Documento

Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos

PSC Codex

Versión 1.1

2 de enero de 2023

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 Constancias de Conservación de Mensajes de Datos 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 Constancia de Conservación de Mensajes de Datos se presenta con la firma electrónica de documentos, donde la constancia de conservación se utiliza para probar que el mensaje de datos no fue alterado ni modificado con posterioridad a la firma del mismo y la emisión de la constancia.

El uso y aplicación de los Constancias de Conservación de Mensajes de Datos dentro de las transacciones comerciales está 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos.

Fuentes

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

Glosario de Términos

Concepto	Descripción
ACCMD	Autoridad de Constancias de Conservación de Mensaje de Datos
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)	Persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas. Art. 2 inciso e) Ley CNUDMI 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. Art. 89 C de Com. Las instituciones públicas conforme a las leyes que le son aplicables, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo a lo establecido en el Código de comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada y, en su caso, expedir certificados digitales. Art. 2 Fr. XIX LFEA

Framework de referencia

PSC Codex ha desarrollado la presente Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos 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)*". Si bien el documento de referencia está enfocado en la generación de Sellos Digitales de Tiempo, además de que las Reglas Generales no establecen un estándar para la definición de la presente Declaración de Prácticas, PSC Codex considera la implementación de dicho estándar como una buena práctica y por ello la réplica para su servicio de emisión de Constancias de Conservación de Mensajes de Datos. 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 Constancias de Conservación de Mensajes de Datos.
2. Aplicabilidad de la Política definida en el presente documento.
3. Identificador de la Política de Emisión de Constancias de Conservación de Mensajes de Datos.
4. Obligaciones y responsabilidades.

Conceptos Generales

Constancia de Conservación de Mensajes de Datos

Si bien no existe una definición oficial para el término “Constancia de Conservación de Mensaje de Datos”, PSC Codex como parte de su servicio establece que una constancia de conservación es todo aquel elemento que se genera a partir de un algoritmo criptográfico y es firmado por su Autoridad de Constancias de Conservación de Mensajes de Datos y tiene como finalidad generar la evidencia para comprobar que un mensaje de datos se mantiene integro e inalterable en el tiempo.

Servicio de emisión de Constancias de Conservación de Mensajes de Datos

El servicio de emisión de Constancias de Conservación de Mensajes de Datos 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 las constancias que son generados por la Autoridad de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos

PSC Codex define su Autoridad de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos.

La Autoridad de Constancias de Conservación de Mensajes de Datos obtiene la escala de tiempo, con la cual emite Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos 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 de la Constancia de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos

Identificación

La Política de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos.

El identificador asignado por la Secretaría a la Política de Constancias de Conservación de Mensajes de Datos 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 Constancias, será incluido en la Autoridad de Constancias de Conservación de Mensajes de Datos y, por ende, en cada una de las constancias de conservación que emita dicha autoridad.

OID de la Declaración de Practicas de CCMD de PSC Codex: 2.16.484.101.10.316.100.10.1.2.2.1.1.1

Inicio de operaciones

Con fecha de 15 de diciembre de 2023 la Secretaría de Economía resolvió otorgar la acreditación como Prestador de Servicios de Certificación a PSC Codex para el servicio de emisión de Constancias de Conservación de Mensajes de Datos, publicando en el Diario Oficial de la Federación la acreditación correspondiente.

Publicada la acreditación, PSC Codex inicio operaciones del servicio de emisión de Constancias de Conservación de Mensajes de Datos con fecha 27 mayo de 2024

Usuarios y aplicabilidad

La presente Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos 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* de la Constancia de Conservación de Mensajes de Datos por la Autoridad correspondiente y atendiendo a la definición y alcance que se establece para las constancias de conservación de mensajes de datos.

Tecnológicamente esta Política establece los lineamientos a través de los cuales se da cumplimiento a los requerimientos para el uso de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos que proporciona PSC Codex, entendiendo como comunidad de usuarios a los suscriptores del servicio, así como a las partes interesadas en el mismo. La Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos es considerada como un documento de acceso público por parte de PSC Codex por lo que será consultable en la dirección www.psccodex.com/practicas_conservacion/.

Conformidad

PSC Codex declara que conforme lo establece el RFC 3628 su Autoridad de Constancias de Conservación de Mensajes de Datos incluye dentro de los *tokens* de constancias de conservación 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 Constancias de Conservación de Mensajes de Datos.

El OID que se incluye en las Constancias de Conservación de Mensajes de Datos es: 2.16.484.101.10.316.100.10.1.1.1.1.1.0

PSC Codex hará del conocimiento de los suscriptores y partes interesadas en el servicio de emisión de Constancias de Conservación de Mensajes de Datos del OID asignado por la Secretaría dentro de su portal de internet, además de que el mismo se incluye dentro de la Política de Constancias de Conservación de Mensajes de Datos y en la presente Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos.

Obligaciones y responsabilidades

Los participantes de la emisión de Constancias de Conservación de Mensajes de Datos, 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 las Constancias de Conservación de Mensajes de Datos pueden derivar en la suspensión del servicio y, en su caso, en las acciones legales que PSC Codex pudiera considerar pertinentes.

Obligaciones de la ACCMD 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 Constancias de Conservación de Mensajes de Datos.

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

Obligaciones de la ACCMD 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 Constancias de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos 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 las Constancias de Conservación de Mensajes de Datos se emiten conforme a las disposiciones de la Secretaría de Economía.
d) Garantizar la confidencialidad de la información de las Constancias de Conservación de Mensajes de Datos 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 las Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos de PSC Codex.

Responsabilidades de la ACCMD

Adicionalmente a las obligaciones que enuncia PSC Codex como Prestador de Servicios de Certificación acreditado para la emisión de Constancias de Conservación de

Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos.

Obligaciones de los suscriptores

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

En ese sentido, los suscriptores y sujetos relacionados del servicio de emisión de Constancias de Conservación de Mensajes de Datos de PSC Codex tendrán las obligaciones siguientes:

- Generar el hash del documento respecto del cual requiere la emisión de una Constancia de Conservación de Mensajes de Datos conforme al algoritmo criptográfico dado a conocer por PSC Codex.
- Verificar que la Constancia de Conservación de Mensajes de Datos emitido corresponde con el hash con el cual se realizó la solicitud de emisión.
- Conocer y aceptar contenido de la Política de Constancias de Conservación de Mensajes de Datos y de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos.
- Gestionar adecuadamente las credenciales que se le asignan para el consumo del servicio.

Responsabilidades de los suscriptores

Una vez que PSC Codex genera y entrega la constancia de conservación de mensaje de datos a sus suscriptores, estos últimos serán responsables del uso, manejo y resguardo de dicha constancia. Al respecto, los suscriptores del servicio tendrán las responsabilidades siguientes:

- Notificar a la Autoridad de Constancia de Conservación de Mensaje de Datos si el hash contenido en la constancia de conservación no coincide con el mensaje de datos original.
- Gestionar adecuadamente las credenciales que se le asignan para el consumo del servicio.
- Solicitar de manera oportuna a la PSC Codex la asignación de nuevas credenciales de usuario en caso de sospechar o tener conocimiento de que las asignadas han sido robadas, extraviadas, o sean conocidas por terceros.

- Mantenerse al corriente en el pago de las transacciones generadas como parte del servicio.

Obligaciones de las partes que confían

Las partes que confían en el servicio de emisión de constancias de conservación por parte de la Autoridad de Constancias de Conservación de Mensajes de Datos 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.

Adicionalmente, PSC Codex establece que es obligación de las partes que confían desarrollar los mecanismos necesarios para poder acceder a los medios de consulta de información y de validación de la llave pública del certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos con el cual fue emitida la constancia de conservación.

Responsabilidades de las partes que confían

Las partes que confían en el servicio de emisión de sellos digitales de tiempo por parte de la ACCMD 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 las constancias de conservación emitidas por PSC Codex deberán ejecutar las siguientes acciones:

- Verificar la cadena de certificación presente en la constancia de conservación.
- Verificar que la constancia de conservación este correctamente firmada por la ACCMD de PSC Codex.
- Verificar que la constancia de conservación corresponde al hash respecto del cual se realizó la solicitud.
- Considerar las limitaciones que se establecen para el uso de las constancias de conservación de mensajes de datos emitidas por PSC Codex.

Requerimientos de las Prácticas de la ACCMD

Los requerimientos respecto de las prácticas de la ACCMD 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 Constancias de Conservación de Mensajes de Datos.

La implementación de la Autoridad de Constancias de Conservación de Mensajes de Datos conlleva el desarrollo y ejecución de diversos controles y mecanismos de seguridad para la emisión de una Constancia de Conservación de Mensajes de Datos.

En ese sentido, la emisión de un *token* de Constancia de Conservación de Mensajes de Datos 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.

Declaración de prácticas de la ACCMD

PSC Codex como Prestador de Servicios de Certificación para la emisión de Constancias de Conservación de Mensajes de Datos tiene la responsabilidad de establecer los mecanismos necesarios que permitan garantizar a las partes interesadas la fiabilidad del servicio proporcionado.

Al respecto, PSC Codex tiene implementados diversos procesos y ha establecidos lineamientos con relación a la seguridad de la información en busca de privilegiar sus tres principales características, como son la integridad, confidencialidad y disponibilidad. Entre las acciones y procesos implementados, se encuentran:

1. El desarrollo e implementación del documento denominado “Análisis y Evaluación de Riesgos y Amenazas” en el cual se identifican los riesgos y vulnerabilidades presentes en la infraestructura de la Autoridad de Constancias de Conservación de Mensajes de Datos, así como se establecen las acciones necesarias para mitigarlos o eliminarlos.
2. Se elaboró una Política de Seguridad de la Información la cual fue transmitida a todos los miembros de PSC Codex con la finalidad de concientizarlos respecto de la importancia de su participación.
3. Se identifican las dependencias que tiene PSC Codex con organizaciones externas para la prestación del servicio de Constancias de Conservación de Mensajes de Datos.
4. PSC Codex pone a disposición de sus suscriptores y partes interesadas la Política y Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos, así como los documentos que puedan considerarse relevantes para la seguridad de la información.
5. El Comité de Seguridad en coordinación con la Alta Dirección de PSC Codex establecen las acciones necesarias para garantizar que los procesos de seguridad, así como las Políticas del servicio se implementan correctamente en la organización.
6. PSC Codex como parte de los procesos definidos en el Sistema de Gestión de Seguridad de la Información revisa periódicamente la Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos.
7. PSC Codex hace del conocimiento de suscriptores y partes interesadas los términos y condiciones relacionados a la emisión de Constancias de Conservación de Mensajes de Datos.

Declaración de divulgación de la ACCMD

El presente documento de la Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos se considera público al no contener información relevante que pueda poner en riesgo la operación del servicio de emisión de Constancias de Conservación de Mensajes de Datos por parte de PSC Codex, ni de la información que a través de sus diferentes interfaces es procesada.

Ubicación

Las oficinas administrativas de PSC Codex para la atención de clientes, suscriptores y partes interesadas del servicio de emisión de Constancias de Conservación de Mensajes de Datos se encuentran ubicadas en: Paseo de la Reforma 422 Piso 2, Colonia Juárez, Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06600.

Ilustración 1 Ubicación de las oficinas administrativas de PSC Codex

Datos de contacto

1. ***Teléfono*** ***5575005283***
2. ***Correo electrónico:*** ***contacto@psccodex.com***
3. ***Página de internet:*** ***https://www.psccodex.com***

Identificación de la Declaración de Prácticas

Una vez que se otorgó la acreditación como Prestador de Servicios de Certificación a PSC Codex, la Secretaría de Economía asigno los siguientes OID's:

a. Política de Constancias de Conservación de Mensajes de Datos: 2.16.484.101.10.316.100.10.1.2.1.1.1.0

b. Declaración de Prácticas: 2.16.484.101.10.316.100.10.1.2.2.1.1.1

Política de Privacidad

En cumplimiento a la Ley de Protección de Datos Personales en Posesión de Particulares, PSC Codex en su sitio electrónico tiene publicado el Aviso de Privacidad aplicable a los servicios que ofrece como Prestador de Servicios de Certificación. El aviso de privacidad es consultable en la página https://www.psccodex.com/aviso-de-privacidad/.

Algoritmo criptográfico utilizado

PSC Codex conforme a lo publicado por la Secretaría de Economía en la dirección electrónica http://www.firmadigital.gob.mx/marco_juridico.html utiliza el algoritmo criptográfico conocido como SHA-256 para la emisión del servicio de Constancias de Conservación de Mensajes de Datos.

Periodo de resguardo de información

Como parte de la política de operación del servicio de emisión de Constancias de Conservación de Mensajes de Datos, PSC Codex ha determinado que todos aquellos registros relacionados con el servicio, principalmente los *tokens* de Constancias de Conservación de Mensajes de Datos serán resguardados por un periodo de 3 años.

Disponibilidad del servicio

PSC Codex tiene implementada una infraestructura redundante de la Autoridad de Constancias de Conservación de Mensajes de Datos, la cual se encuentra distribuida en los centros de datos que tienen arrendados los cuales se encuentran permanentemente activos y cada uno de los cuales puede atender el volumen de operación total del servicio. Por tanto, PSC Codex garantiza a sus suscriptores y partes interesadas una disponibilidad de sus servicios del 99.9%.

Ciclo de vida de las llaves criptográficas de la ACCMD

Se denomina ciclo de vida de las llaves criptográficas de la ACCMD de PSC Codex el 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 Constancias de Conservación de Mensajes de Datos 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 ACCMD.

Generación de las llaves de la ACCMD

La generación de los datos de creación de firma de la ACCMD se lleva a cabo en un procedimiento conocido como Ceremonia de Generación en la cual se generan tanto la llave pública como la llave privada de la ACCMD. En esta ceremonia participa el personal asignado por la Secretaría de Economía, así como los elementos humanos que PSC Codex presentó para la acreditación de dicho servicio. Como parte de las medidas de seguridad que se toman durante la generación del certificado, todo el personal que ingresa a los centros deberá registrarse y su acceso estará autorizado por el Auxiliar de Apoyo Informático de Seguridad.

El certificado se generará y almacenará en un módulo criptográfico que cumple con los requisitos que establecen las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, es decir, es un módulo criptográfico

certificado en el estándar FIPS 140-2 nivel 3. También, en concordancia con la Regla 12 de las Reglas Generales, el certificado de la ACCMD de PSC Codex tendrá una vigencia de hasta cuatro quintas partes del periodo de validez del Certificado de la Autoridad Certificadora de la Secretaría de Economía.

Tanto la longitud de llave, como el algoritmo mediante el cual se emite el certificado deberán ser los establecidos por la Secretaría de Economía y deberán ser reconocidos por el mercado con relación a procesos de infraestructuras PKI. En este caso la longitud de llave será de 4096 bits y se utilizará el algoritmo criptográfico conocido como SHA-256.

Protección y almacenamiento de las llaves de la ACCMD

PSC Codex para la operación de su servicio de emisión de Constancias de Conservación de Mensajes de Datos cuenta con dos módulos criptográficos para el almacenamiento, resguardo y protección de sus datos de creación de firma que, conforme a las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, están certificados con el estándar FIPS 140-2 nivel 3. Estos módulos criptográficos se encuentran ubicados dentro de los centros de datos que alojan la infraestructura de Codex como PSC.

Para incrementar la seguridad de los datos de creación de firma de la ACCMD aun y cuando los certificados se almacenan en el HSM, el acceso físico a dichos módulos se encuentra limitado únicamente al Profesional Informático y al Auxiliar de Apoyo Informático de Seguridad quienes son las únicas personas autorizadas para acceder a los racks donde se encuentran ubicados los equipos en los centros de datos.

Distribución de la llave Pública

Los procesos y servicios basados en infraestructura de clave pública, como es el caso del servicio de emisión de Constancias de Conservación de Mensajes de Datos de PSC Codex, tienen la obligación y el compromiso de asegurar que las partes interesadas puedan verificar la autenticidad e integridad de los procesos que de ella emanan.

Al respecto, PSC Codex distribuye la llave pública de su Autoridad de Constancias de Conservación de Mensajes de Datos a las partes interesadas en su servicio de emisión de constancias de conservación con la finalidad de que puedan verificar que los *tokens* de constancias de conservación que les son proporcionados han sido firmados por dicha autoridad.

El certificado se encuentra disponible en el portal de internet de PSC Codex, en la dirección https://www.psccodex.com/certificados_conservacion, así como en el portal de la Secretaría de Economía, en la dirección http://www.firmadigital.gob.mx/directorio.html donde además se podrá consultar la acreditación de PSC Codex, como Prestador de Servicios de Certificación, publicada en el Diario Oficial de la Federación.

Reemisión de las llaves de la ACCMD

El RFC 3628 establece diversas consideraciones respecto del periodo de vida de los datos de creación de firma de una Autoridad de Constancias de Conservación de Mensajes de Datos para garantizar la seguridad la integridad de los datos que se generan a partir de este certificado. Entre las consideraciones más importante, el RFC refiere que la vigencia del certificado debe ser menor al tiempo de vida estimado para el algoritmo criptográfico utilizado para la firma del certificado, así como de la longitud de las llaves. En ese sentido, es la Secretaría de Economía la encargada de definir los algoritmos y longitudes que debe utilizar PSC Codex en la emisión de sus datos de creación de firma. Los parámetros vigentes son longitud de llave de 4096 bits y el algoritmo criptográfico conocido como SHA-256.

En caso de que la longitud de llave o el algoritmo de firma dejen de ser válidos, se considerará que las llaves alcanzaron el fin de su ciclo de vida. En el apartado siguiente se establecen los escenarios adicionales que propician el fin del ciclo de vida de los datos de creación de firma y las acciones que se deben ejecutar para continuar con la emisión del servicio.

Fin del ciclo de vida de las llaves de la ACCMD

Se dice que el certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos de PSC Codex ha llegado al final de su ciclo de vida cuando se cumplen algunas condiciones que impiden que dicha autoridad pueda seguir garantizando la integridad y confidencialidad de la información que se genera en los procesos que utilizan dicho certificado, específicamente la emisión de Constancias de Conservación de Mensajes de Datos.

Los supuestos que pueden derivar en el final del ciclo de vida son los siguientes:

1. Fin de vigencia.
2. Revocación de claves.
3. Función hash obsoleta.
4. Longitud de claves no segura.

PSC Codex mantendrá una estrecha y continua comunicación con la Secretaría de Economía, con la finalidad de solicitar la emisión de un nuevo par de llaves para poder continuar prestando el servicio de emisión de Constancias de Conservación de Mensajes de Datos, conforme a los supuestos y requisitos aplicables en cada escenario.

Ciclo de vida de los módulos criptográficos

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 Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos de PSC Codex puede consultarse en el documento denominado "*Plan de Administración de Claves de la ACCMD*".

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 constancias de conservación de mensajes de datos que se tiene acreditado como PSC.

Los objetivos de seguridad de la información para el servicio de emisión de constancias de conservación de mensajes de datos 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. Garantizar que una vez que la información ingresa al servicio de PSC Codex la misma se mantiene integra y confidencial durante todo el proceso.
12. Monitorear permanentemente el servicio de constancias de conservación de mensajes de datos para garantizar que se cuenta con la capacidad tecnológica necesaria para brindar comercialmente el servicio.
13. Emitir constancias de conservación de mensajes de datos únicamente a los suscriptores que hayan completado el proceso de contratación con PSC Codex.
14. Distribuir de forma segura la llave pública del certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos para que los suscriptores y partes interesadas puedan verificar la validez de las constancias emitidas por PSC Codex.

Constancia de Conservación de Mensajes de Datos

Procedimiento para la emisión de una Constancia de Conservación de Mensajes de Datos

El servicio de emisión de Constancias de Conservación de Mensajes de Datos se pondrá disposición de los suscriptores de PSC Codex a través de un servicio web el cual tendrá una interfaz pública mediante la cual dichos suscriptores podrán solicitar la Constancia de Conservación de Mensajes de Datos 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 de la constancia de conservación.

El servicio web que implementa PSC Codex para su servicio de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos 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 una constancia de conservación de mensajes de datos.

Contratación del servicio de emisión de Constancias de Conservación de Mensajes de Datos

El proceso de contratación del servicio para la emisión de Constancias de Conservación de Mensajes de Datos por parte de la Autoridad de Constancias de Conservación de Mensajes de Datos 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 él.

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 Constancias de Conservación de Mensajes de Datos.

Registro de usuario en la plataforma

Los interesados o suscriptores del servicio de emisión de Constancias de Conservación de Mensajes de Datos como parte inicial para la emisión del servicio de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos conforme se haya convenido en términos contractuales y asignará dentro de la plataforma el número de constancias que podrá disponer el usuario, así como su tiempo de vigencia. Una vez que se asigna el inventario correspondiente a las Constancias de Conservación de Mensajes de Datos, 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 Constancias de Conservación de Mensajes de Datos cuenta con mecanismos de autenticación para la solicitud y respuesta que permite garantizar que únicamente se emitan tokens de Constancias de Conservación de Mensajes de Datos a los suscriptores del servicio de PSC Codex.

PSC Codex, implementa la autenticación para su servicio de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos para que puedan

realizar el desarrollo de sus sistemas cliente a través del cual realizarán la solicitud de token de Constancias de Conservación de Mensajes de Datos.

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 Constancias de Conservación de Mensajes de Datos. 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 desarrollo 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 Constancias de Conservación de Mensajes de Datos.

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 de la Constancia de Conservación de Mensajes de Datos

Petición de la Constancia de Conservación de Mensajes de Datos

PSC Codex brindará a sus suscriptores el servicio de emisión de Constancias de Conservación de Mensajes de Datos 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 de la Constancias de Conservación de Mensajes de Datos, la 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 de la Constancia de Conservación de Mensajes de Datos 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 nom_hash que espera como valor de entrada el hash o huella digital del mensaje de datos sobre el cual se requiere la emisión de la Constancia de Conservación de Mensajes de Datos, que debe de ser generada utilizando el algoritmo criptográfico SHA-256.

Emisión del token de la Constancia de Conservación de Mensajes de Datos

Una vez que PSC Codex recibe la solicitud de Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos para la emisión de la constancia solicitada.

Como parte del proceso de emisión de Constancias de Conservación de Mensajes de Datos PSC Codex se asegura que se cumplan las siguientes condiciones:

1. El token de Constancia de Conservación de Mensajes de Datos incluye el identificador de las Políticas de Constancias de Conservación de Mensajes de Datos asignado por la Secretaría de Economía.
2. Cada una de las Constancias de Conservación de Mensajes de Datos emitidas 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 Constancias de Conservación de Mensajes de Datos pierde sincronía con la fuente de tiempo confiable no se emitirán constancias de conservación.
6. La Constancia de Conservación de Mensajes de Datos se emite con los datos de creación de firma de uso específico que la Secretaría de Economía proporciona a PSC Codex.

Contenido del token de Constancia de Conservación de Mensajes de Datos

PSC Codex es responsable de asegurar que las Constancias de Conservación de Mensajes de Datos que son generadas por su ACCMD son emitidas de forma segura e incluyen la escala de tiempo precisa dentro de los tokens de respuesta. Para ello, PSC Codex emite sus Constancias de Conservación de Mensajes de Datos siguiendo la estructura de datos señalada en el RFC 3161, conforme a lo requerido por la NOM-151-SCFI-2016, 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 Constancias de Conservación de Mensajes de Datos de PSC Codex genera el token de constancia de conservación conforme al RFC 3161 se puede asegurar que dicho token contiene al menos la siguiente información:

1. Identificador de la Autoridad de Constancias de Conservación de Mensajes de Datos.
2. Fecha y hora de la emisión de la constancia de conservación.
3. OID asignado por la Secretaría a la Política del servicio.
4. Algoritmo criptográfico utilizado.
5. Número de serie de la Constancia de Conservación de Mensajes de Datos.
6. Precisión de la constancia de conservación de mensajes de datos conforme a los parámetros aceptados por el RFC 3161.
7. Cadena de certificación de los datos de creación de firma de la ACCMD.

Entrega de la Constancia de Conservación de Mensajes de Datos

Una vez que se emite la constancia de conservación, PSC Codex a través de la interfaz por la cual fue realizada la petición de emisión de la constancia entrega el token de Constancia de Conservación de Mensajes de Datos 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 de la constancia de conservación se llevó a cabo exitosamente.
    b. false. Indica que hubo un error en la petición y que el token de constancia de conservación 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 de al Constancia de Conservación de Mensajes de Datos.
3. file. Contiene el token de Constancia de Conservación de Mensajes de Datos el cual se encuentra codificado en Base64.

Una vez que se entrega el token de Constancia de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos 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 una Constancia de Conservación de Mensajes de Datos 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 de la constancia.

El resguardo de la información antes y después de la solicitud y emisión de una Constancia de Conservación de Mensajes de Datos es responsabilidad de los suscriptores y partes interesadas.

Fuente de tiempo confiable

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 Constancias de Conservación de Mensajes de Datos, 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.

Administración y operación de la ACCMD

Gestión de la seguridad

PSC Codex garantiza a los suscriptores y partes interesadas que la gestión y administración de los procesos asociados a la emisión de Constancias de Conservación de Mensajes de Datos se realiza de conformidad con las Políticas de Constancias de Conservación de Mensajes de Datos, así como en la presente Declaración de Prácticas en concordancia con los estándares y mejores prácticas de referencia que establece la Secretaría de Economía dentro de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.

En ese sentido, PSC Codex declara que cuenta con infraestructura y desarrollo propios para la integración de su Autoridad de Constancias de Conservación de Mensajes de Datos y por tanto es el único responsable de los aspectos y componentes relacionados con la emisión de Constancias de Conservación de Mensajes de Datos. Además, PSC Codex mantienen la responsabilidad y obligación de divulgar el contenido de la presente Declaración de Prácticas entre sus suscriptores y personas interesadas en el servicio.

Para la gestión de la seguridad relaciona con el servicio, la Alta Dirección de PSC Codex a conformado un Comité de Seguridad el cual ha sido el responsable de la definición de la Política de Seguridad de la Información aplicable a los servicios que PSC Codex tiene acreditados como Prestador de Servicios de Certificación. Conforme a los criterios definidos en el Sistema de Gestión de Seguridad de la Información PSC Codex hace de conocimiento de sus empleados y colaboradores los diversos documentos relacionados con la Seguridad de la Información y mantiene un constante programa de concientización y capacitación.

Los controles de seguridad aplicables al servicio de Constancias de Conservación de Mensajes de Datos de PSC Codex están documentados en los documentos de seguridad de la información del servicio, principalmente en el Sistema de Gestión de Seguridad de la Información y el Plan de Seguridad de Sistemas.

Clasificación y gestión de activos

PSC Codex como parte del proceso de implementación de su Sistema de Gestión de Seguridad de la Información, de la Política de Seguridad de la Información, de la Política de Seguridad Física, así como del Análisis de Riesgos se asegura que sus diferentes activos, ya sea información, activos intangibles o equipos que integran la infraestructura de la ACCMD se encuentren clasificados conforme al nivel de criticidad que representan para la operación del servicio de emisión de Constancias de Conservación de Mensajes de Datos.

En ese sentido, PSC Codex dentro del aparatado de activos críticos del “Análisis y Evaluación de Riesgos y Amenazas” ha relacionado aquellos componentes de la ACCMD que por su importancia son considerados como indispensables para la

prestación del servicio. Una vez identificados los activos y clasificados conforme a su nivel de criticidad les son aplicadas las políticas de protección de activos relacionadas con cada nivel de riesgo.

Seguridad del personal

PCS Codex como parte de los procesos que se implementan para incrementar la seguridad de la información en lo relativo a la Autoridad de Constancias de Conservación de Mensajes de Datos se asegura que los procesos de contratación, así como la selección de candidatos soportan la integridad de las operaciones de su Autoridad. Para ello, PSC Codex ha desarrollado e implementado el "Proceso de reclutamiento y selección" recursos humanos el cual establece el procedimiento a seguir durante la contratación de personal.

Ahora bien, particularmente para las vacantes y candidatos a puestos relacionados con la operación de la ACCMD, PSC Codex aplica las siguientes consideraciones:

a. El personal que labora directamente en la gestión y operación de la ACCMD tiene conocimiento experto, experiencia y calificaciones necesarias para las funciones propias del servicio de emisión de Constancias de Conservación de Mensajes de Datos. El conocimiento experto en temas relacionados a la ACCMD se puede comprobar mediante constancias y cursos de capacitación, así como por experiencia previa laborando con servicios similares.
b. Los roles de seguridad, así como sus responsabilidades se encuentran definidos en la Política de Seguridad de la Información, así como en el Sistema de Gestión de Seguridad de la Información y son documentados en el perfil de puesto correspondiente.
c. Los roles de confianza como son el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad son los responsables directos de gestionar las operaciones de la ACCMD y son acreditados ante la Secretaría de Economía.
d. El personal que labora en actividades relacionadas a la ACCMD está sujeto a los controles de Gestión de usuarios definidos en el Plan de Seguridad de Sistemas implicando, entre otros: la separación de actividades, asignación de privilegios mínimos, niveles de acceso, comprobación de antecedentes y referencias, así como la capacitación y concientización respecto de las actividades inherentes a su puesto.
e. El personal asignado a los roles de confianza se encuentra libre de cualquier conflicto de interés que pueda obstaculizar la operación de la ACCMD 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, Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos, 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 ACCMD 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 ACCMD.
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 ACCMD 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos, donde adicionalmente se hace uso de routers y switches para implementar mayores niveles de seguridad para el servicio de Constancias de Conservación de Mensajes de Datos. El Firewall, además, tiene restringidos todos aquellos protocolos que no están relacionados con las constancias de conservación 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos.

La operación del servicio implica que el personal de confianza que opera el servicio de emisión de constancias de conservación 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 ACCMD 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 Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos, 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.

Compromiso de la ACCMD

PSC Codex como Autoridad de Constancias de Conservación de Mensajes de Datos acreditada por la Secretaría de Economía para la emisión de Constancias de Conservación de Mensajes de Datos 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 ACCMD 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 ACCMD fue comprometida, PSC Codex realizará una auditoría en conjunto con suscriptores y partes interesadas para identificar los *tokens* de constancias de conservación legítimas de aquellas que fueron emitidas indebidamente como consecuencia del compromiso de la llave privada.

Terminación de la ACCMD

Ante una eventual terminación o cese de funciones de la Autoridad de Constancias de Conservación de Mensajes de Datos, PSC Codex se asegurará de minimizar las afectaciones a sus suscriptores y partes interesadas como parte de la terminación del servicio de emisión de Constancias de Conservación de Mensajes de Datos, además de asegurarse de mantener mecanismos que permitan a los interesados verificar la validez de las constancias de conservación emitidas 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 ACCMD 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 ACCMD para el servicio de emisión de Constancias de Conservación de Mensajes de Datos. 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 ACCMD sean eliminadas de los módulos criptográficos y cualquier medio electrónico de tal maneta 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 Constancias de Conservación de Mensajes de Datos, 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 de Protección de Datos Personales en Posesión de Particulares.

Registro de información relativa a la operación del servicio

Registros físicos

Como parte de la operación de la ACCMD para la emisión de Constancias de Conservación de Mensajes de Datos, PSC Codex integra registros de información que resguardan los datos a partir de los cuales se generó dicha constancia de conservación. En ese sentido, se integra un expediente físico en el cual se incluye el contrato de prestación del servicio firmado entre PSC Codex y las partes interesadas, así como la información que soporte dicho contrato, mismo que queda bajo la responsabilidad del Profesional Jurídico quien deberá de resguardar en un espacio seguro los expedientes y tenerlos identificables en caso de que sean requeridos por la autoridad.

Registros informáticos

Además de los registros físicos, PSC Codex conforme a su modelo operativo ha diseñado e implementado una base de datos de información, en la cual se registra la información relativa a la emisión de Constancias de Conservación de Mensajes de Datos. Se generan y almacenan los metadatos necesarios para vincular el hash respecto del cual se solicita la emisión del Constancia de Conservación de Mensajes de Datos con el token de dicha constancia de conservación una vez que fue firmado y emitido por la ACCMD de PSC Codex.

Los sistemas de información de PSC Codex, en especial la base de datos donde se resguardan los datos que se generan en la emisión de Constancias de Conservación de Mensajes de Datos se rige conforme a los controles de acceso a sistemas de información definidos por PSC Codex y son responsabilidad del Profesional Informático quien es el encargado de establecer los procedimientos para asegurar la Seguridad de la Información del servicio.

Proceso de auditoría

El programa de auditorías internas de PSC Codex establece que esta actividad se llevará a cabo de manera anual o en el momento que se considere necesario cuando los cambios en materia tecnológica así lo requieran o cuando se detecten vulnerabilidades graves en los componentes de la arquitectura tecnológica de los servicios de emisión de certificados digitales, sellos digitales de tiempo o constancias de conservación de mensajes de datos.

El programa de auditoría deberá ser de conocimiento de las áreas que gestionan, administran y operan los servicios que PSC Codex tiene autorizados como Prestador de Servicios de Certificación, a fin de que coordinen actividades y puedan facilitar oportunamente la información que requieran los auditores asignados. Durante el proceso de auditoría, además de los criterios y alcance definidos en el programa de auditoría, se deberán de considerar los resultados de las auditorías anteriores a fin de verificar que las observaciones y no conformidades encontradas hayan sido solventadas.

Ahora bien, en lo que respecta a las auditorías que se realizan sobre los sistemas de información relacionados con los servicios de emisión de certificados digitales, sellos digitales de tiempo o constancias de conservación de mensajes de datos, es importante conocer que cada uno de los componentes cuenta con un registro activo de actividades que en conjunto con las herramientas de monitoreo permite al Profesional Informático y al Auxiliar de Apoyo Informático de Seguridad conocer el comportamiento del sistema, además de identificar posibles amenazas o errores dentro de los procesos.

Los registros de auditoría se componen de los siguientes elementos:

1. Registro de eventos de la AC.
2. Eventos de bitácora relacionados con el servicio.
3. Sistema de directorios de la AC.
4. Registro de eventos de la ASDT.

5. Eventos de bitácora relacionados con el servicio.
6. Sistema de directorios de la ASDT.
7. Registro de eventos de la ACCMD.
8. Eventos de bitácora relacionados con el servicio.
9. Sistema de directorios de la ACCMD.
10. Registro de eventos de la base de datos.
11. Registro de eventos del software EMSISOFT.

Estos elementos son analizados al menos una vez a la semana por el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad para verificar que no se estén presentando errores o incidencias que puedan poner en riesgo la operación en el servicio. De encontrar registro de algún evento relacionado con la seguridad de la información deberán seguir los procedimientos descritos en la “Política de atención de incidentes de seguridad de la información”.

Es importante mencionar que con independencia de las revisiones que periódicamente se realizan a los registros de auditoría, los componentes de seguridad que se implementan como parte de la infraestructura de la Autoridad Certificadora, la Autoridad de Sellado Digital de Tiempo y la Autoridad de Constancias de Conservación de Mensajes de Datos permiten identificar, a través del monitoreo constante, riesgos asociados a la seguridad de la información donde se emiten alertas a los encargados del servicio respecto de los riesgos potenciales.

PSC Codex

PSC Codex declara que es una organización legalmente establecida conforme a los señalamientos de la Ley General de Sociedades Mercantiles y cuyos datos de constitución se encuentran inscritos en el Registro Público de Comercio por lo que le ha sido asignado el folio mercantil electrónico N-2021001797. PSC Codex declara que puede operar como Prestador de Servicios de Certificación una vez que ha dado cumplimiento a los requerimientos que establece la normativa aplicable y ha sido acreditado por la Secretaría de Economía para actuar como tal para la emisión del servicio de Emisión de Constancias de Conservación de Mensajes de Datos.

PSC Codex declara contar con un seguro de responsabilidad civil, así como de las fianzas que señalan las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación para hacer frente a cualquier compromiso derivado de la gestión y operación del servicio de emisión de Constancias de Conservación de Mensajes de Datos. Sin menoscabo de lo anterior, PSC Codex declara contar con la suficiente capacidad y estabilidad financiera para operar adecuadamente el servicio que le ha sido acreditado por la Secretaría de Economía.

Consideraciones de seguridad

El uso de medios digitales, en este caso de los Constancias de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos y las cuales deben de ser observadas por los suscriptores y partes interesadas.

El primer punto de seguridad a considerar es la seguridad del Constancia de Conservación de Mensajes de Datos 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 Constancia de Conservación de Mensajes de Datos 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 Constancias de Conservación de Mensajes de Datos, incluye las llaves públicas tanto de la Autoridad Certificadora de la Secretaría de Economía, como de la Autoridad de Constancias de Conservación de Mensajes de Datos 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 todas las constancias de conservación emitidas, si no que en cada emisión de constancia 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 Constancias de Conservación 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 Constancia de Conservación de Mensajes de Datos por parte de los suscriptores es el garantizar la integridad de la información con anterioridad a la emisión del Constancia de Conservación de Mensajes de Datos. 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 Constancia de Conservación de Mensajes de Datos.

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 Constancia de Conservación de Mensajes de Datos 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 de la Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos 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)**	**Responsable de Validación (Nombre y firma)**	**Observaciones**
03/06/2023	1.1		Cintya López Rodríguez Profesional Jurídico	Esta versión no tiene ninguna actualización o cambio a la fecha de su revisión.
03/06/2024				
03/06/2025				