR PREVENTORIO DE SECRETARIA DE ECONOMIA

1.2	**NOVIEMBRE 2019**	**ACTUALIZACIÓN DRP EN TULTITLAN Y NOM 151 SCFI 2016**

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
D.F.	INSURGENTES SUR 2375	OLGA GARCIA	MAGNETICO Y PAPEL
D.F.	REDIT 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 Constancias de Conservación de mensajes de datos, lo que no implica una actualización del mismo.

FECHAS PROGRAMADAS DE FUTURAS REVISIONES
01/02/2021
Por determinar
Por determinar

2. Introducción

SeguriData Privada S.A. de C.V. esta acreditada para el servicio de certificados de FEA, y está en proceso para las acreditaciones para el servicio de Expedición de Constancias de Conservación de mensajes de datos, ante la Secretaria de Economía.

La presente Política contiene las políticas que regirán el funcionamiento y operación para el servicio de Expedición de Constancias de Conservación de mensajes de datos de acuerdo a la NOM-151-SCFI-2016, así como la gestión de las constancias emitidas.

La presente Política tiene por objeto el permitir a personas físicas o morales (por medio del representante legal), acreditar ante cualquier tercero o autoridad que los documentos electrónicos se han conservados íntegros y sin cambios desde el momento de su generación.

3. Alcance

El ámbito de aplicación se extiende a los comerciantes que deben conservar los mensajes de datos en que se consignen contratos, convenios, o compromisos que den nacimiento a derechos y obligaciones, así como todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

4. Referencias

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

- Norma Oficial Mexicana NOM-151-SCFI-2016, Prácticas Comerciales-Requisitos que deben observarse para la conservación de mensajes de datos. (publicado(a) en el Diario Oficial de la Federación el 04/06/2016).

- Articulo 102 incisos A, Reformas al Código de Comercio. (publicado(a) en el Diario Oficial de la Federación el 29/08/03), Artículos 7, 8 y 9, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación. (publicado(a) en el Diario Oficial de la Federación el 19/07/2004).

- 2 bis, 2 bis.1., Reforma a las Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. (publicado(a) en el Diario Oficial de la Federación el 01/03/2007).

5. 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
Aceptación de autoría	A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente
Acto de comercio	A todo acto que la legislación vigente considera como tal
Autenticación	Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.
Archivo parcial	Al mensaje de datos representado en formato ASN.1, que contiene el nombre, tipo y contenido de los archivos, conforme al apéndice de la Norma Oficial Mexicana
Solicitante	Es la persona física o moral que inicia el trámite para obtener una constancia de conservación de mensajes de datos
Cliente	La persona física o moral que requiere el servicio proporcionado por la Autoridad de Constancias de Conservación de Mensajes de Datos y que han aceptado explícitamente sus términos y condiciones
ASN.1	A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).
BITS	A la unidad mínima de información que puede ser procesada por una computadora
Clave Publica	A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.
Clave privada	A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.
Certificado Digital	Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública
Contrato	Al acuerdo de voluntades que crea o transfiere derechos y obligaciones
Convenio	Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones
Constancia	Al mensaje de datos representado en formato ASN.1, que contiene el nombre del archivo, el expediente, la fecha y hora (sello digital de tiempo) en el momento en que se crea la constancia; la identificación del PSC y la firma electrónica avanzada del PSC; conforme al apéndice de la

TÉRMINO	DEFINICIÓN
	Norma Oficial Mexicana
Criptografía	Al conjunto de técnicas matemáticas para cifrar información.
Destinatario	A aquella entidad a quien va dirigido un mensaje de datos
Emisor	A aquella entidad que genera y transmite un mensaje de datos
Entidad	A las personas físicas o morales.
Firma electrónica avanzada	A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica avanzada establece la relación entre los datos y la identidad del firmante
Formato	A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información
Legislación	A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.
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.
Cliente	El termino cliente se usara de manera indistinta como la figura del operador marcado en la NOM-151-SCFI-2016
Servidor TSA	Se refiere al servidor que otorga el Servicio de Expedición de Sellos Digitales de Tiempo de SeguriData privada S:A. de C.V.

6 Identificación del Documento de Política de la Autoridad de Constancias de Conservación de Mensajes de Datos

Nombre del documento	Política de la autoridad de Constancias de Conservación de Mensajes de datos de SeguriData Privada S.A. de C.V.
Versión del documento	1.2
Autor	SeguriData Privada S.A. de C.V.

Estado del documento	ACTUALIZADO
Fecha de emisión	2/Septiembre/2011
Fecha de inicio de uso	Inmediato
Fecha de expiración	No es aplicable
Identificador Digital de Objetos – OID (Object Identifier Digital)	2.16.484.101.10.316.2.5.1.2.2.1.2
Localización (URL) de la Política de la autoridad de constancias de conservación de mensajes de datos	http://psc.seguridata.com/docs/doc20.pdf
Declaración de Prácticas Asociada	Declaración de Prácticas para la Autoridad de constancias de Conservación de mensajes de datos de SeguriData Privada S.A. de C.V. de acuerdo a la NOM151-SCFI-2016

El servicio de Expedición de constancias de conservación de mensajes de datos, está disponible para personas físicas y morales (a través de un representante legal), que requieran incorporar en sus procesos y/o servicios las constancias de conservación de mensajes de datos, por la Autoridad de Constancias de conservación de mensajes de datos de SeguriData Privada S.A. de C.V.

7 Administración del Documento de Política de la Autoridad de las Constancias de Conservación de Mensajes de Datos

Responsable de la Administración de la Política de la Autoridad de las Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V.

Nombre	SeguriData Privada S.A. de C.V.
Correo electrónico	psc@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

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.

7.1 Determinación de Cambios en esta Política de la Autoridad de Constancias de Conservación de Mensajes de Datos y su Publicación.

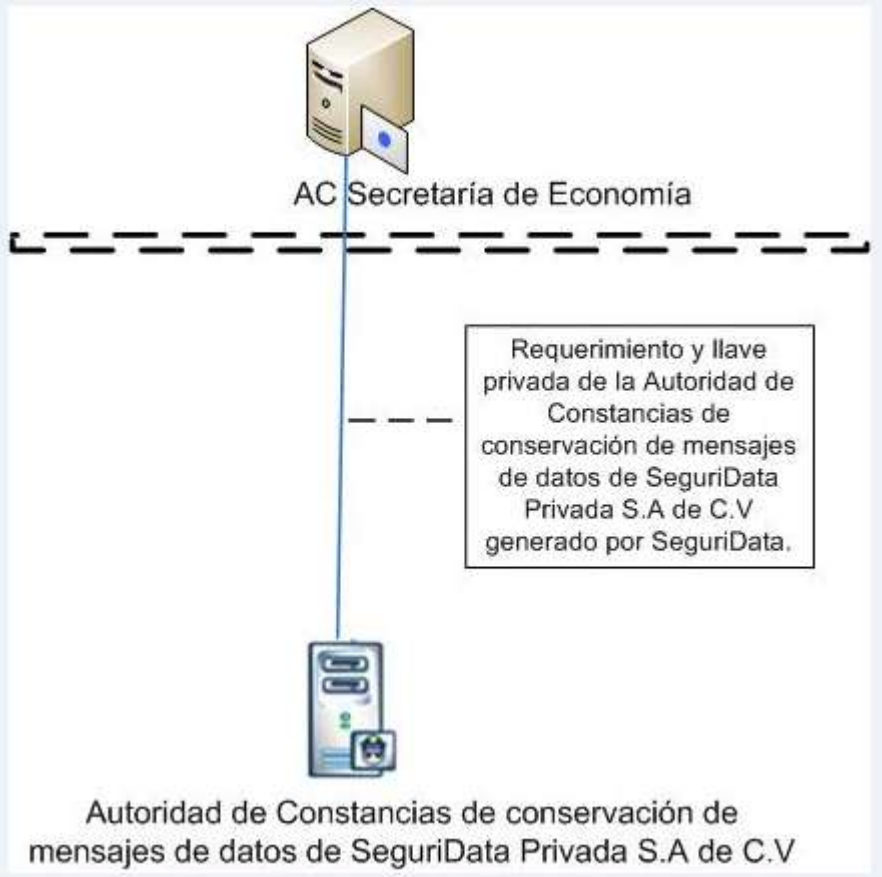
Las modificaciones propuestas o las nuevas aportaciones a incluir en esta Política, deberán, previa a su aprobación, ser contrastadas con la Declaración definida, a fin de asegurar que sean soportados estos cambios.

No se podrán realizar cambios que no sean soportados por la Declaración de prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData privada S.A. de C.V.. Deberá, en todo caso, contemplarse una actualización de dicha Declaración.

La presente Política de la Autoridad de Constancias de Conservación de Mensajes de Datos se publica, en el sitio WEB del PSC SeguriData.

8 Estructura Jerárquica

La representación esquemática de los componentes involucrados en la Infraestructura de la Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. es la que se muestra en la figura.



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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V., con la que se firmaran las Constancias de Conservación de Mensajes de Datos expedidos

La representación esquemática de los componentes involucrados en el servicio de Expedición de Constancias de Conservación de Mensajes de Datos de acuerdo a la NOM-151-SCFI-2016, se muestra a continuación:

8.1 Participantes en el servicio de Expedición de Constancias de Conservación de Mensajes de Datos

8.1.1 Autoridad Certificadora SeguriData

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

8.1.2 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.

8.1.3 Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V.

Autoridad acreditada por la Secretaría de Economía para expedir Constancias de Conservación de Mensajes de Datos.

8.1.4 Clientes-Operadores

A las personas físicas o morales que requieren los servicios proporcionados por la autoridad de Constancias de Conservación de Mensajes de Datos y que han aceptado explícitamente sus términos y condiciones

8.1.5 Profesional Jurídico auxiliado del Agente certificador

El profesional jurídico y el agente certificador 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.

Se define al agente certificador como apoyo al profesional jurídico, en los casos en que este último no se encuentre en las oficinas, de inicio el agente certificador será el que se tiene acreditado en la Secretaria de Economía, sin dejar de contemplar a los agentes certificadores que en un futuro se puedan dar de alta ante dicha Secretaria.

La misión del profesional jurídico y su auxiliar, es realizar las funciones de asistencia a la Autoridad de Constancias de Conservación de Mensajes de Datos 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 las Constancias de Conservación de Mensajes de Datos.

9 Obligaciones y Responsabilidades

9.1 Obligaciones de la Autoridad de Constancias de Conservación de Mensajes de Datos

- La Autoridad Constancias de Conservación de Mensajes de Datos debe asegurar que todos los requerimientos están implementados de acuerdo a lo establecido en la NOM-151-SCFI-2016

- La Autoridad de Constancias de Conservación de Mensajes de Datos debe proporcionar todos sus servicios en forma consistente y como lo establece la Declaración de prácticas de la autoridad de constancias de conservación de mensajes de datos.

- La Autoridad de Constancias de Conservación de Mensajes de Datos debe atender las solicitudes de servicio de acuerdo a los términos y condiciones establecidas en el convenio suscrito por ambas partes, incluyendo los niveles de servicio, la disponibilidad y la exactitud de su servicio.

- La Autoridad de Constancias de Conservación de Mensajes de Datos debe verificar la identidad de los solicitantes del servicio de Expedición de Constancias de Conservación de Mensajes de Datos de acuerdo a lo establecido en la Declaración de prácticas de la autoridad de constancias de conservación de mensajes de datos.

- Proporcionar a los clientes la información necesaria sobre los términos y condiciones respecto al uso del Servicio de expedición de Constancias de Conservación de Mensajes de Datos, a través del contrato.

- Debe contar con la infraestructura necesaria que brinde disponibilidad y acceso permanente al servicio de expedición de Constancias de Conservación de Mensajes de Datos.

- La Autoridad de Constancias de Conservación de Mensajes de Datos 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.

9.2 Obligaciones del Cliente

- El Cliente debe resguardar sus claves de acceso al servicio de Expedición de Constancias de Conservación de Mensajes de Datos
- Verificar que el certificado no esté revocado
- Contar con los elementos necesarios que le permitan correlacionar certificados con los documentos para los cuales fueron solicitados.

9.3 Obligaciones del Administrador del servicio

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. asigno a un Administrador para atender al cliente, y debe realizar sus funciones y obligaciones conforme a:

- Debe realizar la comprobación de datos de los clientes para la expedición de Constancias de Conservación de Mensajes de Datos , 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 la Expedición de Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V.
- 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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V.

9.4 Responsabilidad de la Autoridad de Constancias de Conservación de Mensajes de Datos

La responsabilidad está limitada exclusivamente a proveer el servicio de Expedición de Constancias de Conservación de Mensajes de Datos de acuerdo a lo establecido en la Declaración y en la Política de la Autoridad de Constancias de Conservación de Mensajes de Datos.

La Autoridad de Constancias de Conservación de Mensajes de Datos, establecerá una garantía en el convenio que suscriba con los usuarios, cuando estos así lo soliciten, consistente en una fianza de cumplimiento de sus obligaciones como prestador del servicio de Expedición de Constancias de Conservación de Mensajes de Datos la cual no podrá exceder del 10% del monto total anual del contrato que suscriba con los usuarios.

La Autoridad de Constancias de Conservación de Mensajes de Datos 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 de los servicios por parte de dichos clientes.

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

- Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los clientes del Servicio de Expedición de Constancias de Conservación de Mensajes de Datos en el uso del servicio, sin que estas hayan sido confirmadas expresamente por la Autoridad de Constancias de Conservación de Mensajes de Datos.

- 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 Constancias de Conservación de Mensajes de Datos

- Por la interrupción o alteración temporal del servicio por causas ajenas a la Autoridad de Constancias de Conservación de Mensajes de Datos, 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.

9.5 Responsabilidad del Cliente

- Guardar las claves de acceso definidas para el servicio de Expedición de Constancias de Conservación de Mensajes de Datos
- Guardar las Constancias de Conservación de Mensajes de Datos y administrar su correlación con los mensajes de datos para los cuales fueron solicitadas las Constancias de Conservación de Mensajes de Datos.

9.6 Responsabilidad del Profesional Jurídico y su auxiliar el Agente certificador

- Proporcionar el servicio para la contratación del servicio de Expedición de Constancias de Conservación de Mensajes de Datos

10 Publicación y Consulta de Información

10.1 Consulta de Información del Servicio de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos, es responsable de poner a disposición del público en general, la información relacionada con el servicio de Expedición de Constancias de Conservación de Mensajes de Datos, a través del sitio WEB del PSC SeguriData.

10.2 Publicación de Certificado Digital de la Autoridad de Constancias de Conservación de Mensajes de Datos

El Certificado Digital de la Autoridad de Constancias de Conservación de Mensajes de Datos, se publica en el sitio WEB del PSC SeguriData y en el de la Secretaría de Economía, para que los clientes puedan verificar la integridad y la autenticidad de las Constancias de Conservación de Mensajes de Datos que emite.

11 Ciclo de Vida de la Administración de Claves de la Autoridad de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos para emitir Constancias de Conservación de Mensajes de Datos cuenta con una clave pública y una clave privada, dichas claves tienen un ciclo de vida comprendido desde la generación, protección, resguardo y distribución, vigencia y renovación

11.1 Generación de Claves de la Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada.

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada debe asegurar que cualquier clave criptográfica esté generada bajo circunstancias controladas.

La generación de las claves de la Autoridad de Constancias de Conservación de Mensajes de Datos 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 constancias de Conservación de Mensajes de Datos debe llevarse a cabo dentro de un módulo de seguridad de hardware criptográfico que cumpla con los requerimientos identificados en FIPS 140-2.

El algoritmo de la generación de las claves de la Autoridad de Constancias de Conservación de Mensajes de Datos, la longitud de la clave resultante y el algoritmo usado para firmar las Constancias de Conservación de Mensajes de Datos deben ser aprobados por la Secretaría de Economía.

11.2 Protección y resguardo de las Claves Privadas de la Autoridad de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada debe asegurar que se mantenga en todo momento la confidencialidad e integridad de sus claves privadas.

Las claves privadas de la Autoridad de Constancias de Conservación de Mensajes de Datos deben 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.

Las claves privadas que sean respaldadas, deben ser almacenadas y recuperadas solamente por personal con roles de confianza, usando, el control mancomunado 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 Constancias de Conservación de mensajes de SeguriData Privada.

Las copias de respaldo de las claves privadas deben ser protegidas para asegurar su confidencialidad e integridad.

11.3 Distribución de las Claves Públicas de la Autoridad de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada debe asegurar que la integridad y la autenticidad de las claves de verificación de firma de las Constancias de Conservación de Mensajes de Datos se mantienen seguras durante su distribución.

Los Certificados Digitales de la Autoridad de Constancias de Conservación de Mensajes de Datos SeguriData Privada se deben publicar en el sitio Web de la Constancias de Conservación de Mensajes de Datos de SeguriData Privada y de la Secretaría de Economía, para que los clientes puedan verificar la integridad y la autenticidad de los Constancias de Conservación de Mensajes de Datos que emita la Constancias de Conservación de Mensajes de Datos de SeguriData Privada

La Autoridad de Constancias de Conservación de Mensajes de Datos SeguriData Privada debe tener implementadas políticas y controles.

11.4 Renovación de las Claves Criptográficas de la Autoridad de Constancias de Conservación de Mensajes de Datos

El Certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos. De igual forma no debe ser utilizado más allá del periodo de vigencia del mismo

En cualquiera de estas condiciones se debe proceder a emitir nuevas claves de la Autoridad de Constancias de Conservación de Mensajes de Datos e incorporarlas al ambiente productivo, ya que SeguriData no usa ni recomienda la renovación.

11.5 Fin del Ciclo de Vida de las Claves de la Autoridad de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada 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 Constancias de Conservación de Mensajes de Datos SeguriData Privada expiren

Se asegura la Expedición de nuevas claves antes de que éstas expiren, o cuando se vea comprometida su confidencialidad.

11.6 Ciclo de Vida del Módulo Criptográfico – Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada

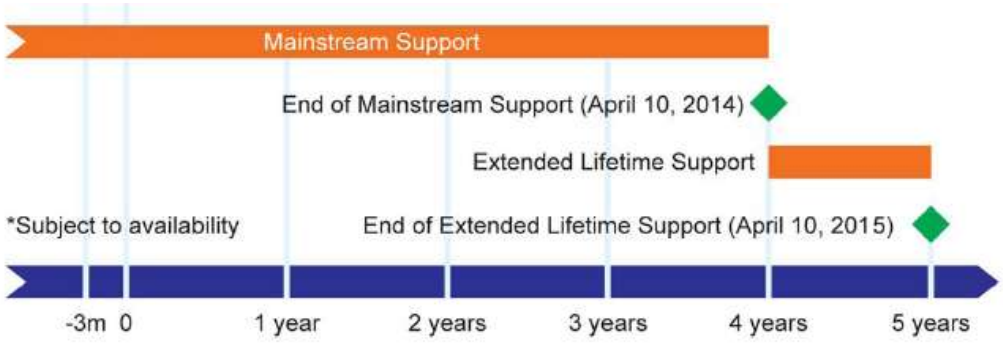
La Autoridad de Constancias de Conservación de Mensajes de Datos SeguriData Privada debe garantizar la seguridad del hardware criptográfico para la administración, almacenamiento y uso de su clave privada de la autoridad de Constancias de Conservación de Mensajes de Datos, que se encuentra en el dispositivo nShield 500. Como parte de la administración del ciclo de vida de los dispositivos criptográficos.

El hardware criptográfico que firma las Constancias de Conservación de Mensajes de Datos debe estar funcionando correctamente y bajo condiciones que garanticen la integridad de las claves privadas de la autoridad de Constancias de Conservación de Mensajes de Datos.

11.6.1 Ciclo de Vida productos Thales

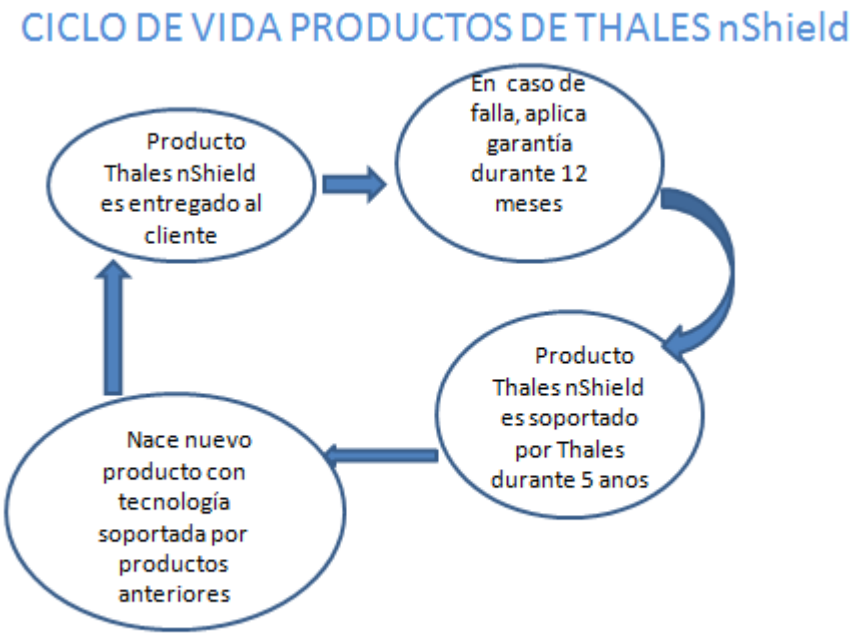
Thales garantiza que sus productos funcionarán sustancialmente. Dicha garantía es válida por un período de doce (12) meses a partir de la fecha de entrega en el caso de hardware. En caso de que la funcionalidad del producto sea materialmente deteriorada en virtud de los defectos de fabricación, THALES 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 nShield, su ciclo de vida es

al año 2015, con la garantía de que su funcionamiento se continúa soportando hacia los nuevos modelos.



12 Constancias de Conservación de Mensajes de Datos - Generalidades

Las Constancias de Conservación de Mensajes de Datos vinculan el expediente enviado por el cliente con las Constancias de Conservación de Mensajes de Datos (con una fecha y hora).

El contenido de los mensajes de datos se conserva integro e inalterado a partir del momento en que se genero por primera vez en su forma definitiva, y es accesible para su ulterior consulta, para aclaración de cualquier controversia, por lo que tiene fuerza probatoria.

Los elementos que se generan para la Conservación de los mensajes son:

- Archivo(s) Parcial(es) mensaje(s) en formato ASN.1 que contiene(n) el nombre, tipo y contenido(s) del/los archivo(s)
- Compendio(s) o resumen(es) digital(es): Se obtienen de los archivos parciales utilizando el algoritmo criptográfico SHA-1.

- Expediente: Mensaje en formato ASN.1 que contiene el nombre del Expediente, un índice (con el nombre y compendio de cada archivo parcial); la identificación de la autoridad de Constancias de conservación de mensajes de datos, y la firma de la autoridad de Constancias de conservación de mensajes de datos.

Con lo anterior el Servicio de Expedición de Constancias de Conservación de mensajes de datos genera la CONSTANCIA, que es un mensaje en formato ASN.1 que contiene: el nombre del archivo, el expediente, la fecha y hora (sello digital de tiempo emitido por el servidor TSA, Autoridad de Sellos Digitales de Tiempo, sincronizado con una fuente confiable de tiempo CENAM), la identificación de la Autoridad y la firma de la autoridad de Constancias de Conservación de mensajes de datos.

12.1 Uso y Limites de Uso de Constancias de Conservación de Mensajes de Datos

Su ámbito de aplicación se extiende a los comerciantes que deben conservar los mensajes de datos en que se consignen contratos, convenios, o compromisos que den nacimiento a derechos y obligaciones, así como a todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

La Autoridad de Conservación de Mensajes de Datos expide Constancias de Conservación de Mensajes de Datos para uso, principalmente, en operaciones de actos de comercio.

Las constancias de Conservación de mensajes de datos brindan seguridad jurídica al comercio electrónico preservando la confidencialidad de los documentos.

El contenido de los mensajes de datos se conserva integro e inalterado a partir del momento en que se genero por primera vez en su forma definitiva, y es accesible para su ulterior consulta, para aclaración de cualquier controversia, por lo que tiene fuerza probatoria, en controversias judiciales.

12.2 Información en las Constancias de Conservación de Mensajes de Datos

Las Constancias de Conservación de Mensajes de Datos de SeguriData Privada deben asegurar que los Constancias de Conservación de Mensajes de Datos sean emitidos a través de un proceso seguro y contengan la fecha y hora correctas.

Las Constancias de conservación de mensajes de datos, están formadas por un mensaje en formato ASN.1 que contiene: el nombre del archivo, el expediente, la fecha y hora (sello digital de tiempo emitido por el servidor TSA, Autoridad de Sellos Digitales de Tiempo, sincronizado con una

fuente confiable de tiempo CENAM), la identificación de la Autoridad y la firma de la autoridad de Constancias de Conservación de mensajes de datos.

12.2.1 Vigencia de los Constancias de Conservación de Mensajes de Datos

La vigencia de las Constancias de Conservación de Mensajes de Datos está en función del periodo de vigencia de las claves de las Constancias de Conservación de Mensajes de Datos (10 años),

12.3 Política de Deshecho – Limitantes

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada debe:

Rechazar las peticiones de Expedición de Constancias de Conservación de Mensajes de Datos, cuando el Certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada SA de CV este revocada o haya vencido.

Asegurar que después de la desincorporación de las claves de la autoridad de Constancias de Conservación de Mensajes de Datos, estas no puedan ser accedidas ni usadas para ningún propósito diferente al menos que se requiera para aclaración de alguna controversia.

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada SA de CV a partir del servidor TSA no debe expedir Constancias de Conservación de Mensajes de Datos, 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, para la fecha y hora de la misma.

12.4 Grado de Fiabilidad de los Mecanismos y Dispositivos utilizados

Los puntos importantes para asegurar la fiabilidad de los mecanismos de Constancias de Conservación de mensajes de datos, son:

1. La seguridad que se da al acceso a la autoridad de emisión de constancias de NOM-151 SCFI 2016

2. La seguridad que se da al software cliente solicitante de constancias NOM-151SCFI 2016

3 La precisión y exactitud de la fuente de tiempo

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

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

6. La disponibilidad de la TSA (cuando se implementa el RFC3161 dentro de la constancia de conservación de mensajes de datos).

12.4.1 Seguridad en el acceso a la Autoridad de Constancias de Conservación de Mensajes de Datos de PSC SeguriData

La Autoridad de Constancias de Conservación de Mensajes de Datos del PSC se encuentra almacenada y custodiada en un módulo HSM que cumple con el FIPS 140-2 nivel 3. Las llaves se generan dentro del módulo y por las características del FIPS 140-2 nivel 3, éstas nunca abandonan el hardware en claro. Incluso, si el hardware fuera manipulado y se abriera, las llaves se eliminarían automáticamente en dicho intento.

13 Proceso para la prestación del servicio de Expedición de Constancias de Conservación de Mensajes de Datos.

Los pasos a seguir por el solicitante para contratar el Servicio de Expedición de Constancias de Conservación de Mensajes de Datos son:

- El solicitante realiza cita telefónica para acudir a oficinas de SeguriData, al menos con 2 días de anticipación.
- PSC Administrador recibe la IP desde la cual solicitara las Constancias de conservación de mensajes de datos
- PSC Administrador realiza el cotejo de documentos originales contra las copias presentadas por el Solicitante, para su autenticación.
- PSC Administrador formaliza la contratación del servicio con la firma del contrato.
- PSC Administrador proporciona aviso de privacidad para firma del cliente.
- PSC Administrador brinda soporte al solicitante durante el proceso de Expedición de Constancias de Conservación de mensajes de datos.

13.1 Autenticación de la Identidad de un Individuo

La Autoridad de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. recaba una serie de documentos para realizar una correcta verificación de la identidad del solicitante de la constancia de conservación de mensajes de datos,

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.

La autenticación la realiza el administrador asignado, validando los documentos originales contra las copias

13.2 Procedimiento para la atención a solicitantes del Servicio de Expedición de Constancias de Conservación de Mensajes de Datos

La atención se realiza a través del administrador, quien es personal se SeguriData Privada SA de CV.

El solicitante del servicio de Expedición de Constancias de Conservación de mensajes de dato debe:

1. Llena el formato "Solicitud de servicio de expedición de Constancias de Conservación de Mensajes de Datos" (Anexo 1) el cual se encuentra disponible en el sitio de Internet http://psc.seguridata.com/constanciasdeconservacion

Consideraciones para el llenado del formato:

Persona Física:

- Nombre completo del Solicitante iniciando por el Nombre(s), Apellido Paterno y Apellido Materno.
- Registro Federal de Contribuyentes.
- Domicilio particular del Solicitante, indicando la calle, número exterior y en su caso, número interior y la colonia.
- Número de Serie del Certificado Digital con el que se autenticará para solicitar la emisión de las Constancias de Conservación de Mensajes de Datos.
- Responsable de la emisión del Certificado Digital: Autoridad Certificadora (AC) Acreditada por la Secretaría de Economía
- IP desde la cual solicitara las Constancias de conservación de mensajes de datos

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 la cual solicitara las Constancias de conservación de mensajes de datos

2. Entregar al Administrador la solicitud del servicio debidamente requisitada y firmada de manera autógrafa por el Solicitante.

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

13.2.1 Otorgamiento del Servicio

Para el otorgamiento del servicio el personal responsable de la autoridad de Constancias de Conservación de Mensajes de Datos y el Cliente desempeña las actividades siguientes:

El Administrador realiza 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 Constancias de Conservación de Mensajes de Datos, para lo cual realiza lo siguiente:

- Recibir solicitud de servicio y verificar la documentación presentada por el Solicitante.
- Formalizar la contratación del servicio con la firma del contrato y del aviso de privacidad
- Es responsable de tramitar el alta del cliente en el sistema de Constancias de Conservación de Mensajes de Datos
- Brinda soporte al usuario para comprobar la funcionalidad de emisión del Constancias de Conservación de Mensajes de Datos

a) Realizar las pruebas de funcionalidad para la emisión de Constancias de Conservación de Mensajes de Datos

14 Administración de la Autoridad de Constancias de Conservación de mensajes de datos de SeguriData Privada

14.1 Administración de la Seguridad

La administración de la autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada debe proporcionar la información sobre la seguridad de la información, la cual se define en el documento Política de la Seguridad de la Información de la Constancias de Conservación de Mensajes de Datos de SeguriData Privada, conteniendo obligaciones, sanciones, amenazas, plan de respuesta de incidencias, política para el Sitio WEB, y el procedimiento para dar a conocer dichas Políticas.

14.2 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de mensajes de Datos. 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 Constancias de Conservación de mensajes de Datos, 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

14.2.1 Ubicación y Construcción

La ubicación de los servicios de la Infraestructura de la autoridad de Constancias de Conservación de mensajes de Datos 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 Constancias de Conservación de mensajes de Datos 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-SITES-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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada SA de CV.

14.2.2 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 de 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 de REDIT
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 inflamable, 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 de 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.

14.2.3 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 Constancias de Conservación de mensajes de Datos 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, 100, 1500, y 6000 litros, que aseguran la continuidad en el servicio.

14.2.4 Riesgos por Inundaciones

La ubicación donde se encuentran los servicios de la Infraestructura de la autoridad de Constancias de Conservación de mensajes de Datos proporciona protección contra las inundaciones, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITES-VERSION1.0.doc.

14.2.5 Prevención de Incendios y Protección

La ubicación donde se encuentran los servicios de la Infraestructura de la autoridad de Constancias de Conservación de mensajes de Datos proporciona protección contra incendios, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITES-VERSION1.0.doc.

14.3 Almacenamiento de Medios

Todos los medios de comunicación magnéticos que contienen la información de la Infraestructura de la autoridad de Constancias de Conservación de mensajes de Datos, incluyendo medios de comunicación de respaldos, son almacenados en gabinetes bajo llave bajo el resguardo de REDIT 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 Constancias de Conservación de mensajes de Datos protegiéndolos contra destrucción y falsificación de acuerdo a la Política de Seguridad de la Información.

14.4 Destrucción de Documentos

Los documentos en papel y aquellos medios que contengan elementos sensibles de la Infraestructura de la autoridad de Constancias de Conservación de mensajes de Datos o información comercialmente sensible o confidencial serán eliminados, solo en caso de que la autoridad de Constancias de Conservación de mensajes de Datos e 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.

14.5 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 Constancias de Conservación de mensajes de Datos, el software de reserva y datos relacionados con elementos críticos especificados en la Política de la Autoridad de Constancias de Conservación de Mensajes de Datos 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 n el documento: PSC-SEGURIDATA-POLITICASDESEGURIDAD-SITES-VERSION1.0.doc

14.6 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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada SA de CV, la Política de la autoridad de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de mensajes de Datos de SeguriData Privada SA de CV, 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.

14.7 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:

- **Oficiales de Seguridad**: Responsabilidad total de administrar las prácticas de seguridad.
- **Administradores del Sistema**: Autorizados para instalar, configurar y mantener sistemas.
- **Operadores del Sistema**: Responsables 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.** Encargado de gestionar la expedición de Constancias de Conservación de Mensajes de Datos de SeguriData Privada SA de CV, desde la contratación del servicio, hasta la expedición y entrega de los mismos.

- **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 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 Constancias de Conservación de mensajes de Datos

14.7.1 Número de Personas Requeridas por Tarea

El número de personas requeridas por tarea se da de acuerdo a:

Tarea	Personas requeridas
Contratación del servicio	Administrador
Generación de Llaves de la autoridad se Constancias de Conservación de Mensajes de Datos	Administrador de sistemas Oficial de seguridad – Profesional Informático
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 Profesional Informático

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 Constancias de Conservación de Mensajes de Datos, 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 Jurídico
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

14.7.2 Identificación y Autenticación para cada Función

Las personas que realizan las funciones relevantes están sometidas a una seguridad apropiada. Cada individuo que realiza cualquiera de las funciones relevantes usará un Certificado emitido por la Autoridad Certificadora de Constancias de Conservación de Mensajes de Datos, para identificarse en la Infraestructura de Constancias de Conservación de Mensajes de Datos

14.7.3 Funciones que Requieren Separación de Deberes

Las funciones que implican la administración de la Autoridad de Constancias de Conservación de Mensajes de Datos son separadas y asignadas a los roles comentados en los puntos 14.7 y 14.7.1

Todas las funciones que implican el mantenimiento de registros de auditoría son separadas y asignadas a los roles comentados en los puntos 15-4.7 y 14.7.1

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.

14.8 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 Constancias de Conservación de Mensajes de Datos.

14.8.1 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 firma electrónica, así como en procedimientos de seguridad para el personal y experiencia en seguridad de la información y prevención de riesgos.

14.8.2 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.

14.8.3 Requisitos de Personal Externo

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

14.8.4 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 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

15.1 Tipos de Eventos Registrados

Todos los actos relacionados con la expedición de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos en conjunto con la propia solicitud y acuerdo firmados por el cliente, los cuales se encuentran en un sitio seguro de manera física almacenados en gavetas bajo llave

15.1.1 Frecuencia de Registro

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

15.1.2 Período de Conservación de los Registros de Auditoria

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 las Constancias de Conservación de Mensajes de Datos.

Las transacciones serán almacenadas al menos 5 (cinco) años después de que la Autoridad de Constancias de Conservación de Mensajes de Datos cese sus operaciones.

15.1.3 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 Constancias de Conservación de Mensajes de Datos.

Solo los Oficiales de Seguridad de la Infraestructura de Constancias de Conservación de Mensajes de Datos 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 una un respaldo de la base de datos que contiene las transacciones descritas, el cual se efectúa diariamente.

15.1.4 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.

Se llevarán a cabo evaluaciones relativas al sistema de base, amenazas corrientes y riesgos de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de Constancias de Conservación de Mensajes de Datos, incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la

Infraestructura de Constancias de Conservación de Mensajes de Datos, así como determinar un índice de riesgo en base a la existencia de protecciones y prácticas de control.

SeguriData Privada S.A. de C.V. realizará una evaluación de 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, y de la información y asignará una clasificación a las exigencias de protección de tales activos, compatible con el análisis de riesgo.

Lo anterior, está definido en el documento de Análisis y Evaluación de manejo de riesgos para el Servicio de Constancias de Conservación de Mensajes de Datos.

15.1.5 Evaluaciones de Vulnerabilidad

Se llevarán a cabo evaluaciones relativas al sistema de base, amenazas corrientes y riesgos de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de Constancias de Conservación de Mensajes de Datos, incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la Infraestructura de Constancias de Conservación de Mensajes de Datos, 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.

15.1.6 Verificación de Autenticidad de la Constancia de Conservación de mensajes de datos.

Para verificar la autenticidad de la Constancia de sigue:

- Verificar la firma electrónica de la autoridad de constancias de conservación de mensajes de datos
- Verificar la firma electrónica del cliente que genero el expediente que forma parte de la constancia

- Recalcular el compendio de archivos parciales y verificar que coinciden con los compendios que forman parte del expediente.

16 Base de datos Utilizada

Se utiliza Microsoft SQL Server 2012 como base de datos para la autoridad de Constancias de Conservación de Mensajes de Datos, para el servidor de la NOM 151 SCFI 2016.

El acceso a las bases de datos se realiza mediante la autenticación de un usuario y password.

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. También se revisa el log de los productos API REST y servidor TSA, donde se pueden detectar accesos no permitidos.

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

- 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 KIO 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 site 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 uso de los productos de software definidos: Servidor TSA, API REST y Modulo de auditoria, y su relación con el manejador de base de datos SQL Server 2012.

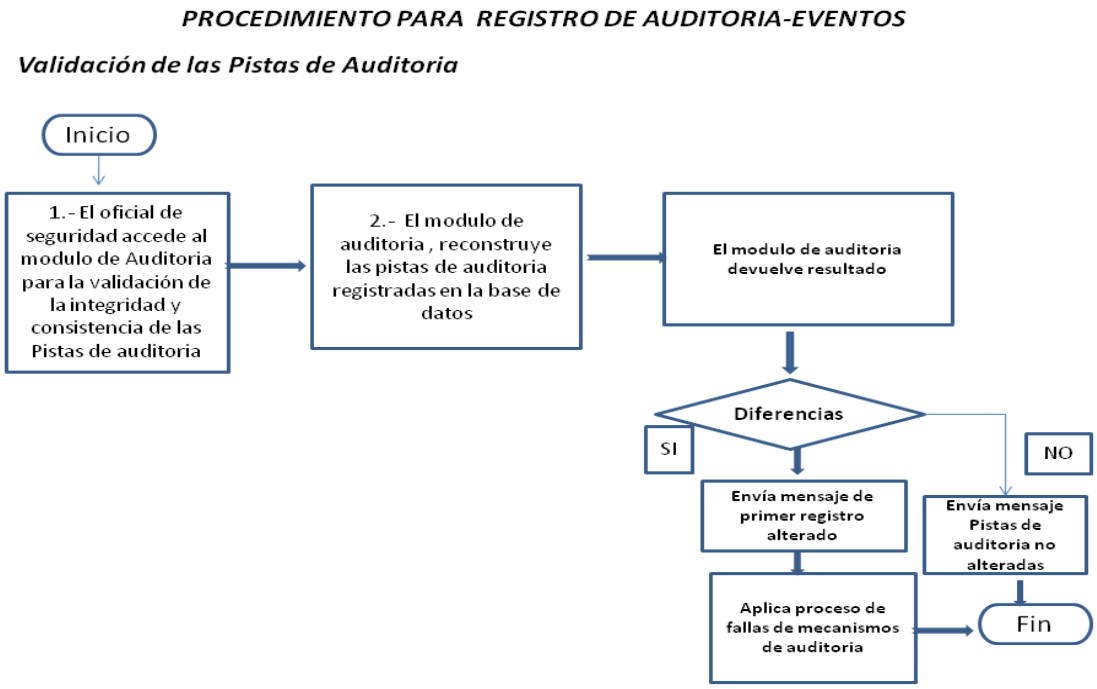
Para los productos (aplicaciones) API REST y Servidor TSA, se audita a través de los logs (Bitácoras de errores), que son archivos de texto, que en un futuro se tiene contemplado la Firma Electrónica Avanzada de los mismos, usando un certificado para este fin, el cual se emitirá desde la auto certificación, 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 los servidores donde residen los sistemas que operan las Constancias de Conservación de Mensajes de Datos, se realiza de manera automática, por lo que ante cualquier caída de los mismos, se asegura que al arrancar de nuevo estos procesos se activen de manera automática.

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

A continuación se muestra el procedimiento de registro 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 Constancias de Conservación de Mensajes de Datos sea registrada durante un

período de tiempo de al menos 5 años, en particular con el objetivo de disponer de pruebas, relativas a las Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos. 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 las Constancias de Conservación de Mensajes de Datos)
- La solicitud de la expedición de las Constancias de Conservación de Mensajes de Datos, contratos firmados por clientes (almacenados físicamente en un sitio seguro en gaveta cerrada con llave)
- Contenido de las Constancias de Conservación de Mensajes de Datos. (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 5 (cinco) años.

Los registros de Constancias de Conservación de Mensajes de Datos serán mantenidos por siempre para proporcionar las pruebas necesarias para sustentar la información, en caso se algún proceso legal.

17.3.1 Protección de Archivos

Los archivos serán conservados y protegidos contra la modificación o destrucción. Sólo los Oficiales de Seguridad de la Autoridad de Constancias de Conservación de Mensajes de Datos, pueden 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 Constancias de Conservación de Mensajes de Datos es registrada durante un período apropiado de tiempo, en particular con el objetivo de disponer de pruebas, relativas a las Constancias de Conservación de Mensajes de Datos, 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 hace diariamente y la replicación 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 la Infraestructura de Constancias de Conservación de Mensajes de Datos, incluyen la fecha y la hora en el que el acontecimiento ocurrió, el sello de tiempo digital es solicitado a la Autoridad de Sellos Digitales de Tiempo, proporcionado por el Servidor TSA que se encuentra sincronizado con una fuente confiable De tiempo 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 Constancias de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos. Tales proyectos incluyen procedimientos para:

- Notificación inmediata a todos los clientes del Servicio de expedición de Constancias de Conservación de Mensajes de Datos.

En caso de revelación de claves de la Autoridad de Constancias de Conservación de Mensajes de Datos, 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-CONSTANCIASDECONSERVACION.doc y en el PSC-SEGURIDATA-PLANCONTINUIDADNEGOCIOYRECUPERACIONANTEDESASTRES-CONSTANCIASCONSERVACION.doc

17.5 Procedimientos de Revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos

En caso de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos, el Certificado afectado será revocado, de acuerdo a los procesos señalados en el Plan de Continuidad del Negocio y Recuperación ante Desastres (PSC-SEGURIDATA PLANCONTINUIDADNEGOCIOYRECUPERACIONANTEDESASTRE-CONSTANCIASCONSERVACION.doc)

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 las Constancias de Conservación de Mensajes de Datos, que las operaciones serán restauradas cuanto antes.

El Plan de Continuidad del Negocio (o el Plan de Recuperación ante Desastres) tratará como un desastre la revelación o sospecha de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de constancias de conservación de mensajes de datos.

17.7 Terminación – Cese de la Autoridad de Constancias de Conservación de Mensajes de Datos

Las causas por las que puede ocurrir el cese de operaciones de la Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V., como Prestador de Servicios, es que se hayan comprometido los Datos de Creación de Firma electrónica avanzada de la autoridad de Constancias de Conservación de Mensajes de Datos, o por toma de decisión de cese de actividades por parte de SeguriData Privada S.A. de C.V.

Adicionalmente el cese de la autoridad de Constancias de Conservación de Mensajes de Datos puede darse por las causas marcadas en los artículos 24, 25, 26 y 27 del Reglamento del Código de Comercio en Materia de Prestadores de Servicio http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_CComer_MPSC.pdf

17.7.1 Suspensión Temporal

Este escenario se presenta cuando la Secretaria de Economía sancione a la autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada 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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada dejará de expedir Constancias de

Conservación de Mensajes de Datos 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 Suspensión Definitiva

Si fuera necesario liquidar el servicio de la Autoridad de Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos. La política al menos considera:

- Asegurar que cualquier interrupción causada por la terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos, es reducida al mínimo.
- Asegurar que los archivos de registro de la Autoridad de Constancias de Conservación de Mensajes de Datos, son conservados.
- Asegurar que la terminación se notifica puntualmente a los clientes, y otras partes relevantes en la Infraestructura de Constancias de Conservación de Mensajes de Datos
- 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 Constancias de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos y asegura el mantenimiento continuado de los registros necesarios para proporcionar pruebas de cara a un posible procedimiento judicial.

Antes de que la Autoridad de Constancias de Conservación de Mensajes de Datos, 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.
- Terminará toda la autorización de subcontratistas para actuar de parte de SeguriData Privada S.A. de C.V. en el funcionamiento de cualesquiera funciones relacionadas con el proceso de expedición de Constancias de Conservación de Mensajes de Datos.
- 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
- Destruirá o impedirá el uso de sus Datos de Creación de Firma Electrónica.

Se establece en la Declaración de prácticas de la autoridad de Constancias de Conservación de Mensajes de Datos y en la Política de la Autoridad de Constancias de Conservación de Mensajes de Datos las provisiones hechas para el cese del servicio. Esto incluirá:

- La notificación a las entidades afectadas.
- La transferencia de sus obligaciones a otras partes.

17.7.3 Clasificación y Administración de Activos

La autoridad de Conservación de Mensajes de Datos de SeguriData Privada mantiene un inventario de todos los activos consistentes con el análisis del riesgo.

18 Privacidad y Seguridad

Limitantes y Restricciones en el Uso de información

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada 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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada 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 Constancias de Conservación de Mensajes de Datos, salvo autorización expresa del propio Cliente o por requerimiento de autoridad competente.

La Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada 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.

Las Constancias de Conservación de Mensajes de Datos expedidos por la Autoridad de Constancias de conservación de mensajes de datos de SeguriData Privada S.A. de C.V., están sujetos únicamente a lo que la presente Política de la Autoridad de Constancias de Conservación de Mensajes de Datos y la Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. no asume ninguna responsabilidad cuando se encuentre ante cualquiera de estas circunstancias:

- Si las Constancias de Conservación de Mensajes de Datos 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 la constancia de conservación de mensajes de datos bajo el control del reclamante fuera emitido como consecuencia de cualquier falsedad o falsificación de los hechos proporcionados por el cliente para la expedición de las Constancias de Conservación de Mensajes de Datos.
- Si las Constancias de Conservación de Mensajes de Datos bajo el control del reclamante ha sido modificado o cambiado de cualquier modo o usado incumpliendo los términos de la Política de la Autoridad de Constancias de Conservación de Mensajes de Datos, de la Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos o del contrato con el cliente.
- Si las Constancias de Conservación de Mensajes de Datos 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 Constancia de Conservación de Mensajes de Datos 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

Constancias de Conservación de Mensajes de Datos 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; incluyendo obligaciones legales, sentencias de un tribunal competente al que la Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. sea, o pueda ser sujeta; y cualquier acontecimiento o circunstancia fuera del control de la Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V.

- Por el uso indebido de la información contenida en el Constancias de Conservación de Mensajes de Datos.

18.2 Responsabilidades Económicas

18.2.1 Indemnización por Parte de la Constancias de Conservación de Mensajes de Datos

Estipulado en la sección 20.9 de la Declaración de Prácticas de la Autoridad de Constancias de conservación de mensajes de datos.

18.2.2 Indemnización por Parte de los Clientes

Al grado permitido por la Declaración de Prácticas de Autoridad de Constancias de Conservación de Mensajes de Datos aplicables a la Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V., los clientes indemnizarán a la Autoridad de Constancias de Conservación de Mensajes de Datos de SeguriData Privada S.A. de C.V. por:

- Falsedad o mala representación de información proporcionada en la solicitud de Constancias de Conservación de Mensajes de Datos.

- Omisión de revelar un hecho destacado en la solicitud de Constancias de Conservación de Mensajes de Datos, si la omisión fue realizada negligentemente o con la intención de engañar a una persona o al Administrador.

- 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.