Documento

Política de Sellos Digitales de Tiempo

PSC Codex

Versión 1.0

3 de enero del 2022

Contenido

Objetivo

La transición que implementan las organizaciones en la transformación de procesos en medios físico a medios digitales o electrónicos requiere de la creación de evidencia confiable y manejable que permita a los involucrados verificar los mensajes de datos con posterioridad a la emisión de estos. Para ello, es necesario contar con mecanismos que permitan asociar los datos de una transacción y el momento en que fue ejecutada con el contenido del mensaje de datos para contar con medios que permitan asegurar que una transacción o mensaje fue emitido dentro del espacio temporal acordado.

En ese sentido, los Prestadores de Servicios de Certificación acreditados por la Secretaría de Economía tienen la facultad de emitir Sellos Digitales de Tiempo que, a través de medios y evidencia criptográfica, permiten establecer la relación de un mensaje de datos con el momento en el que el mismo dice haber sido emitido. Un ejemplo típico de la implementación de un Sello Digital de Tiempo se presenta con la firma electrónica de documentos, donde el sello digital se utiliza para probar que el certificado digital del firmante se encontraba vigente y activo en el momento en que se llevó a cabo la firma del documento.

El uso y aplicación de los Sellos Digitales de Tiempo dentro de las transacciones comerciales esta definido en el Código de Comercio, el cual establece los requisitos que deben de seguir las transacciones electrónicas a fin de ser consideradas plenamente válidas.

Ahora bien, el contenido de la presente Política de Emisión de Sellos Digitales de Tiempo de PSC Codex como Prestador de Servicios de Certificación se basa en la implementación de infraestructura criptográfica de clave pública, así como en el uso de fuentes de tiempo confiables como el Centro Nacional de Metrología y debe considerarse como un documento informativo respecto del uso y aprovechamiento de la Autoridad de Sellado Digital de Tiempo.

Fuentes

- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Glosario de Términos

Concepto	Descripción
ASDT	Autoridad de Sellado Digital de Tiempo
Autoridad Certificadora (AC)	A las dependencias y entidades de la Administración Pública Federal y los Prestadores de Servicios de Certificación que, conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos. *Art. 2 Fr. I Reglas*
ETSI TS	Instituto Europeo de Normas de Telecomunicaciones European Telecommunications Standards Institute Technical Specification es una organización de normalización independiente, sin fines de lucro de la industria de las telecomunicaciones. European Telecommunications Standards Institute Technical Specification. *Art. 2 fr. VI Reglas*
FIPS	Norma Federal para el procesamiento de información (Federal Information Processing Standard). Estándar de seguridad, desarrollado por el grupo de trabajo del gobierno norteamericano y la industria para validar la calidad de módulos criptográficos.
HSM	Módulo Criptográfico de Seguridad (HSM por sus siglas en inglés)
NIST	Instituto Nacional de Estándares y Tecnología – National Institute of Standards and Technology; *Art. 2 Fr. X Reglas*
Prestadores de Servicios de Certificación (PSC)	La persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.

Framework de referencia

PSC Codex ha desarrollado la presente Política de Emisión de Sellos Digitales de Tiempo de la Autoridad de Sellado Digital de Tiempo tomando como referencia los conceptos, rubros y características que se mencionan dentro de las especificaciones técnicas del estándar RFC 3628 que tiene como título "*Policy Requirements for Time-Stamping Authorities (TSAs)*". Este documento tiene como finalidad establecer el estándar mínimo que deben de cumplir las organizaciones en la emisión de las Políticas de los servicios relativos a la emisión de sellos de tiempo, lo anterior con la finalidad de que los suscriptores y partes interesadas tengan pleno conocimiento respecto de la forma en que será prestado el servicio, así como de la delimitación de obligaciones y responsabilidades específicas para cada una de las partes.

Siguiendo este estándar PSC Codex, como Prestador de Servicios de Certificación, dentro del presente documento establecerá la información requerida para los siguientes apartados:

1. Servicios de la Autoridad de Sellado Digital de Tiempo.
2. Aplicabilidad de la Política definida en el presente documento.
3. Identificador de la Política de Emisión de Sellos Digitales de Tiempo.
4. Obligaciones y responsabilidades.

Conforme lo señalan las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, a lo largo del presente documento se desarrollarán cada uno de estos apartados, así como aquellos que no fueron mencionados en el listado y que son mencionados dentro del RFC 3628.

Conceptos Generales

Sello Digital de Tiempo

El Código de Comercio define al Sellos Digital de Tiempo como “El registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello…” el cual sigue los estándares tecnológicos que señala el RFC3161.

Servicio de emisión de Sellos Digitales de Tiempo

El servicio de emisión de Sellos Digitales de Tiempo es el servicio que ofrece PSC Codex a sus suscriptores y partes interesadas como Prestador de Servicios de Certificación acreditado por la Secretaría de Economía. Dicho servicio entrega los sellos que son generados por la Autoridad de Sellado Digital de Tiempo de PSC Codex y que sigue los lineamientos y requisitos que se establecen en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

El servicio se provee a través de las API’s que PSC Codex pone a disposición de sus suscriptores y partes interesadas.

Autoridad de Sellado Digital de Tiempo

PSC Codex define su Autoridad de Sellado Digital de Tiempo como aquella Autoridad subordinada a la Autoridad Certificadora de la Secretaría de Economía a la cual se le ha emitido un certificado digital con el propósito de emitir Sellos Digitales de Tiempo.

La Autoridad de Sellado Digital de Tiempo obtiene la escala de tiempo, con la cual emite sellos digitales de tiempo, del Centro Nacional de Metrología conforme lo establece la Regla 123 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Suscriptores

PSC Codex define a sus suscriptores como todas aquellas personas físicas o morales que requieren consumir el servicio de Sellos Digitales de Tiempo para integrarlos dentro de sus procesos organizacionales. Los interesados en el servicio se convierten en suscriptores cuando se formaliza a través de un contrato contractual la relación entre PSC Codex y el interesado quien, al momento de la firma, adquiere las obligaciones, responsabilidades y derechos derivados de la emisión del Sellos Digital de Tiempo.

Las personas físicas interesadas en ser suscriptores del servicio deberán cumplir con los requisitos y documentación siguientes:

Tratándose de personas físicas nacidas en territorio mexicano:

1. Ser mayor de edad

2. Acta de nacimiento, la cual se validará a través del portal https://cevar.registrocivil.gob.mx/eVAR/
3. Identificación oficial vigente (INE, Pasaporte, Cédula profesional).
    a. La credencial del INE deberá estar vigente, lo cual se acreditará mediante el portal: https://listanominal.ine.mx/scpln/
    b. Se verificará que la cédula profesional se encuentre registrada en el Registro Nacional de Profesionistas mediante el portal: https://www.cedulaprofesional.sep.gob.mx/cedula/presidencia/indexAvanzada.action
    c. El pasaporte deberá encontrarse vigente.
4. Clave Única de Registro de Población (CURP), la cual será verificada a través del portal: https://www.gob.mx/curp/
5. Registro Federal de Contribuyentes (RFC), el cual será validado a través del portal: https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf
6. Comprobante domicilio no mayor a 3 meses
7. Constancia de opinión de cumplimiento de obligaciones fiscales (Art. 32 CFF)
8. Constancia de situación fiscal.
9. Formato KYC firmado.
10. Formato de obligaciones y responsabilidades firmado.

Tratándose de personas físicas nacidas en el extranjero:

1. Pasaporte emitido por el país de origen, el cual deberá encontrarse vigente.
2. Documento oficial expedido por el Instituto Nacional de Migración (Cuando cuente con él, que acredite su internación o legal estancia en el país) FM2 o FM3
3. Comprobante de domicilio no mayor a 3 meses
4. RFC, el cual será validado a través del portal: https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf
5. Formato KYC firmado.
6. Formato de obligaciones y responsabilidades firmado.

Las personas morales interesadas en ser suscriptores del servicio deberán cumplir con los requisitos y documentación siguientes:

- Tratándose de personas morales constituidas en territorio nacional:
    1. Acta constitutiva.
    2. Reformas a la escritura constitutiva.
    3. Poder notarial de apoderado legal.
    4. Validación de la constitución y apoderado de la sociedad a través del portal SIGER. https://rpc.economia.gob.mx/siger2/xhtml/login/login2.xhtml
    5. RFC apoderado legal, el cual se validará a través del portal: https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf
    6. Comprobante domicilio apoderado legal no mayor a 3 meses
    7. RFC de la persona moral, el cual se validará a través del portal: https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf
    8. Comprobante domicilio de la persona moral no mayor a 3 meses.

9. Constancia de opinión de cumplimiento de obligaciones fiscales (Art. 32 CFF).
10. Constancia de situación fiscal.
11. Formato KYC firmado.

- Tratándose de personas morales constituidas en el extranjero:
    1. Documento que compruebe su constitución de acuerdo con las leyes de su país.
    2. Comprobante de domicilio no mayor a 3 meses
    3. Testimonio o copia certificada del instrumento que contenga los poderes del representante o representantes legales, expedido por fedatario público.
    4. Inscripción en el Registro Público de Comercio.
    5. Formato KYC firmado

Política de Sellos Digitales de Tiempo

Identificación

La Política de Sellos Digitales de Tiempo de PSC Codex puede ser identificada a través del OID que asigna la Secretaría de Economía cuando se concluye satisfactoriamente con el proceso de acreditación como Prestador de Servicios de Certificación para el servicio de emisión de Sellos Digitales de Tiempo.

El identificador asignado por la Secretaría a la Política de Sellos Digitales de Tiempo de PSC Codex está estructurado conforme al estándar X.208 descrito en el RFC 3628 y que entre otras cuestiones permite identificar a la organización acreditada, la organización que emite la acreditación, la versión de la política, así como el servicio para el cual se emite dicha política. El OID asignado a PSC Codex para su Política de Sellos, será incluido en la Autoridad de Sellado Digital de Tiempo y, por ende, en cada uno de los sellos digitales que emita dicha autoridad.

OID de la Política de SDT de PSC Codex: [Pendiente de asignación por parte de la Secretaría de Economía].

Inicio de operaciones

Con fecha de [Pendiente de dictamen de la SE] la Secretaría de Economía resolvió otorgar la acreditación como Prestador de Servicios de Certificación a PSC Codex para el servicio de emisión de Sellos Digitales de Tiempo, publicando en el Diario Oficial de la Federación la acreditación correspondiente.

Publicada la acreditación, PSC Codex inicio operaciones del servicio de emisión de Sellos Digitales de Tiempo con fecha [Pendiente de dictamen de la SE].

Usuarios y aplicabilidad

La presente Política de Sellos Digitales de Tiempo cumple con los requerimientos que se establecen en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación con relación a la estructura y contenido que deben de considerarse durante la emisión del *token* del Sello Digital de Tiempo por la Autoridad correspondiente y atendiendo a la definición y alcance que se establece para los sellos digitales dentro del Código de Comercio.

Tecnológicamente esta Política establece los lineamientos a través de los cuales se da cumplimiento a los requerimientos para el uso de sellos digitales de tiempo en firmas electrónicas avanzadas conforme a la Directiva Europea de Firma Electrónica, definidas en el ETSI TS 101 733 vigente.

Esta política será aplicable a la comunidad de usuarios del servicio de sellos digitales de tiempo que proporciona PSC Codex, entendiendo como comunidad de usuarios a los suscriptores del servicio, así como a las partes interesadas en el mismo. La Política de Sellos Digitales de Tiempo es considerada como un documento de acceso público por parte de PSC Codex por lo que será consultable en la dirección https://www.psccodex.com/politicas/sellosdetiempo/.

Conformidad

PSC Codex declara que conforme lo establece el RFC 3628 su Autoridad de Sellado Digital de Tiempo incluye dentro de los *tokens* de sello de tiempo el OID que le ha sido asignado por la Secretaría de Economía, una vez que le ha sido otorgada la acreditación como PSC para el servicio de emisión de Sellos Digitales de Tiempo.

El OID que se incluye en los sellos digitales de tiempo es: [Pendiente de asignación por la SE]

PSC Codex hará del conocimiento de los suscriptores y partes interesadas en el servicio de emisión de Sellos Digitales de Tiempo del OID asignado por la Secretaría dentro de su portal de internet y será consultable en la dirección [URL donde se publicará el OID], además de que el mismo se incluye dentro de la Política de Emisión de Sellos Digitales de Tiempo y en la Declaración de Prácticas de la Autoridad de Sellado Digital de Tiempo.

Obligaciones y responsabilidades

Los participantes de la emisión de sellos digitales de tiempo, tanto PSC como Prestador de Servicios de Certificación, como los suscriptores, sujetos relacionados y partes interesadas conocen, aceptan y asumen las obligaciones y responsabilidades que se generan como parte del servicio. Cada uno de los participantes mencionados deberá cumplir con las obligaciones que se establecen en el presente documento y que forman parte del documento de términos y condiciones del servicio.

La inobservancia u omisión de obligaciones y responsabilidades, así como el mal uso de los sellos digitales de tiempo pueden derivar en la suspensión del servicio y, en su caso, en las acciones legales que PSC Codex pudiera considerar pertinentes.

Obligaciones de la ASDT de PSC Codex

Obligaciones generales

PSC Codex como Prestador de Servicios de Certificación acreditado por la Secretaría de Economía tiene la obligación de cumplir con los criterios y requerimientos que se establecen en la normatividad aplicable a fin de brindar servicios de certificación confiables y que en todo momento privilegien las tres principales características de la seguridad de la información como son la integridad, confidencialidad y disponibilidad.

Entre las principales obligaciones que PSC Codex cumple, se encuentran las siguientes:

a) Contar con un seguro de responsabilidad civil para cada año y durante el tiempo que permanezca acreditado como Prestador de Servicios de Certificación.
b) Contar con una fianza para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.
c) Contar con el espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección y políticas necesarias para garantizar la seguridad para la emisión de Sellos Digitales de Tiempo.
d) Contar con una oficina administrativa sujeta a los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.
e) Contar con dos centros de datos, uno principal y otro alterno, que deberán cumplir con las certificaciones y estándares de calidad y seguridad, así como contar con procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.
f) Contar con los elementos humanos, económicos, materiales y tecnológicos requeridos en el Título Sexto de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de certificación.

Obligaciones de la ASDT con sus suscriptores

Además de las obligaciones que tiene PSC Codex inherentes a su actuar como Prestador de Servicios de Certificación, la organización con la finalidad de brindar un servicio de confianza y calidad para sus suscriptores ha establecido una serie de obligaciones para su servicio de emisión de sellos digitales de tiempo.

Estas obligaciones están directamente relacionadas con sus suscriptores y los compromisos que tiene PSC Codex con ellos.

a) Establecer los mecanismos necesarios para que los suscriptores puedan realizar la solicitud de sellos digitales de tiempo a través de los procedimientos proporcionados en el momento de la contratación.

b) Contar con un sitio electrónico de alta disponibilidad en el cual los usuarios puedan consultar la clave pública de los certificados que les han sido emitidos.
c) Implementar procesos de verificación de algoritmos criptográficos para garantizar que los sellos digitales de tiempo se emiten conforme a las disposiciones de la Secretaría de Economía.
d) Garantizar la confidencialidad de la información de los sellos digitales de tiempo al requerir para su emisión únicamente el hash o huella digital del mensaje de datos.
e) Establecer los mecanismos y procedimientos de seguridad de la información que permitan que los Sellos Digitales de Tiempo emitidos por PSC Codex sean considerados como confiables.
f) Notificar a los suscriptores y partes interesadas en el servicio de emisión de certificados digitales los procesos a seguir en caso de presentarse o presumirse la vulneración de los datos de creación de firma de la Autoridad de Sellado Digital de Tiempo de PSC Codex.

Responsabilidades de la ASDT

Adicionalmente a las obligaciones que enuncia PSC Codex como Prestador de Servicios de Certificación acreditado para la emisión de sellos digitales de tiempo, a continuación, se dan a conocer las responsabilidades de la organización con respecto a la prestación del servicio:

a) Para la recolección y manejo de datos personales, PSC Codex implementará procedimientos que privilegien la seguridad de la información teniendo como enfoque principal la confidencialidad de la información.
b) Poner a disposición de los suscriptores y partes interesadas la llave pública del certificado de su Autoridad de Sellado Digital de Tiempo.

Obligaciones de los suscriptores

Con la finalidad de mantener un esquema de confiabilidad en el servicio de emisión de sellos digitales de tiempo por parte de la ASDT de PSC Codex, es necesario que los suscriptores observen conductas que no pongan en riesgo la confianza que las partes interesadas depositan en la ASDT de PSC Codex como parte de sus transacciones.

En ese sentido, los suscriptores y sujetos relacionados del servicio de emisión de sellos digitales de tiempo de PSC Codex tendrán las obligaciones siguientes:

- Generar el hash del documento respecto del cual requiere la emisión de un sello digital de tiempo conforme al algoritmo criptográfico dado a conocer por PSC Codex.
- Verificar que el Sello Digital de Tiempo emitido corresponde con el hash con el cual se realizó la solicitud de emisión.
- Conocer y aceptar contenido de la Política de Sellos Digitales de Tiempo y de la Declaración de Prácticas de Sellos Digitales de Tiempo.
- Gestionar adecuadamente las credenciales que se le asignan para el consumo del servicio.

Obligaciones de las partes que confían

Las partes que confían en el servicio de emisión de sellos digitales de tiempo por parte de la ASDT de PSC Codex tienen la obligación de conocer los términos y condiciones del servicio prestado, donde se establecen los preceptos generales del servicio y su funcionamiento.

Además, en aquellas acciones o transacciones que requieran del uso de los sellos digitales de tiempo emitidos por PSC Codex deberán ejecutar las siguientes acciones:

- Verificar la cadena de certificación presente en el sello digital de tiempo.
- Verificar que el sello digital de tiempo este correctamente firmado por la ASDT de PSC Codex.
- Verificar que el sello digital de tiempo corresponde al hash respecto del cual se realizó la solicitud.
- Considerar las limitaciones que se establecen para el uso de los sellos digitales de tiempo emitidos por PSC Codex.

Requerimientos de las Prácticas de la ASDT

Los requerimientos respecto de las prácticas de la ASDT de PSC Codex establecen los objetivos, controles y procesos relevantes que permitan incrementar el nivel de la seguridad de la información en los componentes y servicios de infraestructura directamente relacionados con la emisión de Sellos Digitales de Tiempo.

La implementación de la Autoridad de Sellado Digital de Tiempo conlleva el desarrollo y ejecución de diversos controles y mecanismos de seguridad para la emisión de un sello digital de tiempo. En ese sentido, la emisión de un *token* de sello digital de tiempo en respuesta a una solicitud queda a discreción de PSC Codex en atención al cumplimiento de los procesos de seguridad en coordinación con los suscriptores, así como los niveles de servicio acordados.

Ciclo de vida del módulo criptográfico

Los servicios de certificación tienen como uno de sus principales activos críticos al módulo criptográfico esto ya que, como se ha venido señalando, es el dispositivo que resguarda el certificado emitido por la Secretaría de Economía a PSC Codex como Prestador de Servicios de Certificación para el servicio de emisión de Sellos Digitales de Tiempo, es decir, es el centro y origen de la confianza del servicio.

En ese sentido, PSC Codex ha establecido una serie de medidas y controles que permiten garantizar la seguridad de sus módulos criptográficos y, por ende, de sus Datos de Creación de Firma Electrónica Avanzada.

El detalle del ciclo de vida de los módulos criptográficos de la Autoridad de Sellado Digital de Tiempo de PSC Codex puede consultarse en el documento denominado "*Plan de Administración de Claves de la ASDT*".

Ciclo de vida de las claves criptográficas

Se denomina ciclo de vida de las llaves criptográficas de la ASDT de PSC Codex al periodo de tiempo en el cual los datos de creación de firma permanecen vigentes y activos conforme a los criterios que establece la Autoridad Certificadora que los emite que, en el caso de PSC Codex, son emitidas por la Autoridad Certificadora de la Secretaría de Economía. Dichas llaves son válidas para la emisión de Sellos Digitales de Tiempo desde el momento en que son emitidas y hasta el fin de su vigencia o en el momento que sean revocadas al presentarse alguno de los supuestos definidos en el apartado de fin del ciclo de vida de las llaves de la ASDT.

El ciclo de vida de las llaves criptográficas incluye el manejo de todos aquellos procedimientos y etapas necesarias para el correcto resguardo, uso y aprovechamiento de dichas llaves. Por ello, se establecen procedimientos de almacenamiento que permitan garantizar que los datos de creación de firma se mantienen seguros mediante el uso de módulos criptográficos.

El ciclo de vida de las claves también atiende a los requerimientos normativos respecto de los atributos que debe de incluir, así como las medidas criptográficas de seguridad que se deben implementar, tales como el algoritmo criptográfico a utilizar (SHA-256) y la longitud de firma (4096 bits) características que son establecidas y publicadas por la Secretaría de Economía. El ciclo de vida también contempla la distribución de la llave pública del certificado de la ASDT el cual es consultable en el portal de internet de PSC Codex, en la dirección https://www.psccodex.com/certificado/sellosdetiempo/.

Compromiso de la ASDT

PSC Codex como Autoridad de Sellado Digital de Tiempo acreditada por la Secretaría de Economía para la emisión de Sellos Digitales de Tiempo esta comprometido con sus suscriptores y partes interesadas a poner a su disposición la información relevante relacionada, entre otros escenarios, con el compromiso o vulneración de los datos de creación de firma electrónica o de la pérdida de sincronía con la fuente de tiempo confiable.

Para ello, dentro del Plan de Continuidad de Negocio y Recuperación ante Desastres ha establecido los procedimientos que se deberán seguir al interior de la organización en caso de que sus llaves criptográficas se vean comprometidas, así como las comunicaciones y acciones que debe de detonar con sus suscriptores y partes interesadas, incluyendo la Secretaría de Economía. Además, también establece las acciones que deberá seguir ante la pérdida de sincronía con la fuente de tiempo confiable y los procesos de notificación que deberá ejecutar.

PSC Codex define que las llaves criptográficas de su ASDT se encuentran comprometidas cuando existe evidencia o indicios suficientes que indiquen que un tercero ha obtenido los datos de creación de firma de PSC Codex. En ese sentido,

PSC Codex notificará a suscriptores y partes interesadas una descripción general del compromiso identificado.

De confirmarse que la llave privada de los datos de creación de firma de la ASDT fue comprometida, PSC Codex realizará una auditoría en conjunto con suscriptores y partes interesadas para identificar los *tokens* de sellos de tiempo legítimos de aquellos que fueron emitidos indebidamente como consecuencia del compromiso de la llave privada.

Objetivos de seguridad de la información

PSC Codex como parte de la implementación del SGSI y de su Política de Seguridad de la Información ha establecido diversos objetivos para la seguridad de la información de sus servicios los cuales están orientados a garantizar a los suscriptores y partes interesadas que los servicios que proporciona PSC Codex son confiables y brindan certeza en el manejo de la información y los datos generados. Ahora bien, PSC Codex ha definido una serie de objetivos generales aplicables a la organización y sus sistemas, además de objetivos de seguridad específicos para el servicio de emisión de sellos digitales de tiempo que se tiene acreditado como PSC.

Los objetivos de seguridad de la información para el servicio de emisión de sellos digitales de tiempo de PSC Codex son los siguientes:

1. Mantener la Política de Seguridad de la Información de PSC Codex actualizada conforme a los riesgos y retos que representan los avances tecnológicos para asegurar su eficacia.
2. Generar lineamientos para la administración de la información generada por PSC Codex conforme a su nivel de criticidad asegurando el cumplimiento de las principales características de la seguridad de la información como son: integridad, disponibilidad, confidencialidad y no repudio.
3. Garantizar que los servicios que ofrece PSC Codex como Prestador de Servicios de Certificación se mantienen accesibles y disponibles para suscriptores y partes interesadas.
4. Gestionar la información que se recibe y genera como parte de los servicios que se tienen acreditados asegurando en todo momento la confidencialidad de la información.
5. Establecer procesos y mecanismos de verificación para garantizar que la información que se genera como resultado de los servicios se mantiene integra e inalterable en todas las fases de los servicios.
6. Implementar mecanismos de seguridad y autenticidad que permitan asegurar que los servicios acreditados como PSC únicamente se brindan a los suscriptores y partes interesadas que cumplan con los requerimientos que se establecen en las Políticas y Declaración de Prácticas de cada servicio.
7. Definir perímetros de control de acceso a las áreas seguras tanto de los centros de datos como de las oficinas administrativas para resguardar la información de los servicios que PSC Codex considera como información crítica.

8. Asegurar la protección de la infraestructura crítica, definida en el Análisis y Evaluación de Riesgos y Amenazas implementando correctamente los protocolos de seguridad que establecen los centros de datos contratados.
9. Configurar las redes internas de la infraestructura de los servicios de PSC Codex como PSC para que la comunicación se permita únicamente entre los equipos que componen la infraestructura.
10. Evitar la fuga de información generada como parte de los servicios de PSC Codex a partir de la concientización organizacional respecto de la importancia de cada uno de los colaboradores en la consecución de los objetivos.
11. Asegurar la sincronía permanente y la transferencia de la unidad de tiempo con el Centro Nacional de Metrología.
12. Mantener la precisión en la emisión de sellos digitales de tiempo en un segundo o mejor conforme lo establece el RFC 3161.
13. Emitir sellos digitales de tiempo únicamente a los suscriptores que hayan completado el proceso de contratación con PSC Codex.
14. Monitorear permanentemente el servicio de emisión de sellos digitales de tiempo para garantizar que se cuenta con la capacidad tecnológica necesaria para brindar comercialmente el servicio.

Sello Digital de Tiempo

Procedimiento para la emisión de un sello digital de tiempo

El servicio de sellado digital de tiempo se pondrá disposición de los suscriptores de PSC Codex a través de un servicio web el cual tendrá una interfaz pública a través de la cual dichos suscriptores podrán solicitar el sello digital de tiempo para sus mensajes de datos y una vez que PSC Codex recibe y procesa dicha solicitud por esa misma interfaz procederá a entregar el token del sello digital de tiempo.

El servicio web que implementa PSC Codex para su servicio de Sellos Digitales de Tiempo implementa tecnología RESTFUL donde las peticiones se realizan a través de un método POST, además de utilizar JSON Web Tokens como medida de autenticación/seguridad adicional. Es importante mencionar que los suscriptores interesados en consumir el servicio de sellos digitales de tiempo deberán desarrollar el cliente a través del cual realizarán el consumo del servicio conforme a la documentación técnica que entrega PSC Codex.

En los siguientes apartados se describen las actividades del procedimiento para la emisión de un sello digital de tiempo.

Contratación del servicio de emisión de sellos digitales de tiempo

El proceso de contratación del servicio para la emisión de sellos digitales de tiempo por parte de la Autoridad de Sellado Digital de Tiempo de PSC Codex se realiza en dos etapas: la primera de ellas requiere que el usuario ingrese a la página de internet de PSC Codex y llene el formulario de cotización de servicio con los datos solicitados para que un ejecutivo de cuenta se ponga en contacto con el.

Una vez que el ejecutivo de PSC Codex cuenta con la información requerida se pondrá en contacto con el usuario para tener mayor detalle del requerimiento de servicio y solicitará la información correspondiente a la persona física o moral que realiza la solicitud, tras lo cual se generará la cotización correspondiente con base en los requerimientos y características solicitadas del servicio.

Una vez que el usuario cuenta con la cotización correspondiente, si le parece pertinente, deberá firmar dicho documento, además de los términos y condiciones correspondientes al servicio de emisión de sellos digitales de tiempo.

Registro de usuario en la plataforma

Los interesados o suscriptores del servicio de emisión de sellos digitales de tiempo como parte inicial para la emisión del servicio de sellos digitales de tiempo deberán registrarse en la página de internet https://app.psccodex.com/register donde deberán asignar los datos generales del usuario o empresa para que PSC Codex una vez establecidas las condiciones contractuales correspondientes pueda activar el servicio y créditos asociados al usuario. Como parte del registro el usuario deberá de ingresar el nombre, nombre de usuario, correo electrónico y contraseña con lo cual podrán registrar y gestionar los movimientos correspondientes a su consumo de sellos digitales de tiempo.

Asignación de inventarios y generación de token

Una vez que el usuario culmina con el registro y activación de su cuenta de usuario, el personal administrativo de PSC Codex procederá a actualizar el inventario de sellos digitales de tiempo conforme se haya convenido en términos contractuales y asignará dentro de la plataforma el número de sellos que podrá disponer el usuario, así como su tiempo de vigencia. Una vez que se asigna el inventario correspondiente a los sellos digitales de tiempo, el administrador de PSC Codex generará el JWT o token de autenticación para el servicio mismo que deberá ser utilizado conforme se señala en la documentación del servicio que se entrega al suscriptor.

Entrega de token de acceso

Una vez que el administrador comercial del servicio de PSC Codex genera el token de autenticación del usuario, procederá a la entrega de este a través del correo electrónico proporcionado por el representante legal de la sociedad o interesado en el servicio proporciona durante el proceso de contratación.

El uso, manejo y resguardo del token de autenticación es responsabilidad única y exclusivamente del interesado, conforme a los términos y condiciones del servicio, quien será responsable de notificar a PSC Codex en caso de mal uso o pérdida de confianza dicho token de autenticación, así como de solicitar la revocación y emisión de un nuevo token.

Mecanismos de seguridad del proceso (JSON Web Tokens)

El servicio de emisión de Sellos Digitales de Tiempo cuenta con mecanismos de autenticación para la solicitud y respuesta que permite garantizar que únicamente se emitan tokens de sello digital de tiempo a los suscriptores del servicio de PSC Codex.

PSC Codex, implementa la autenticación para su servicio de sellos digitales de tiempo a través de la tecnología conocida como JWT que se especifica dentro del documento del estándar RFC 7519 donde se define este mecanismo que es un medio de autenticación que permite propagar o compartir, de forma segura, información con una serie de privilegios relacionados con la lectura del servicio. Estos privilegios se codifican en objetos JSON que se incrustan en el cuerpo del mensaje de respuesta y que van firmados digitalmente.

El token JWT se conforma por una cadena de texto dividida en tres partes, las cuales se encuentran codificadas en Base64, donde cada una de las partes se encuentra separada por un punto, cada una de las cuales al decodificarse nos permite obtener la siguiente información:

- Header. Indica el algoritmo y tipo de token que se está utilizando. PSC Codex atendiendo a los algoritmos autorizados por la Secretaría de Economía, utiliza el SHA-256.
- Payload. Contiene los datos del usuario y privilegios, así como información adicional que pueda requerirse.
- Signature. Es la firma del JWT que nos permite validar que la comunicación no se ha visto alterada y que el JWT se mantiene válido.

Imagen 1 Autenticación por JWT

Entrega de documentación

Vía correo electrónico se proporcionará a los suscriptores la documentación del servicio de emisión de sellos digitales de tiempo para que puedan realizar el desarrollo de sus sistemas cliente a través del cual realizarán la solicitud de token de sello digital de tiempo.

La documentación generada por PSC Codex es auto explicativa y permitirá que los equipos tecnológicos de los suscriptores generen el cliente del servicio conforme a las especificaciones señaladas.

Desarrollo del sistema cliente

Como se ha mencionado, PSC Codex pone a disposición de sus suscriptores las interfaces a través de las cuales los suscriptores podrán realizar la solicitud de sellos digitales de tiempo. Ahora bien, considerando que los suscriptores pueden tener implementadas soluciones de diferentes características y desarrolladas con distintas tecnologías, PSC Codex requiere que los suscriptores realicen el desarrolle de sus propias plataformas cliente las cuales se adecuen a sus procesos de negocio y sistemas para lograr una mejor integración del servicio de emisión de sellos digitales de tiempo.

El desarrollo de los sistemas cliente deberá realizarse de conformidad con la documentación que PSC Codex entrega donde establece los métodos, variables y endpoints a considerar para el consumo del servicio. PSC Codex, además, durante la fase de desarrollo y como parte del proceso de implementación pone a disposición de los suscriptores al equipo de soporte técnico con la intención de que el desarrollo e implementación de servicios se lleve a cabo de una forma más eficiente y sencilla.

Solicitud del Sello Digital de Tiempo

Petición del Sello Digital de Tiempo

PSC Codex brindará a sus suscriptores el servicio de emisión de Sellos Digitales de Tiempo a través de un servicio web mediante el cual el interesado hará llegar a PSC Codex el hash o huella digital del mensaje de datos respecto del cual se requiera la emisión del Sello Digital de Tiempo, el cual debe emitirse utilizando el algoritmo criptográfico SHA-256 conforme lo publica la Secretaría de Economía en el sitio electrónico relativo a los Prestadores de Servicios de Certificación http://www.firmadigital.gob.mx/marco_juridico.html.

El servicio web a través del cual se expone el servicio utiliza la tecnología RESTFUL con método POST para realizar la solicitud del sello digital de tiempo teniendo como mecanismo de autenticación el conocido como “Bearer token” que es proporcionado por PSC Codex según se describe en el apartado de Entrega de token de acceso.

El servicio cuenta con un solo parámetro de solicitud descrito con la variable tsa_hash que espera como valor de entrada el hash o huella digital del mensaje de datos sobre el cual se requiere la emisión del sello digital de tiempo, el cual debe de ser generado utilizando el algoritmo criptográfico SHA-256.

Emisión del token del sello digital de tiempo

Una vez que PSC Codex recibe la solicitud de sello digital de tiempo por parte del suscriptor el servicio de PSC Codex integra el hash o huella digital enviado conforme al estándar RFC 3161 integrando el OID asignado por la Secretaría de Economía y genera un archivo .tsq que es enviado a la Autoridad de Sellado Digital de Tiempo para la emisión del sello solicitado.

Como parte del proceso de emisión de sellos digitales de tiempo PSC Codex se asegura que se cumplan las siguientes condiciones:

1. El token del sello digital de tiempo incluye el identificador de las Políticas de Sellos Digitales de Tiempo asignado por la Secretaría de Economía.
2. Cada uno de los sellos de tiempo emitidos por PSC Codex tiene asignado un identificador único.
3. La escala de tiempo que se incluye dentro del token proviene de una fuente confiable, en este caso el Centro Nacional de Metrología.
4. El tiempo que se incluye dentro del token esta sincronizado con el tiempo UTC y tiene una precisión de un segundo o mejor.
5. Si la Autoridad de Sellado Digital de Tiempo pierde sincronía con la fuente de tiempo confiable no se emitirán sellos digitales de tiempo.
6. El sello digital de tiempo se emite con los datos de creación de firma de uso específico que la Secretaría de Economía proporciona a PSC Codex.

Contenido del token del Sello Digital de Tiempo

PSC Codex es responsable de asegurar que los sellos digitales de tiempo que son emitidos por su ASDT son emitidos de forma segura e incluyen la escala de tiempo precisa dentro de los tokens de respuesta. Para ello, PSC Codex emite sus Sellos Digitales de Tiempo siguiendo la estructura de datos señala en el RFC 3161, conforme a lo requerido por las Reglas Generales, e incluye el tiempo exacto de emisión al obtener la escala de tiempo de una fuente confiable conforme se describe en el apartado Fuente de tiempo confiable del presente documento.

Una vez que la Autoridad de Sellado Digital de PSC Codex genera el token de sellos digital de tiempo conforme al RFC 3161 se puede asegurar que dicho token contiene al menos la siguiente información:

1. Identificador de la Autoridad de Sellado Digital de Tiempo.
2. Fecha y hora de la emisión del sello digital de tiempo.
3. OID asignado por la Secretaría a la Política del servicio.
4. Algoritmo criptográfico utilizado.
5. Número de serie del sello digital de tiempo.
6. Precisión del sello digital de tiempo conforme a los parámetros aceptados por el RFC 3161.
7. Cadena de certificación de los datos de creación de firma de la ASDT.

Entrega del Sello Digital de Tiempo

Una vez que se emite el sello digital de tiempo, PSC Codex a través de la interfaz por la cual fue realizada la petición de emisión del sello entrega el token de sello digital al cliente donde la respuesta se entrega en formato JSON y se encuentra compuesta de siguientes parámetros:

1. status. Puede contener los valores true y false.
    a. true. Indica que la solicitud y generación del sello digital de tiempo se llevó a cabo exitosamente.
    b. false. Indica que hubo un error en la petición y que el token de sello digital de tiempo no fue emitido.

2. hash-processed. Devuelve el valor del hash generado con SHA-256 a partir del cual se realizó la solicitud de emisión del sello digital de tiempo.
3. file. Contiene el token de sello digital de tiempo el cual se encuentra codificado en Base64.

Una vez que se entrega el token de sello digital de tiempo es responsabilidad del suscriptor verificar que dicho token concuerde con el hash o huella digital a partir del cual se realiza la solicitud.

Protección de datos personales y confidencialidad

El servicio de emisión de Sellos Digitales de Tiempo asegura a sus suscriptores la confidencialidad de su información, así como que no existe proceso o procedimiento que permita a terceras personas acceder a la información respecto de la cual se genera un sello digital de tiempo una vez que la información es recibida por el servicio de PSC Codex. Lo anterior se puede garantizar ya que los suscriptores o partes interesadas únicamente entregan a PSC Codex el hash o huella digital del mensaje de datos respecto del cual solicitan la emisión del sello digital.

El resguardo de la información antes y después de la solicitud y emisión de un sello digital de tiempo es responsabilidad de los suscriptores y partes interesadas.

Fuente de tiempo confiable

En cumplimiento con lo establecido en la Regla 123 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, PSC Codex ha celebrado un contrato de prestación de servicios con el Centro Nacional de Metrología, para obtener la transferencia segura de la escala de tiempo UTC, que se envía a la Autoridad de Sellado Digital de Tiempo, así como su redundancia por seguridad.

Para garantizar la seguridad en el proceso de transferencia segura de la escala de tiempo, se ha implementado una conexión VPN entre el CENAM y los centros de datos donde se ubica la infraestructura del servicio de PSC Codex.

Seguridad física y ambiental

PSC Codex implementa una Política de Seguridad Física la cual tiene como objeto el establecer los lineamientos, procedimientos y mecanismos de seguridad que se deberán de atender dentro de la organización y las instalaciones donde realice cualquier tipo de actividad con la finalidad de asegurar que sus activos de información, de infraestructura, de comunicaciones y de recursos humanos, entre otros, se mantienen íntegros y disponibles para garantizar la disponibilidad de los servicios que soportan.

Los lineamientos que se establecen en materia de seguridad física, a su vez, deben ayudar a generar las condiciones propicias que permitan dar cumplimiento a los

procesos establecido dentro del Sistema de Gestión de Seguridad de la Información, así como a la consecución de los objetivos de seguridad de la información. Desde la perspectiva de PSC Codex la seguridad física de su infraestructura como Prestador de Servicios de Certificación está directamente relacionada con la seguridad de la información al ser el primer elemento de control a través del cual se establecen limitaciones de acceso a los equipos dentro de los cuales se realizan los procesos de emisión de certificados digitales, sellos digitales de tiempo y de constancias de conservación de mensajes de datos.

El detalle de los controles de acceso y procedimientos de seguridad física y ambiental que se tienen implementados en los centros de datos y oficinas administrativas de PSC Codex se pueden consultar a detalle en el documento de la "*Política de Seguridad Física*".

Gestión de las operaciones

PSC Codex dentro de sus obligaciones como Prestador de Servicios de Certificación está obligado a asegurar que los componentes de la Autoridad de Sellado Digital de Tiempo, tanto en software como en hardware, operan correctamente y con un limitado nivel de fallo. Por lo anterior y atendiendo a lo establecido en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, PSC Codex implementa, entre otras, las siguientes medidas:

1. La infraestructura física de la ASDT se resguarda en dos centros de datos.
2. Se establecen procedimientos de acceso a las oficinas administrativas y centros de datos.
3. Se utilizan sistemas antivirus en los componentes de la ASDT.
4. Se utilizan herramientas de detección de vulnerabilidades.
5. Las instalaciones de los centros de datos cuentan con sistemas de detección y protección de intrusiones.

Adicionalmente, la infraestructura tecnológica que forma parte de la ASDT de PSC Codex cuenta con mantenimientos preventivos programados lo que permite extender el tiempo de vida útil de sus componentes. El mantenimiento lo lleva a cabo personal de PSC Codex que cuenta con los conocimientos técnicos necesarios para realizar este tipo de tareas.

El Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad monitorean constantemente la demanda del servicio de emisión de sellos digitales de tiempo para conocer si la capacidad instalada de infraestructura es suficiente para continuar soportando el servicio o se requiere escalar los componentes de infraestructura a fin de continuar brindando el servicio que suscriptores y sujetos relacionados esperan.

Gestión de acceso al sistema

PSC Codex garantiza que el acceso a su infraestructura física y a los componentes lógicos que integran la Autoridad de Sellado Digital de Tiempo se encuentra limitado al personal de confianza designado por la organización y que se encuentra acreditado como parte de los elementos humanos ante la Secretaría de Economía.

Como ya se ha señalado, la infraestructura física de PSC Codex se encuentra ubicada dentro de los centros de datos que se tienen contratados a los cuales únicamente tiene acceso el personal acreditado por PSC Codex que para el ingreso a las instalaciones debe de cumplir con todos los lineamientos que señalan los propios centros de datos para el acceso a sus instalaciones. Además, los centros de datos, como parte de la Política de Seguridad Física tienen implementados sistemas de detección y protección de intrusiones los cuales permiten contar con los elementos necesarios para recibir las alertas relacionadas con intentos de acceso no autorizados a las instalaciones y particularmente a las áreas seguras de los centros de datos.

En la protección de los elementos lógicos implementa elementos como firewall para restringir el tráfico de peticiones que ingresan a la Autoridad de Sellado Digital de Tiempo, donde adicionalmente se hace uso de routers y switches para implementar mayores niveles de seguridad para el servicio de sellos digitales de tiempo. El Firewall, además, tiene restringidos todos aquellos protocolos que no están relacionados con los sellos de tiempo para limitar las vulnerabilidades que puedan presentarse en ese sentido.

Respecto de la seguridad implementada en las comunicaciones, mediante el uso de los routers, switch y firewalls PSC Codex garantiza que la infraestructura de se Autoridad de Sellado Digital de Tiempo tiene restringidas las comunicaciones a equipos que integran dicha Autoridad y que toda comunicación con los suscriptores y partes interesadas se da mediante las interfaces del servicio que, en este caso, son servicios web para la solicitud y recepción de los *tokens* de sellos digitales de tiempo.

La operación del servicio implica que el personal de confianza que opera el servicio de emisión de sellos de tiempo se encuentra plenamente identificado en todo momento dentro de los sistemas con medidas que permiten separar las funciones dentro del sistema. La operación de la ASDT también implica que las actividades se encuentran monitoreadas constantemente con la finalidad de detectar, registrar y reaccionar a cualquier intento de acceso no autorizado que pueda poner en riesgo la operación del servicio.

Implementación y mantenimiento de sistemas confiables

El sistema, componentes y servicios de software que componen la Autoridad de Sellado Digital de Tiempo de PSC Codex han sido desarrollados e implementados por personal de la organización que sigue las mejores prácticas en el desarrollo de aplicaciones y sistemas con la finalidad de asegurar que los sistemas cuentan con las

medidas de seguridad necesarias para proteger la seguridad de la información generada como parte del servicio.

Durante el proceso de levantamiento de requerimientos del sistema, ya sea durante el desarrollo inicial o durante la implementación de mejoras, particularmente en la etapa de diseño del sistema el equipo de PSC Codex analiza e identifica los componentes o procesos que pudieran generar vulnerabilidades en la operación del servicio y construye la solución corrigiendo dichas vulnerabilidades.

Adicionalmente, para una mejor gestión del ciclo de vida del software del sistema de emisión de sellos digitales de tiempo, PSC Codex hace uso de herramientas de control de versionamiento con la cual se puede tener un seguimiento puntual de los cambios que se realizaron en cada una de las liberaciones realizadas como parte del proceso de mejora continua del sistema.

Terminación de la ASDT

Ante una eventual terminación o cese de funciones de la Autoridad de Sellado Digital de Tiempo, PSC Codex se asegurará de minimizar las afectaciones a sus suscriptores y partes interesadas como parte de la terminación del servicio de emisión de sellos digitales de tiempo, además de asegurarse de mantener mecanismos que permitan a los interesados verificar la validez de los sellos digitales emitidos con anterioridad al cese de funciones.

Como parte del procedimiento de cese, PSC Codex se asegurará de notificar y poner a disposición de sus suscriptores y partes interesadas la información concerniente a la terminación del servicio con al menos 90 días de anticipación. Durante este periodo, PSC Codex se asegurará de transferir a otro Prestador de Servicios de Certificación, acreditado por la Secretaría de Economía, los archivos de registro y de auditoría que permitan verificar que la ASDT de PSC Codex estuvo operando dentro de la normativa aplicable.

Finalmente, PSC Codex solicitará a la Secretaría de Economía la revocación de los certificados que hayan sido emitidos para la operación de la ASDT para el servicio de emisión de Sellos Digitales de Tiempo. Además, como parte del procedimiento de terminación de actividades, PSC Codex se asegurará que las llaves privadas de los datos de creación de firma de la ASDT sean eliminadas de los módulos criptográficos y cualquier medio electrónico de tal manera en que no puedan ser recuperadas.

Cumplimiento de la legislación aplicable

El marco jurídico mexicano establece los lineamientos de operación de los servicios que los Prestadores de Servicios de Certificación pueden emitir, donde parte fundamental de los requerimientos se centra en la seguridad de la información.

Entre la normativa aplicable a PSC Codex como Prestador de Servicios de Certificación y particularmente para el servicio de emisión de sellos digitales de tiempo, se encuentran los ordenamientos siguientes:

1. Ley de Firma Electrónica Avanzada.
2. Disposiciones Generales de la Ley de Firma Electrónica Avanzada.
3. Código de Comercio.
4. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
5. Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.
6. Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.
7. Ley Federal de Protección de Datos Personales en Posesión de Particulares.
8. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Consideraciones de seguridad

El uso de medios digitales, en este caso de los Sellos Digitales de Tiempo emitidos por PSC Codex como Prestador de Servicios de Certificación implica un claro entendimiento por parte de los suscriptores y partes interesadas respecto del funcionamiento, estructura, aplicación y alcance de este servicio. Parte de este entendimiento requiere del conocimiento de las consideraciones de seguridad que son aplicables a la emisión de Sellos Digitales de Tiempo y las cuales deben de ser observadas por los suscriptores y partes interesadas.

El primer punto de seguridad a considerar es la seguridad del Sello Digital de Tiempo es la verificación de la cadena de certificación, es decir, que el certificado del Prestador de Servicios de Certificación no se encuentra comprometido ni ha sido revocado. Esto significa que la seguridad del sello digital de tiempo depende de la seguridad de la Autoridad Certificadora que emite su certificado, en este caso la Secretaría de Economía, y que el mismo incluye la información relevante respecto de los certificados. PSC Codex para incrementar el nivel de seguridad y presentar la completa la cadena de certificación dentro de los sellos digitales de tiempo, incluye las llaves públicas tanto de la Autoridad Certificadora de la Secretaría de Economía, como de la Autoridad de Sellado Digital de Tiempo de PSC Codex.

Ahora bien, este proceso de verificación de la cadena de certificación no puede acreditarse como una validación única que sea aplicable a todos los sellos de tiempo emitidos, si no que en cada emisión de sello digital se requiere realizar esta verificación, lo anterior dado que el estatus del certificado puede modificarse de un momento a otro en caso de que las llave privada de la Autoridad de Sellado Digital se vea comprometida o que la Secretaría de Economía conforme a las disposiciones aplicables decida revocar dicho servicio.

Otro de los puntos de seguridad a considerar en la solicitud y emisión de un sello digital de tiempo por parte de los suscriptores es el garantizar la integridad de la

información con anterioridad a la emisión del sello digital de tiempo. Garantizar la integridad de la información es una de las obligaciones de los suscriptores y partes interesadas, tal como se describe en el apartado Obligaciones de los suscriptores, ya que con la finalidad de mantener la confidencialidad de la información PSC Codex únicamente recibe el hash o huella digital del mensaje de datos sobre el cual se requiere la emisión del sello digital de tiempo.

Finalmente, los suscriptores conforme lo señalan el RFC 3628 debieran asegurarse de que el hash o huella digital que se incluye dentro del *token* de sello digital de tiempo coincide con el que se integró en la solicitud de este.

Calendario de revisiones

PSC Codex dentro de sus procesos organizacionales ha establecido que la revisión a la Política de Sellado Digital de Tiempo se realizará de forma anual. Ahora bien, las revisiones podrán realizarse de forma extraordinario si las condiciones tecnológicas, sociales, ambientales o de cualquier otra naturaleza así lo requieran.

Fecha de la revisión	Versión revisada	Responsable (Nombre y firma)	Observaciones
03/06/2022			
03/06/2023			
03/06/2024			
03/06/2025			