incode psc

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

OID de la Declaración de Prácticas de

Constancias de Conservación de Mensajes de Datos:

2.16.484.101.10.316.100.12.1.2.2.1.1.1

Tabla de Contenido

Tabla de Imágenes

Control de versiones

Versión	Modificado Por	Modificaciones Realizadas	Fecha de Modificación
1.0	LAVG	Primera versión	03/2023
1.1	LAVG	Se reemplazan dos referencias a la Autoridad de Sellado Digital de Tiempo como parte de las observaciones de la Secretaría de Economía	10/2023
1.2	LAVG	1. Se incluye el OID proporcionado por la Secretaría de Economía. 2. Se indica la fecha de acreditación, publicación en DOF e inicio de operaciones. 3. Formato general del documento	05/2024

Calendario de revisiones

La Declaración de Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode será sometida a un proceso de revisión y actualización de forma anual o antes si las condiciones de operación del servicio así lo requieren.

Fecha de la revisión	Responsable	Observaciones
03/2024	LAVG	Sin observaciones
03/2025		
03/2026		

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

1 Introducción

Las organizaciones que basan su operación en sistemas de información o en medios electrónicos transaccionales o de estructura de datos requieren de la generación de evidencia confiable que les permita establecer una relación de confianza entre el tiempo en que los datos fueron generados o cuando las transacciones fueron realizadas de tal forma que puedan ser verificados y comparadas con posterioridad a la emisión del acto.

La presente Declaración de Prácticas y su correspondiente Política de Constancias de Conservación de Mensajes de Datos está estructurada para establecer los procedimientos que permitan aplicar la emisión de tokens de constancias de conservación para probar que un mensaje de datos no ha sido alterado con posterioridad a la emisión de la constancia.

La Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos establece los lineamientos básicos generales que Incode como Prestador de Servicios de Certificación deberá de implementar como parte del proceso de emisión de constancias de conservación implementando procesos de generación seguros del token de dicha constancia. Adicionalmente, define los requerimientos de operación de la Autoridad de Constancias de Conservación de Mensajes de Datos que opera bajo el ecosistema de una infraestructura de clave pública.

Una de las características principales de la emisión de las constancias de conservación es la precisión con la que se emite este tipo de evidencia, donde derivado del RFC 3161 y de la NOM 151 se establece que la precisión de tiempo para la emisión de la

constancia el cual deberá ser de un segundo o mejor, lo cual genera un elemento de comprobación en los procesos transaccionales donde es fundamental establecer el momento preciso en el cual se realiza una acción.

Es precisamente la función y responsabilidad del Prestador de Servicios de Certificación que opera el servicio de emisión de constancias de conservación, proporcionar a sus usuarios y partes interesadas elementos emitidos a través de procesos criptográficos donde se establezca una relación no repudiable del contenido de un mensaje de datos a partir de la emisión de la constancia.

Ahora bien, como elemento fundamental de la emisión de las constancias de conservación se encuentra la fuente de tiempo confiable a través de la cual se obtendrá la escala de tiempo con el protocolo NTP que garantiza que la fecha y hora de emisión de la constancia no puede ser manipulada al encontrarse vinculada con una fuente oficial de tiempo.

2 Política de Constancias de Conservación de Mensajes de Datos

La Política de Constancias de Conservación de Mensajes de Datos forma parte de la Declaración de Prácticas de CCMD y busca establecer las reglas mínimas de operación aplicables a la generación de una constancia de conservación para garantizar que la información relacionada con la emisión de la constancia puede ser verificada en el tiempo. Una de las características de los tokens de constancias de conservación que implementa Incode es que la precisión en la emisión del token es de un segundo o mejor.

Resulta fundamental, en el proceso de emisión de constancias de conservación, la vinculación del token con la Política de Constancias de Conservación de Mensajes de Datos la cual se establece al incluir como parte del token el OID que asigna la Secretaría de Economía a la Política.

2.1 Identificación

El Objeto Identificador (OID) de la Política de Constancias de Conservación de Mensajes de Datos es el identificador que asigna la Secretaría de Economía a la Autoridad de Constancias de Conservación de Mensajes de Datos una vez que ha acreditado a Incode como Prestador de Servicios de Certificación.

El OID es un identificador único que permitirá a la Secretaría de Economía y partes interesadas identificar la Autoridad de Constancias de Conservación de Mensajes de Datos que emitió un *token* de constancia de conservación.

OID de la Política de Constancias de Conservación de Mensajes de Datos:

2.16.484.101.10.316.100.12.1.2.1.1.1.1

OID de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos:

2.16.484.101.10.316.100.12.1.2.2.1.1.1

2.2 Inicio de operaciones

La Secretaría de Economía por oficio No. 192.2024.000219 de fecha 24 de enero de 2024 notificó a Incode la procedencia de su acreditación como Prestador de Servicios de Certificación para el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

Con fecha de 22 de mayo de 2022 la propia Secretaría de Economía publicó en el Diario Oficial de la Federación la acreditación como Prestador de Servicios de Certificación para el servicio de emisión de Constancias de Conservación de Mensajes de Datos de Incode.

Completadas las formalidades correspondientes, así como las publicaciones oficiales por parte de la Secretaría de Economía, Incode inicio la operación del servicio de emisión de Constancias de Conservación de Mensajes de Datos el 03 de junio de 2024.

2.3 Usuarios y aplicabilidad

La Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos, la Política de Constancias de Conservación de Mensajes de Datos y los procedimientos de emisión de constancias de conservación de Incode establecen los procedimientos a través de los cuales se da cumplimiento al uso de constancias de conservación para el resguardo de la integridad de un mensaje de datos de conformidad con el Código de Comercio.

Como parte de la presente Declaración se establece que el servicio de emisión de constancias de conservación será aplicable a los usuarios o suscriptores del servicio y las partes interesadas relacionadas con la emisión, verificación o auditoría de los procesos generados a través de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode.

2.4 Conformidad

La Autoridad de Constancias de Conservación de Mensajes de Datos declara su conformidad con la implementación de infraestructura de llave pública al incorporar como parte de los tokens de constancias de conservación el OID asignado a la Política de Constancias de Conservación de Mensajes de Datos como uno de los elementos de identificación de los tokens que emite.

La Autoridad de Constancias de Conservación de Mensajes de Datos declara su conformidad al establecer las siguientes acciones:

1. Poner a disposición de sus usuarios y partes interesadas la evidencia necesaria para soportar su conformidad.
2. La declaración de conformidad de la Autoridad de Constancias de Conservación de Mensajes de Datos fue validada por la Secretaría de Economía como parte del proceso de acreditación como Prestador de Servicios de Certificación.

2.5 Distribución de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos

De conformidad con las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación y conforme al análisis realizado por el departamento de Seguridad y Cumplimiento del contenido de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos se considera que el presente documento es de interés público por lo cual se clasifica como información pública y será distribuido dentro de la página de internet del servicio de constancias de conservación de Incode.

URL de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos:

https://psc.incode.com/repositorio/

3 Metodología de implementación

Para el diseño, desarrollo e implementación de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos, Incode de conformidad con los requerimientos de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, considero los lineamientos que se establecen en el documento del RFC 3628 que lleva por título "*Policy Requirements for Time-Stamping Authorities (TSAs)*", que si bien hace referencia al servicio de emisión de sellos digitales de tiempo, sirve como marco de referencia para establecer las generalidades para la emisión de una constancia de conservación de mensajes de datos.

Dentro de los elementos que se señalan en la presente Declaración de Prácticas y que resultan de mayor relevancia para la emisión de constancias de conservación, se encuentran:

1. Identificador (OID) de la Política de Constancias de Conservación de Mensajes de Datos.
2. Obligaciones de la Autoridad de Constancias de Conservación de Mensajes de Datos.
3. Obligaciones de los consumidores de Constancias de Conservación de Mensajes de Datos.
4. Ciclo de vida de las llaves criptográficas de la Autoridad de Constancias de Conservación de Mensajes de Datos.
5. Sincronía con la fuente de tiempo confiable para la transmisión de la escala de tiempo.

4 Objetivo de la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos

La Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos tiene como objetivo dar a conocer a los interesados en el servicio los lineamientos y consideraciones a través de los cuales Incode realizará la emisión de constancias de conservación a través de su Autoridad de Constancias de Conservación de Mensajes de Datos como Prestador de Servicios de Certificación acreditado por la Secretaría de Economía.

5 Legislación aplicable al servicio de Constancias de Conservación de Mensajes de Datos

La operación de los Prestadores de Servicios de Certificación y de las actuaciones en medios electrónicos tiene sustento jurídico en diversas leyes de aplicación general y sus disposiciones secundarias que establecen los requisitos que deben cumplir los Prestadores para poder fungir como tales, así como los elementos que pueden emitir y el alcance de su aplicación.

Entre los ordenamientos relacionados a la implementación de medios electrónicos y su relación con los Prestadores de Servicios de Certificación, se encuentran:

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

6 Conceptos Generales

6.1 Servicio de emisión de Constancias de Conservación de Mensajes de Datos

El servicio de emisión de constancias de conservación de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode es un conjunto de componentes que permiten a los suscriptores solicitar y recibir un token de constancia de conservación. Uno de los elementos del servicio es el componente para la administración y control que tiene la función de asegurar que la constancia de conservación se genera de conformidad con los lineamientos que establece la Autoridad de Constancias de Conservación de Mensajes de Datos, mismos que se describen en la presente Declaración de Prácticas.

Por otro lado, se encuentra el componente a través del cual se proporciona a los suscriptores y partes interesadas la constancia de conservación, donde Incode ha

implementado un servicio web a través del cual se realiza la solicitud y respuesta de la emisión de la constancia de conservación de mensajes de datos.

6.2 Autoridad Certificadora Raíz Segunda de la Secretaría de Economía

De acuerdo con la Política de Certificados publicada por la Secretaría de Economía, su Autoridad Certificadora se define como:

"*La Autoridad Certificadora Raíz Segunda de la Secretaría de Economía es la colección de hardware, software y personal, que genera, firma y emite CDs de clave pública a sí misma, a su servicio de OCSP, a sus servicios adicionales de firma electrónica avanzada, a ACs de la DGNM y del Siger, a ACs de los PSCs, a las autoridades de servicios adicionales de firma electrónica avanzada de los PSCs, y a entidades de la SE de alto nivel, de acuerdo al Código de Comercio, el RPSC, las RGPSC, esta Política, y LFEA.*

"La ACR2-SE es responsable de la emisión y administración de CDs, incluyendo:

- *Generar los certificados;*
- *Publicar los certificados;*
- *Revocar los certificados;*
- *Generar y destruir las claves criptográficas de la ACR2-SE;*
- *Poner el certificado a disposición de las entidades, después de confirmar que éstas han reconocido formalmente sus obligaciones como se describe en el Código de Comercio, RPSC, RGPSC, y esta Política;*
- *Asegurar que todos los aspectos de los servicios, operaciones e infraestructura de la ACR2-SE relacionados con los CDs emitidos bajo esta Política de Certificados, se realicen de acuerdo con los requisitos de esta Política."*

6.3 Autoridad de Constancias de Conservación de Mensajes de Datos

La Autoridad de Constancias de Conservación de Mensajes de Datos de Incode es la encargada de la emisión de los tokens de Constancias de Conservación de Mensajes de Datos, la cual recibe la confianza de los suscriptores y partes interesadas del servicio de emisión de constancias de conservación. La Autoridad de Constancias de Conservación de Mensajes de Datos es la encargada de firmar los tokens de constancias de conservación con los Datos de Creación de Firma Electrónica Avanzada proporcionados por la Secretaría de Economía, además de ser la responsable de emitir constancias de conservación que sean identificables y puedan ser vinculados con la Política de Constancias de Conservación de Mensajes de Datos a través del OID asignado.

6.4 Suscriptores

Se reconocen como suscriptores del servicio de emisión de Constancias de Conservación de Mensajes de Datos a todos aquellos individuos u organizaciones que tienen un interés legítimo en la solicitud de constancias de conservación y que han completado el proceso de contratación contractual con Incode para poder acceder de forma recurrente al servicio.

Los suscriptores del servicio de emisión de Constancias de Conservación de Mensajes de Datos reconocen y aceptan las responsabilidades y obligaciones de la Autoridad de Constancias de Conservación de Mensajes de Datos, así como las

responsabilidades y obligaciones que asumen como usuarios del servicio y del uso de los tokens de Constancias de Conservación de Mensajes de Datos que solicitan y les son proporcionados.

6.5 Partes interesadas

Se reconocen como partes interesadas en el servicio de emisión de Constancias de Conservación de Mensajes de Datos a los suscriptores, receptores directos o indirectos de un token de constancias de conservación, así como a las autoridades que tienen un interés legítimo en el contenido de dicha constancia y su relación de integridad con el mensaje de datos respecto del cual fue emitida.

6.6 Constancias de Conservación de Mensajes de Datos

Una constancia de conservación de mensaje de datos es el elemento o evidencia que resulta de la implementación de procesos criptográficos dentro de un esquema de infraestructura de clave pública que tiene como finalidad validar o probar que un mensaje de datos se mantiene integro e inalterable con posterioridad a la emisión de la constancia de conservación.

En México, los Prestadores de Servicios de Certificación son los únicos entes acreditados para la emisión de constancias de conservación las cuales deben emitirse siguiendo los requerimientos que establece la NOM 151 y de conformidad con el RFC 3161.

7 Obligaciones y responsabilidades

Las obligaciones y responsabilidades asociadas con la operación, administración, gestión y consumo del servicio de constancias de conservación establecen de forma general la forma en que deben de interactuar los participantes de la emisión de constancias de conservación, así como los compromisos que adquieren al ser parte del ecosistema de la Autoridad de Constancias de Conservación de Mensajes de Datos.

Para el correcto desarrollo del servicio de constancias de conservación es fundamental que tanto Incode como los suscriptores y partes interesadas conozcan y acepten las obligaciones y responsabilidades que asumen, ya que al dar cumplimiento reducen el riesgo latente sobre el servicio y ayudan a mantener la percepción de confianza que los agentes externos tienen sobre este.

7.1 Por parte de Incode

7.1.1 Obligaciones

Las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación establecen las obligaciones que las organizaciones que se acreditan bajo esta figura deben cumplir y que tienen como objetivo generar procesos confiables para la generación de evidencia aplicable a las actuaciones que se realizan en medios electrónicos de conformidad con la normativa vigente.

Las obligaciones que adquiere Incode como Prestador de Servicios de Certificación del servicio de emisión de constancias de conservación de mensajes de datos:

a) Contar con los elementos económicos que se señalan en el Título Séptimo de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, como son el seguro de responsabilidad civil y fianzas.
b) Contar con instalaciones que implementen controles de acceso físico y cuenten con medidas de seguridad física.
c) Contar con centros procesamiento de datos que operen en forma redundante y en alta disponibilidad para garantizar el acceso al servicio.
d) Contar con los recursos humanos, económicos y tecnológicos necesarios para la operación del servicio de emisión de constancias de conservación de mensajes de datos.
e) Obtener la transferencia confiable de la escala de tiempo del Centro Nacional de Metrología para la emisión de constancias de conservación de mensajes de datos con una precisión de un segundo o mejor.

Por su parte las obligaciones que adquiere la Autoridad de Constancias de Conservación de Mensajes de Datos hacía sus suscriptores son las siguientes:

a) Poner a disposición de las partes interesadas la llave pública de los datos de creación de firma electrónica avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos.
b) Proporcionar un servicio de emisión de constancias de conservación de mensajes de datos confiable y consistente con los procedimientos descritos en la Declaración de Prácticas y la presente Política de Constancias de Conservación de Mensajes de Datos.
c) Brindar a los suscriptores soporte en el servicio de emisión de constancias de conservación de mensajes de datos de conformidad con los niveles de servicio establecidos en el contrato de servicios firmado.

7.1.2 Responsabilidades

Al poner a disposición de suscriptores y partes interesadas el servicio de emisión de conservación de mensajes de datos, Incode adquiere responsabilidades que buscan mantener la confianza que dichos actores depositan en el servicio. Parte de la confianza que se tiene en el servicio corresponde a los procedimientos de seguridad de la información que se implementan como Prestador de Servicios de Certificación y que están orientados en garantizar la integridad, confidencialidad y disponibilidad de los datos que se generan en el procesamiento de la solicitud y respuesta del servicio.

Las responsabilidades que adquiere Incode con los suscriptores del servicio de emisión de constancias de conservación de mensajes de datos son:

a) Proporcionar el servicio de emisión de conservación de mensajes de datos conforme a los lineamientos descritos en la Declaración de Prácticas y la presente Política de constancias de conservación de mensajes de datos.
b) Garantizar la integridad de la información durante el proceso de emisión la constancia de conservación.

c) Garantizar la confidencialidad de la información como parte del proceso de emisión la constancia de conservación.
d) Notificar oportunamente a los suscriptores y partes interesadas la presencia de incidentes de seguridad de la información en el servicio de emisión de constancias de conservación de mensajes de datos.
e) Manejar los datos sensibles de conformidad con los lineamientos que establece la Ley de Protección de Datos Personales en Posesión de Particulares.
f) Implementar controles de seguridad como parte de la operación de la Autoridad de constancias de conservación de mensajes de datos que permitan a los suscriptores y partes interesadas mantener la confianza en la emisión de constancias de conservación.
g) Poner a disposición de los suscriptores las guías técnicas y documentales de interoperabilidad para el desarrollo de los sistemas cliente del servicio de emisión de constancias de conservación de mensajes de datos.

Incode y su Autoridad de constancias de conservación de mensajes de datos no serán responsables, de manera enunciativa, mas no limitativa en los siguientes supuestos:

1. Suspensión de servicios por compromiso de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía.
2. Por los daños o afectaciones que puedan resultar derivados del mal uso o indebida implementación del servicio de emisión de constancias de conservación de mensajes de datos.
3. Por la emisión de constancias de conservación cuando la solicitud de dicha constancia no se integre con el hash del mensaje de datos respecto del cual se requiere la emisión.
4. Del resguardo de las constancias de conservación de mensajes de datos solicitadaspor sus suscriptores.
5. Por la interrupción temporal del servicio de emisión de constancias de conservación de mensajes de datos por causas ajenas a Incode y su Autoridad de constancias de conservación de mensajes de datos, como pueden ser:
    a. La interrupción de la transferencia de la escala de tiempo por situaciones de competencia del Centro Nacional de Metrología.

7.2 Por parte de los suscriptores

7.2.1 Obligaciones

Al contratar el servicio de emisión de constancias de conservación de mensajes de datos, los suscriptores de Incode adquieren y aceptan las obligaciones inherentes al consumo de dicho servicio. Las obligaciones que adquieren los suscriptores están orientadas a garantizar el correcto uso del servicio de emisión de constancias de conservación de mensajes de datos, así como la implementación de procesos de verificación y de resguardo de la integridad de la información en el tramo de control del suscriptor, es decir dentro de sus propios sistemas.

Las obligaciones que adquieren los suscriptores del servicio de emisión de constancias de conservación de mensajes de datos son:

1. Verificar que Incode es un Prestador de Servicios de Certificación acreditado ante la Secretaría de Economía para el servicio de emisión de constancias de conservación de mensajes de datos.
2. Validar que el certificado de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode se encuentra vigente y no ha sido revocado, lo cual podrá consultar en la página de firma digital de la Secretaría de Economía.
3. Conocer los procedimientos asociados a la emisión de constancias de conservación de mensajes de datos, como son la Política del servicio y la Declaración de Prácticas.
4. Notificar a Incode cuando se tenga conocimiento o se presuma que las credenciales de acceso al servicio estan siendo utilizadas por terceros no autorizados.
5. Verificar la concordancia entre el hash que se incluye como parte de la solicitud de la constancias de conservación de mensajes de datos, contra el que se integra como parte de la constancia.
6. Realizar el pago del servicio de constancias de conservación de mensajes de datos de conformidad con el contrato de prestación de servicio.
7. Utilizar las constancias de conservación de mensajes de datos de conformidad con el alcance que establece Incode para su uso.

7.2.2 Responsabilidades

Además de las obligaciones que se adquieren al contratar el servicio de emisión de constancias de conservación de mensajes de datos, los suscriptores también adquieren responsabilidades relacionadas con el mismo.

Las responsabilidades que adquieren los suscriptores del servicio de emisión de constancias de conservación de mensajes de datos son:

1. Resguardar adecuadamente las credenciales de acceso al servicio de emisión de constancias de conservación de mensajes de datos.
2. Generar la solicitud de constancia de conservación de acuerdo con los lineamientos que establece la documentación para la implementación de los sistemas cliente.
3. Para la generación de la solicitud de constancia de conservación se deberá utilizar el algoritmo criptográfico que establece Incode dentro de su guía técnica de implementación, mismo que es establecido por la Secretaría de Economía.
4. Verificar que la constancias de conservación de mensajes de datos haya sido firmado correctamente con los Datos de Creación de Firma Electrónica de la Autoridad de constancias de conservación de mensajes de datos de Incode.
5. Resguardar las constancias de conservación de mensajes de datos que son emitidos por la Autoridad de constancias de conservación de mensajes de datos como parte del proceso de solicitud que realizan.
6. Resguardar la integridad del mensaje de datos sobre el cual se solicita la emisión de la constancia de conservación de mensajes de datos.

7.3 Por las partes interesadas

7.3.1 Obligaciones

Las partes que confían en el servicio de emisión de constancias de conservación de mensajes de datos, cuando reciben una constancia de conservación, tienen las siguientes obligaciones:

a. Verificar que dentro de la constancia de conservación de mensajes de datos se integre la cadena de certificación que permita validar los Datos de Creación de Firma.
b. Obtener de manera segura el certificado de la Autoridad de constancias de conservación de mensajes de datos para poder realizar la verificación del token.
c. Verificar que el token este correctamente firmado por la Autoridad de constancias de conservación de mensajes de datos de Incode.
d. Verificar la vigencia de los Datos de Creación de Firma Electrónica Avanzada de la Autoridad de constancias de conservación de mensajes de datos al momento de la emisión del token.
e. Verificar que la constancia de conservación de mensajes de datos corresponde al hash respecto del cual se realizó la solicitud.

7.3.2 Responsabilidades

Las partes que confían en el servicio de emisión de constancias de conservación de mensajes de datos, cuando reciben una constancia de conservación, tienen las siguientes responsabilidades:

a. Considerar las limitaciones para el uso de las constancias de conservación de mensajes de datos que se establecen en la Política de constancias de conservación de mensajes de datos.
b. Administrar los procesos de gestión y almacenamiento de las constancias de conservación de mensajes de datos, así como de los mensajes de datos sobre los cuales se emitieron dichas constancias.

8 Requerimientos de las Prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos

Los requerimientos de las prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos tienen como objetivo establecer la ejecución de controles de seguridad que permitan mantener la fiabilidad en la operación de la Autoridad conforme a las disposiciones generales de operación del servicio de emisión de constancias de conservación.

En ese sentido, la emisión de constancias de conservación requiere del establecimiento de un vínculo contractual entre los suscriptores e Incode, como Autoridad de Constancias de Conservación de Mensajes de Datos, quienes se obligarán a cumplir con las condiciones del servicio que se establecen como parte del funcionamiento de la plataforma a través de los términos y condiciones que

deberán ser dados a conocer por Incode y aceptados por el suscriptor y partes interesadas.

8.1 Declaración de prácticas de la Autoridad de Constancias de Conservación de Mensajes de Datos

Incode como operador de su Autoridad de Constancias de Conservación de Mensajes de Datos ha demostrado que los mecanismos e infraestructura que tiene implementados para el procesamiento de información son confiables y que garantizan la integridad, confidencialidad y disponibilidad de la información durante el proceso.

La fiabilidad del servicio y del proceso se expresa con la acreditación que otorga la Secretaría de Economía a Incode para operar como Prestador de Servicios de Certificación para el servicio de emisión de constancias de conservación. Entre los elementos, acciones y prácticas que han permitido a Incode obtener dicha acreditación, se encuentran:

1. La identificación de riesgos asociados a la prestación del servicio, así como la descripción de los controles de seguridad que se implementan para su mitigación.
2. El diseño e implementación de un Plan de Continuidad de Negocio y Recuperación ante Desastres el cual permite reactivar el servicio a la brevedad en caso de la presencia de alguna incidencia.
3. Se establece una Política de Seguridad Física la cual tiene como objetivo asegurar las instalaciones de procesamiento de datos y de operación administrativa.
4. Se implementa un Política de Seguridad de la Información para establecer los lineamientos y objetivos generales que ha definido Incode para asegurar el servicio de Constancias de Conservación de Mensajes de Datos.
5. Emite las Constancias de Conservación de Mensajes de Datos de conformidad con los requerimientos de la NOM 151.

Ahora bien, en relación con la Presente Declaración de Prácticas define una serie de acciones que debe ejecutar durante la operación del servicio y que contribuyen a mantener la fiabilidad en el servicio. Entre las acciones que se implementa se encuentran:

a. Incode como Prestador de Servicios de Certificación deberá de dar aviso a la Secretaría de Economía respecto de la intención de realizar modificaciones en su Declaración de Prácticas o Política de Constancias de Conservación de Mensajes de Datos. Deberá notificar a las partes interesadas los cambios realizados una vez que la Secretaría de Economía autorice las modificaciones.
b. Como parte de la operación de la Autoridad de Constancias de Conservación de Mensajes de Datos se establece un calendario de revisiones de la Declaración de Prácticas.

c. Identifica las obligaciones y responsabilidades de los suscriptores y partes interesadas en el servicio de emisión de constancias de conservación y las hace de su conocimiento.
d. Establece procedimientos de concientización a los colaboradores de Incode para reafirmar su participación en la consecución de los objetivos señalados en la Política de Seguridad de la Información.
e. Pone a disposición de sus suscriptores y partes interesadas la Política y Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos.
f. Hace de conocimiento de sus suscriptores y partes interesadas los términos y condiciones bajo los cuales se proporciona el servicio.
g. El Profesional Informático de Incode es el encargado de asegurar el cumplimiento de todos los procesos y medidas de seguridad que se tienen definidos para el servicio.

8.2 Prácticas de divulgación de la Autoridad de Constancias de Conservación de Mensajes de Datos

Incode pone a disposición de sus suscriptores y partes interesadas la información de contacto referente al servicio de emisión de constancias de conservación, así como de los términos y condiciones de dicho servicio además de la información relevante y que pueda ser de interés.

8.2.1 Ubicación de oficinas

Incode estableces las oficinas administrativas de atención a clientes, partes interesadas y autoridades, para el servicio de emisión de constancias de conservación de mensajes de datos en: Av. Río San Joaquín 498, Piso 2, Suites 11 y 13, Colonia Ampliación Granada, Ciudad de México, C.P. 11529.

Dentro de las oficinas administrativas se ejecutan los procesos relacionados con la administración, comercialización, marketing y actividades jurídicas relacionadas con el servicio de emisión de constancias de conservación de mensajes de datos, no así el procesamiento de datos el cual se lleva a cabo en los centros de datos que ha establecido Incode.

Incode pone a disposición de los interesados en el servicio, los siguientes datos de contacto:

1. **Página de internet:** https://psc.incode.com
2. **Correo de contacto:** psc@incode.com

8.2.2 Términos y condiciones del servicio de constancias de conservación

Incode pone a disposición de suscriptores, partes interesadas y autoridades los términos y condiciones que establecen el funcionamiento del servicio y las características y mecanismos a través de los cuales se ofrece a sus usuarios. Los términos y condiciones del servicio se encuentran disponibles para su consulta en la página de internet de Incode, además de que serán dados a conocer y deberán de

ser aceptados por los suscriptores como parte del proceso de contratación del servicio.

8.2.3 Política de Privacidad

Las organizaciones que procesan cualquier tipo de información de sus clientes por cualquier medio están obligadas en términos de la Ley Federal de Protección de Datos Personales en Posesión de Particulares a dar a conocer a sus usuarios el tratamiento que se dará a su información una vez que se encuentre en poder de la organización. En ese sentido, Incode pone a disposición de sus usuarios y partes interesadas el aviso de privacidad correspondiente al servicio de emisión de Constancias de Conservación de Mensajes de Datos.

El aviso de privacidad se encuentra disponible para su consulta en la página de internet de Incode, además de que será dado a conocer y deberá de ser aceptado por los suscriptores como parte del proceso de contratación del servicio.

URL del aviso de privacidad:

https://psc.incode.com/legales/aviso-de-privacidad.html

8.2.4 Algoritmo criptográfico para la emisión del hash para la solicitud de la CCMD

Con relación a los servicios que ofrece Incode, en este caso la emisión de constancias de conservación de mensajes de datos es la Secretaría de Economía de conformidad con la NOM 151, la autoridad encargada de establecer el algoritmo criptográfico que deberá ser utilizado como parte del proceso.

Al respecto, la Secretaría de Economía en su página de internet dedicada a los Prestadores de Servicios de Certificación, establece que el algoritmo criptográfico que se deberá de utilizar para la emisión de constancias de conservación de mensajes de datos es el SHA256. En caso de requerir un cambio en el algoritmo por cuestiones de seguridad, la Secretaría notificará a Incode para que realice los ajustes correspondientes a sus procesos y extienda la notificación a sus suscriptores y partes interesadas.

URL de la designación del algoritmo criptográfico por la Secretaría de Economía:

https://psc.economia.gob.mx/marco_juridico.html

8.2.5 Precisión la Constancia de Conservación de Mensajes de Datos

De conformidad con la NOM 151 las constancias de conservación de mensajes de datos que emiten los Prestadores de Servicios de Certificación deben de atener a los lineamientos que se describen en el estándar conocido como RFC 3161 conocido como "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*".

Dentro de los lineamientos que establece dicho estándar destaca que, atendiendo a que las constancias de conservación buscan garantizar la integridad de un mensaje de datos con posterioridad a la emisión de dicha constancia resulta fundamental establecer la precisión con la cual son emitidas para permitir a las partes interesadas ubicar en el tiempo el momento de su emisión.

En ese sentido, Incode establece que sus constancias de conservación de mensajes de datos son emitidas, considerando la sincronía de la escala de tiempo con el Centro Nacional de Metrología, con una precisión de un segundo o mejor.

URL de consulta del RFC 3161:

https://www.ietf.org/rfc/rfc3161.txt

8.2.6 Alta disponibilidad del servicio

Las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación establecen que los acreditados deberán contar con una infraestructura de alta disponibilidad para la provisión de sus servicios a suscriptores y partes interesadas. Al respecto, Incode cuenta con una infraestructura desplegada en dos diferentes regiones de procesamiento de cómputo en la nube, donde la región principal cuenta con una implementación redundante en dos diferentes zonas de disponibilidad las cuales cuentan con una configuración activo-activo que gestiona las operaciones a través de un balanceador de cargas.

Este despliegue tecnológico permite garantizar a los suscriptores y partes interesadas que el servicio de constancias de conservación de mensajes de datos se encontrará disponible el 99.5% de tiempo.

9 Ciclo de vida de los módulos criptográficos

Las implementaciones de infraestructura de clave pública establecen en gran medida su seguridad en el uso de módulos criptográficos que son los equipos encargados de resguardar la información de los Datos de Creación de Firma Electrónica, en este caso, de la Autoridad de Constancias de Conservación de Mensajes de Datos. Incode despliega su Autoridad de Constancias de Conservación de Mensajes de Datos con un proveedor de servicios de cómputo en la nube, en este caso AWS, donde hace uso de los módulos criptográficos denominados CloudHSM, los cuales están basados en HSM físicos certificados bajo el estándar FIPS 140-2 nivel 3.

Como todo equipo o componente de infraestructura los módulos criptográficos requieren del establecimiento de un proceso de gestión de su ciclo de vida que permita mantener un rendimiento óptimo de cada uno de los componentes

El ciclo de vida de los módulos criptográficos utilizados por Incode está integrado por las siguientes fases:

1. Habilitación del HSM
    a. Creación de un clúster
    b. Creación de una instancia de HSM
    c. Autenticar el clúster de HSM
    d. Configurar la operación del HSM
2. Administración y operación
3. Respaldo del HSM
4. Recuperación del HSM
5. Eliminación del HSM

El detalle del ciclo de vida de los módulos criptográficos de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode puede consultarse en el documento del "*Plan de Administración de Claves*".

10 Ciclo de vida de los Datos de Creación de Firma Electrónica Avanzada de la ACCMD

Se conoce como ciclo de vida de los Datos de Creación de Firma Electrónica Avanzada o llaves criptográficas de la Autoridad de Constancias de Conservación de Mensajes de Datos, al periodo de vigencia en el que dichas llaves son válidas jurídicamente para su uso. El ciclo de vida de las llaves criptográficas además del periodo de vigencia considera el estatus de dichas llaves al momento en que pretender ser utilizadas evitando generar cualquier constancia de conservación si dichas llaves han sido revocadas o canceladas por cualquiera que sea el motivo.

Las llaves criptográficas de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode son emitidas por la Secretaría de Economía y subordinadas a su Autoridad Certificadora Raíz y tienen como objetivo la emisión de constancias de conservación de mensajes de datos.

10.1 Gestión del ciclo de vida de los datos de creación de firma

Los certificados digitales que son emitidos como Datos de Creación de Firma Electrónica de la Autoridad de Constancias de Conservación de Mensajes de Datos están sujetos a procedimientos que delimitan el ciclo de vida de estos, donde se puede establecer con toda certeza que dichos certificados son válidos y permiten la emisión de Constancias de Conservación de Mensajes de Datos.

En ese sentido, Incode PSC a fin de simplificar la gestión administrativa de la información relacionada con los datos de creación de firma electrónica de su Autoridad de Constancias de Conservación de Mensajes de Datos establece que el ciclo de vida de su certificado estará compuesto por las siguientes etapas:

1. Generación de los Datos de Creación de Firma
2. Gestión del certificado
3. Fin del ciclo de vida de los Datos de Creación de Firma

10.1.1 Generación de las llaves de la ACCMD

Los Datos de Creación de Firma Electrónica de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode se llevó a cabo a través de un procedimiento que se conoce como "Ceremonia de generación de los Datos de Creación de Firma" donde Incode como administrador de la infraestructura de clave pública, genera el requerimiento de emisión de un certificado digital y, posteriormente el propio certificado, a través del cual brindarán el servicio de emisión de constancias de conservación de mensajes de datos. Como parte del proceso se tiene la presencia del personal de la Autoridad Certificadora Raíz que estará firmando el certificado y quienes tienen la función de auditar que tanto el certificado, como el

servicio que se prestará, cuenten con las condiciones necesarias de seguridad para un servicio de confianza.

10.1.1.1 Generación del requerimiento y llave privada

La generación del requerimiento y llave privada para la generación de los Datos de Creación de Firma Electrónica se lleva a cabo dentro de los módulos criptográficos, ubicados dentro de las áreas seguras de regiones de procesamiento de cómputo en la nube, que forman parte de la infraestructura de Incode. Para la generación del requerimiento de los datos de creación de firma electrónica de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode se consideraron los datos señalados para cada uno de los atributos del certificado de conformidad con el apartado nueve de la "Política de Certificados de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía".

En ese sentido los atributos del Distinguished Name del campo de Emisor, considerando a la Autoridad Certificadora Raíz de la Secretaría de Economía, utilizará los siguientes datos:

E= acr2se@economia.gob.mx
O= Secretaría de Economía
OU= Dirección General de Normatividad Mercantil
CN= Autoridad Certificadora Raíz Segunda de Secretaría de Economía
C= MX
Street= Insurgentes Sur 1940, Col. Florida
PostalCode= 01030
ST= Ciudad de México
L= Álvaro Obregón

Ahora bien, el Distinguished Name para el campo del Sujeto, en este caso Incode, para la región de Frankfurt, utilizará los siguientes datos:

O= Incode
OU= Incode PSC Frankfurt
CN= Autoridad de Constancias de Conservación de Mensajes de Datos de Incode PSC
C= MX
Street= Av Rio San Joaquin 498 Ampliacion Granada
PostalCode= 11529
ST= Ciudad de México
L= Miguel Hidalgo

Por su parte, el Distinguished Name para el campo del Sujeto para la región de Milán, utilizará los siguientes datos:

O= Incode
OU= Incode PSC Milán
CN= Autoridad de Constancias de Conservación de Mensajes de Datos de Incode PSC

C= MX
Street= Av Rio San Joaquin 498 Ampliacion Granada
PostalCode= 11529
ST= Ciudad de México
L= Miguel Hidalgo

Para los datos de vigencia del certificado de la ACCMD de Incode, la Secretaría de Economía determinó que serían emitidos con una vigencia de siete años considerando que el certificado de la Autoridad Certificadora Raíz Segunda de la Secretaría de Economía tiene fecha de fin de vigencia del 07 de febrero de 2032.

En este proceso también se genera la llave privada de los Datos de Creación de Firma Electrónica Avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode, la cual se genera y resguarda directamente en el módulo criptográfico presentado.

10.1.1.2 Generación de la llave pública del certificado

Una vez que se generó el requerimiento para la emisión del certificado y el mismo fue entregado al personal asistente por parte de la Secretaría de Economía quienes de conformidad con su propio procedimiento llevaron a cabo la generación de la llave pública de los datos de creación de firma.

Concluido el proceso de emisión de la llave pública del certificado, dicha llave es entregada al personal de confianza de Incode quien lo integra a la infraestructura de la Autoridad de Constancias de Conservación de Mensajes de Datos.

10.2 Gestión del certificado

10.2.1 Almacenamiento del certificado

Los servicios de un Prestador de Servicios de Certificación son considerados como servicios de confianza que brindan a los interesados en el servicio, en este caso la emisión de constancias de conservación de mensajes de datos, la evidencia calificada que les permitirá demostrar de manera fehaciente que un mensaje de datos no ha sido alterado o modificado con posterioridad a la emisión de la constancia, es decir, que se mantiene integro. Por ello, es fundamental que se implementen controles y mecanismos de seguridad que permitan asegurar que los Datos de Creación de Firma de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode PSC podrá garantizar la confianza que sus clientes, suscriptores y partes interesadas depositan en su servicio.

En ese sentido, atendiendo a la fracción VII de la Regla 165 de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, así como con relación al apartado 7.2.2 del ETSI de referencia, Incode PSC para el resguardo y almacenamiento de los Datos de Creación de Firma electrónica que le han sido emitidos por la Secretaría de Economía cuenta con tres HSM que son compatibles con el estándar FIPS 140-2 nivel 3.

10.2.2 Longitud de llave de los Datos de Creación de Firma

La longitud de clave que se utiliza para la Autoridad de Constancias de Conservación de Mensajes de Datos es de 4096, además de utilizar SHA 256 con RSA como algoritmo de firmado. En ese sentido, Incode se ha asegurado que su HSM cuente con la funcionalidad y sea compatible condicha longitud de clave y algoritmos de firma.

La longitud de las claves de la Autoridad de Constancias de Conservación de Mensajes de Datos podrá modificarse y actualizarse conforme a la longitud que establezca la Secretaría de Economía, previo comunicado, cuando los avances tecnológicos así lo requieran.

10.2.3 Algoritmo criptográfico

De conformidad con los criterios publicados por la Secretaría de Economía en la página de internet de Firma Digital, el algoritmo criptográfico que deberá utilizarse en la emisión de los datos de creación de firma electrónica avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos será SHA256.

10.2.4 Distribución de la llave Pública

Incode de conformidad con las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación y con las buenas prácticas relacionadas con la implementación de servicios basados en infraestructura de clave pública pone a disposición de suscriptores y partes interesadas la clave pública de los Datos de Creación de Firma Electrónica Avanzada de su Autoridad de Constancias de Conservación de Mensajes de Datos en su página de internet.

La llave pública permitirá a las partes interesadas verificar que el token de constancias de conservación fue emitido por una Autoridad de Constancias de Conservación de Mensajes de Datos autorizada por la Secretaría de Economía, además de verificar que al momento de la emisión de la constancia de conservación los Datos de Creación de Firma de la Autoridad de Constancias de Conservación de Mensajes de Datos se encontraban vigentes.

Adicionalmente, las partes interesadas podrán obtener la llave pública de los Datos de Creación de Firma Electrónica Avanzada del directorio publicado en la página de internet que la Secretaría de Economía dedica a los Prestadores de Servicios de Certificación.

URL de consulta de la llave pública en la página de Incode:

https://psc.incode.com/repositorio-de-confianza/

URL de consulta de la llave pública en el directorio de la Secretaría de Economía:

https://psc.economia.gob.mx/directorio.html

10.3 Fin del ciclo de vida de las llaves de la ACCMD

Incode establece que se alcanzará el fin de ciclo de vida de los Datos de Creación de Firma Electrónica Avanzada de su Autoridad de Constancias de Conservación de

Mensajes de Datos cuando las condiciones de seguridad u operación no permitan garantizar a suscriptores, partes interesadas y autoridades que el servicio de emisión de constancias de conservación se emite bajo un ecosistema seguro y confiable, que es la finalidad de implementaciones de infraestructura de clave pública como es el caso. Otro criterio bajo el cual se puede afirmar el fin del ciclo de vida de las claves es cuando se alcanza el periodo de vigencia por el cual fueron emitidos por la Autoridad Certificadora de la Secretaría de Economía.

En general, Incode afirma que se puede alcanzar el fin del ciclo de vida de sus llaves criptográficas en las siguientes circunstancias:

1. Fin del periodo de vigencia.
2. Revocación de claves (Compromiso de los datos de creación de firma, perdida de la contraseña, terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos).
3. Algoritmos criptográficos obsoletos o no seguros.
4. Longitud de claves no segura.
5. Procesos de recuperación no exitosos en la falla de un módulo criptográfico.
6. Sanciones por parte de la Secretaría (Temporales o permanentes).

11 Objetivos de seguridad de la información

Incode considera que, si bien los objetivos de las diversas áreas operacionales son importantes, son los objetivos de seguridad de la información de la organización los que le permiten brindar elementos para que cada una de las áreas pueda lograr las metas planteadas y alcanzar sus objetivos.

Incode como objetivo principal de Seguridad de la Información establece que se deberá mantener la integridad, confidencialidad y disponibilidad de la información en cualquiera de los procesos implementados, principalmente para la emisión de constancias de conservación de mensajes de datos.

Ahora bien, para alcanzar este objetivo general de la organización, se plantean los siguientes objetivos:

1. Esta política considera todos los sistemas, los datos y las redes de comunicación de Incode implementados en las instalaciones propiedad de la empresa; infraestructuras de nube privada, híbrida y/o pública, además de todos otros activos de tecnologías de Incode.
2. Está Política busca fomentar los principios de seguridad de la información organizacionales entre los colaboradores generando dinámicas de concientización.
3. Implementación exitosa de un Sistema de Gestión de Seguridad de la Información.
4. El departamento de Seguridad y Cumplimiento definirá los procesos y procedimientos de seguridad que se seguirán al interior de Incode.
5. El departamento de Seguridad y Cumplimento definirá los sistemas de software y sistemas especializados para reducir las amenazas seguridad de la

información y realizará periódicamente pruebas de penetración y otros métodos que permitan conocer el nivel de implementación de los controles de seguridad.

6. El departamento de Seguridad y Cumplimiento elaborará y documentará los planes de seguridad de la información de Incode y los dará a conocer a los empleados de la empresa.
7. El departamento de Seguridad y Cumplimiento utilizando las herramientas y procedimientos definidos realizará una evaluación periódica de riesgos y amenazas para la operación de sus sistemas.
8. El departamento de Seguridad y Cumplimiento establecerá programas de capacitación que permitan a los empleados de Incode conocer diversos riesgos de seguridad, entre los que destacan los ataques de phishing. Estas capacitaciones vendrán acompañadas de una campaña de concientización a los empleados respecto de su papel en la seguridad de la información de Incode.
9. Incode implementa procesos que le permiten identificar posibles brechas de seguridad dentro de sus procesos, así como determinar la naturaleza y origen de dichas vulnerabilidades a fin de notificar a la Alta Dirección y los dueños de los procesos afectados.
10. Incode como parte de sus programas de capacitación implementará programas de educación y concientización en ciberseguridad.
11. Incode como parte de sus controles de seguridad incluirá los Planes de Continuidad de Negocio y Recuperación ante Desastres.
12. El departamento de Seguridad y Cumplimiento definirá como se llevará a cabo el reporte y manejo de incidentes relacionados con la seguridad de la información.
13. La información en propiedad o custodia de Incode, deberá de contar con mecanismos de control y seguridad que permitan garantizar su integridad. Incode buscará que dicha información, cuando sea viable, se encuentre encriptada.
14. Como parte del proceso de contratación el personal de Incode deberá de firmar el código de conducta, convenio de confidencialidad, así como las políticas de seguridad de la información aplicables a Incode.
15. El departamento de Seguridad y Cumplimiento se asegurará que todas las Políticas y procedimientos asociados con la seguridad de la información se implementen de conformidad con las leyes, reglamentos, normas y estándares aplicables.
16. Cualquier cambio propuesto a la presente Política de Seguridad de la Información deberá de ser documentado como parte de la Información documentada del Sistema de Gestión de Seguridad de la Información.
17. Incode establece una política específica para la seguridad de la información de su Autoridad de Constancias de Conservación de Mensajes de Datos.
18. Incode establece una política específica para la seguridad de la información de su Autoridad de Constancias de Conservación de Mensajes de Datos

19. Incode establecerá con claridad las obligaciones y responsabilidades de sus suscriptores y partes interesadas en el servicio de emisión de constancias de conservación de mensajes de datos.
20. Incode dará a conocer a sus suscriptores y partes interesadas en el servicio de emisión de constancias de conservación de mensajes de datos, los mecanismos de seguridad aplicables al servicio, mismos que deberán de ser reconocidos y aceptados.
21. Incode deberá implementar mecanismos y procedimientos de seguridad que permitan asegurar y proteger los Datos de Creación de Firma Electrónica Avanzada de su Autoridad de Constancias de Conservación de Mensajes de Datos.
22. Incode pondrá a disposición de sus suscriptores y partes interesadas una Declaración de Prácticas del servicio de emisión de constancias de conservación de mensajes de datos donde se establecerán con claridad las generalidades del servicio.
23. Incode implementará mecanismos de monitoreo continuo sobre su servicio de emisión de constancias de conservación de mensajes de datos a fin de identificar comportamientos no comunes y amenazas a la prestación del servicio.
24. La Autoridad de Constancias de Conservación de Mensajes de Datos restringirá la comunicación de sus componentes de infraestructura únicamente a aquellos recursos que estan dentro la red interna de Incode. Los módulos criptográficos implementados por Incode únicamente tendrán comunicación con la Autoridad de Constancias de Conservación de Mensajes de Datos.
25. Inconde emitirá constancias de conservación de mensajes de datos de conformidad con la NOM-151-SCFI-2016.
26. Incode habilitará a sus suscriptores y partes interesadas en su servicio de emisión de constancias de conservación de mensajes de datos la consulta segura de la llave pública de sus datos de creación de firma electrónica avanzada para la verificación de las constancias emitidas.
27. Incode se mantendrá la conformidad de su Constancias de Conservación de Mensajes de Datos con las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación y demás legislación aplicable.

12 Constancia de Conservación de Mensajes de Datos

12.1 Origen de la escala de tiempo

Para la emisión de constancias de conservación a través de su Autoridad de Constancias de Conservación de Mensajes de Datos, Incode obtiene del Centro Nacional de Metrología la transferencia segura de la escala de tiempo. La escala de tiempo que se integra como parte de las constancias de conservación se establece en formato UTC lo que evita que se tenga que realizar alguna adecuación o interpretación respecto del huso horario en el que se emite.

12.2 Contratación del servicio de emisión de constancias de conservación de mensajes de datos

Para la contratación del servicio de constancias de conservación de mensajes de datos, las partes interesadas en convertirse en suscriptores deberán de solicitar la cotización correspondiente conforme al volumen de constancias de conservación que requieran, tras lo cual Incode emitirá la correspondiente cotización la cual tendrá una validez de 30 días naturales.

En caso de estar conforme con la cotización, el interesado deberá notificar su aceptación a Incode quien solicitará una serie de datos y documentos para la integración del contrato de prestación de servicios. Una vez que se integra el contrato se envía para revisión y firma con el solicitante y cuando se completa el proceso de firmado Incode procede a la generación de la cuenta de usuario y la emisión del token de autenticación al sistema.

12.3 Servicio de emisión de una Constancia de Conservación de Mensaje de Datos

Las Constancias de Conservación de Mensajes de Datos que emite Incode como Prestador de Servicios de Certificación se emiten de conformidad con los requerimientos que establece el RFC 3161, está diseñado como un sistema transaccional donde a partir de una solicitud se realiza el procesamiento de los parámetros que se reciben para poder entregar una respuesta conforme a los criterios señalados como parte de la documentación del servicio que le fue proporcionada al solicitante.

Para ello, Incode desarrollo un API (Application Programming Interface) específica para su servicio de emisión de constancias de conservación de mensajes de datos, la cual tiene como objetivo recibir peticiones de constancias de conservación y devolver una respuesta a dicha petición. Esta API es compartida con los clientes y suscriptores del servicio que requieren integrar las constancias de conservación en sus procesos de negocio. Es relevante señalar que es responsabilidad de los usuarios y clientes el desarrollo e integración del sistema cliente para el consumo del servicio de emisión de constancias de conservación de mensaje de datos.

Es importante mencionar que el servicio de emisión de constancias de conservación de mensajes de datos de Incode cuenta con mecanismos de seguridad que restringen el acceso a la emisión de constancias de conservación a aquellos suscriptores o clientes, sean personas físicas o personas morales, que hayan culminado el proceso de contratación del servicio. Una vez que se concluye el proceso de contratación, a través de sus representantes legales, se le entregarán los accesos correspondientes al servicio, así como los manuales de implementación.

Finalmente, resulta necesario establecer la conformidad de la Autoridad de Constancias de Conservación de Mensajes de Datos con la NOM-151-SCFI-2016 por lo cual la Autoridad de Incode da cumplimiento a lo siguiente:

1. Basa su estructura y conformación en el estándar descrito en el RFC 3161.

2. Utiliza una fuente confiable de tiempo, en este caso el Centro Nacional de Metrología, conforme a las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.
3. Incluye un valor de tiempo confiable en cada una de las constancias de conservación de mensajes de datos que emite.
4. Incluye un identificador único para cada una de contancias de conservación de mensajes de datos emitidas.
5. Genera un token de constancia de conservación al recibir una solicitud válida por parte de los suscriptores.
6. Incluye en cada constancia de conservación de mensaje de datos el OID de la Política de Constancias de Conservación de Mensajes de Datos.
7. Genera la constancia de conservación a partir del hash del mensaje de datos, el cual se genera utilizando un algoritmo de "una sola dirección" el cual es identificable por un OID.
8. Examina el OID del algoritmo utilizado para la generación del hash y verifica que la longitud del hash que se solicita estampar coincida con la descripción del OID.
9. No inlcuye datos de identificación del suscriptor solicitante la constancia de conservación de mensaje de datos.
10. Firma cada una de las constancias de conservación con los Datos de Creación de Firma Electrónica emitidos con el propósito específico de la Autoridad de Constancias de Conservación de Mensajes de datos.

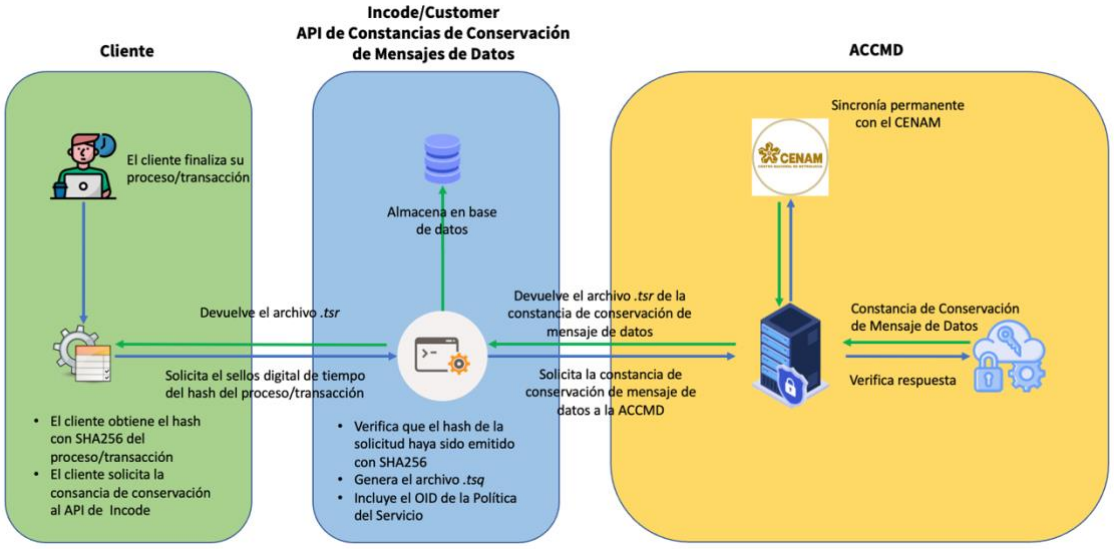

Imagen 1 Proceso de emisión de una constancia de conservación de mensajes de datos

12.3.1 Endpoint del servicio de emisión de constancias de conservación

El servicio de emisión de constancias de conservación de mensajes de datos será proporcionado por Incode a sus suscriptores y partes interesadas a través del endpoint que para dichos fines se ha dispuesto, mismo que será entregado a los interesados al momento de la contratación del servicio.

12.3.2 Parámetros del servicio de emisión de una constancia de conservación

Para la emisión de una constancia de conservación de mensajes de datos es necesario que el solicitante integre dentro de su solicitud los siguientes parámetros:

1. Hash del mensaje de datos sobre el cual se quiere emitir la constancia de conservación. El hash que se envía como parámetro de la solicitud deberá de haber sido generado utilizando el algoritmo criptográfico SHA256, de lo contrario la solicitud devolverá un mensaje de error de conformación.
2. OID. Se debe de proporcionar el OID de la Política del Servicio proporcionado por la Secretaría de Economía, el cual será proporcionado a los clientes una vez que concluyen su proceso de contratación. En caso de que se incluya un OID incorrecto el servicio regresará un mensaje de error.

12.3.3 Seguridad en el proceso de emisión de una Constancias de Conservación de Mensajes de Datos

Además de los controles de seguridad físicos y lógicos que se implementan para el resguardo de la infraestructura de su Autoridad de Constancias de Conservación de Mensajes de Datos, Incode considera medidas de seguridad adicionales para el servicio web a través del cual presta el servicio a sus suscriptores.

Entre las medidas de seguridad específicas del servicio se encuentra la autenticación vía certificado digital entre la API de servicios que se expone a los suscriptores y la Autoridad de Constancias de Conservación de Mensajes de Datos, de esta forma Incode se asegura que únicamente se emitirán constancias de conservación respecto de las peticiones que provengan de las instancias de sus servicios web que han sido publicadas y autenticadas a través de este mecanismo.

En caso de no autenticarse correctamente la instancia que solicita la emisión de una constancia, la Autoridad de Constancias de Conservación de Mensajes de Datos descarta la solicitud recibida y retorna un mensaje de error. El Profesional Informático es el encargado de configurar los certificados de autenticación necesarios para cada una de las instancias que ejecutan el API de servicios a fin de garantizar la seguridad en el proceso de emisión de las constancias de conservación de mensajes de datos.

Ahora bien, para el consumo del servicio por parte de los suscriptores se tiene implementado un sistema de autenticación basado en credenciales de usuario las cuales están compuestas por un usuario y contraseña.

Dichas credenciales de usuario son entregadas a los suscriptores una vez que se concluye el proceso de contratación del servicio de emisión de constancias de conservación de mensajes de datos. Como parte de la entrega de las credenciales de usuario, Incode hace del conocimiento de los suscriptores su responsabilidad en el resguardo de los datos de autenticación, siendo responsables del correcto uso, resguardo y almacenamiento para el acceso al servicio de emisión de constancias de conservación. En ese sentido, los suscriptores son responsables de notificar a Incode el compromiso o mal uso de sus credenciales de acceso para lo cual Incode

procederá a la revocación de dichas credenciales de usuario y a la generación de nuevas credenciales.

Finalmente, resulta relevante mencionar que, como parte final de la entrega a los suscriptores de las credenciales de autenticación, estos deberán de firmar la recepción de dichas credenciales, además del documento de obligaciones y responsabilidades relacionadas con el servicio de emisión de constancias de conservación de mensajes de datos.

12.3.4 Controles de registro auditoria y de seguridad

Además de los mecanismos de autenticación que implementa Incode para las interacciones con su API de emisión de constancias de conservación, así como su comunicación con la Autoridad de Constancias de Conservación de Mensajes de Datos, también se tienen implementadas diversas herramientas que permiten establecer controles adicionales de monitoreo y de seguridad con los cuales se busca asegurar la integridad del servicio de emisión de constancias de conservación de mensajes de datos. Entre las herramientas de registro de auditoría y seguridad que se tienen implementadas se encuentran:

1. Sistemas de monitoreo de red
    a. Amazon CloudWatch
    b. AWS X-Ray
    c. AWS CloudTrail
2. Antivirus
    a. Trend Micro
3. Herramientas para la detección de vulnerabilidades
    a. Amazon Inspector
4. Firewall
5. Detección y protección contra intrusiones
    a. Amazon GuardDuty

El detalle de los controles de seguridad dentro del Plan de Seguridad de Sistemas de la Autoridad de Constancias de Conservación de Mensajes de Datos.

12.4 Proceso de emisión de una constancia de conservación de mensajes de datos

12.4.1 Solicitud de una constancia de conservación

La solicitud de emisión de una constancia de conservación de mensajes de datos por parte de los suscriptores se realiza a través del API que Incode pone a su disposición, debiendo integrar la siguiente información:

1. Credenciales de autenticación al servicio
2. Hash del mensaje de datos sobre el cual se requiere la emisión de la constancia de conservación de mensaje de datos.
    a. El hash deberá ser generado utilizando el algoritmo SHA 256 o cualquier otro que haya sido publicado por la Secretaría de Economía.
3. OID de la Política de Constancias de Conservación de Mensajes de Datos asignado por la Secretaría de Economía.

En caso de que el hash que se recibe como parámetro no haya sido generado con el algoritmo SHA256 no se emitirá la constancia de conservación solicitada. Lo anterior considerando que las constancias de conservación deben de ser emitidos sobre solicitudes que hayan sido generadas con los algoritmos criptográficos publicados por la Secretaría de Economía dentro de la página de firma digital.

12.4.2 Integración del servicio de constancias de conservación de mensajes de datos con los sistemas de los suscriptores

Una vez que los interesados completan el proceso de contratación y se convierten en suscriptores les corresponde llevar a cabo el proceso de integración de las constancias de conservación de mensajes de datos en sus procesos de negocio. Para ello, Incode a través de su Profesional Jurídico entregará al suscriptor las credenciales de acceso y variables de seguridad requeridas para la conexión y consumo del servicio para la solicitud del token de constancias de conservación. Es importante mencionar que, como se establece en los términos y condiciones del servicio, los suscriptores son los responsables de la adecuada gestión de las credenciales de acceso que les son proporcionadas.

Para el proceso de integración Incode entregará al suscriptor el documento técnico de interoperabilidad en el cual se describen y comentan las funcionalidades del servicio, así como los mecanismos de conectividad y estándares que serán aplicados para la integración de los sistemas. La solución que proporciona Incode respeta los principios de neutralidad tecnológica por lo que no se requiere una tecnología específica para la conectividad y se facilita que los suscriptores consuman el servicio sin importar las especificaciones tecnológicas de sus sistemas.

12.4.3 Emisión del token de constancia de conservación

Una vez que Incode recibe la solicitud de constancias de conservación de mensajes de datos, el servicio deberá de generar la solicitud interna del token de constancia de conservación, también conocida como *TimeStampReq* o *tsq*, el cual será enviado a la Autoridad de Constancias de Conservación de Mensajes de Datos.

Para la integración del tsq de solicitud a la Autoridad de Constancias de Conservación de Mensajes de Datos, Incode considerará los siguientes valores para las variables requeridas por el estándar:

1. messageImprint: OID del algoritmo utilizado para obtener el hash y el hash del mensaje de datos sobre el cual se requiere la emisión de la constancia de conservación.
2. reqPolicy: el OID de la Política de Constancias de Conservación de Mensajes de Datos asignado por la Secretaría de Economía a Incode. En esté caso 2.16.484.101.10.316.100.12.1.2.1.1.1.1
3. certReq: Verdadero.

Incode establece el valor de la variable certReq como verdadero con lo cual se integrará en cada una de las constancias de conservación emitidas el certificado

digital de la Autoridad de Constancias de Conservación de Mensajes de Datos con el cual son firmados las constancias de conservación emitidas.

Una vez que el servicio recibe la respuesta de la Autoridad de Constancia de Conservación de Mensajes de Datos, es decir un *TimeStampResp* o *tsr* se debe de verificar la validez de la firma electrónica contenida en el token de la constancia de conservación; adicionalmente, el servicio debe de verificar que el objeto sobre el cual se emitió la constancia de conservación de mensajes de datos sea aquel que se incluyó como parte del *tsq*.

Una vez verificado el contenido y al no presentarse errores en la emisión la constancia de conservación de mensajes de datos, el servicio procederá a devolver el token de constancia de conservación al suscriptor solicitante.

12.4.3.1 Contenido del token de Constancia de Conservación de Mensajes de Datos

Para asegurar su conformidad con el RFC 3161, así como con la NOM 151 como parte del proceso de emisión de constancias de conservación de mensajes de datos, Incode PSC se asegura que dicho token contenga:

1. Hash del mensaje de datos respecto del cual se emite constancia de conservación de mensaje de datos.
2. Referencia al algoritmo criptográfico utilizado.
3. Número de serie de la constancia de conservación de mensajes de datos.
4. OID de la Política del servicio asignado por la Secretaría de Economía.
5. Fecha y hora de la emisión de la constancia de conservación.
6. Referencia a la precisión en la emisión de la constancia de conservación de mensaje de datos.
7. Identificador de la Autoridad de Constancia de Conservación de Mensaje de Datos.
8. Cadena de certificación de los datos de creación de firma de la Autoridad de Constancia de Conservación de Mensajes de Datos.
9. Referencia al OCSP y CRL de la cadena de certificación de la Autoridad de Constancias de Conservación de Mensajes de Datos.

12.4.4 Respuesta del servicio de emisión de Constancias de Conservación de Mensajes de Datos

Una vez que la constancia de conservación de mensaje de datos fue emitida conforme a lo señalado en el apartado 12.4.3 del presente documento, el servicio procederá a entregar el token de la constancia de conservación al suscriptor que lo ha solicitado.

El servicio entregará al suscriptor el *TimeStampResp* o *tsr* codificado en base 64, mismo que deberá de ser decodificado por el interesado, quien deberá de verificar que la constancia de conservación de mensaje de datos corresponda con el hash sobre el cual se requirió la emisión. Para ello deberá verificar que el hash forme parte de la constancia de conservación emitida y será responsabilidad del suscriptor resguardar el mensaje de datos original respecto del cual se solicitó la emisión.

13 Administración y operación de la ACCMD

13.1 Gestión de la seguridad

La información que genera Incode como Prestador de Servicios de Certificación durante el proceso de emisión de constancias de conservación es considerada como uno de los activos más importantes de la organización y respecto del cual se implementan procesos que garantizan la seguridad de la información en cada una de las etapas del servicio.

La implementación de controles de seguridad esta homologada con los requerimientos que establece la ISO 27001 como parte del Sistema de Gestión de Seguridad de la Información, concretamente en lo referente a la declaración de aplicabilidad, así como de los controles de seguridad que se establecen como parte del Plan de Seguridad de Sistemas.

Estos controles no están enfocados únicamente en la gestión de la seguridad lógica de los procesos, sino que establecen medios de control físico con los que Incode resguarda la seguridad de sus equipos, instalaciones y personal aportando a la seguridad general del proceso y de sus operaciones de negocio. El seguimiento respecto de la correcta implementación y desarrollo de los controles de seguridad es responsabilidad del Profesional Informático quien participa desde el diseño de los controles para un mejor entendimiento de estos.

Entre los diversos mecanismos de seguridad que implementa Incode y que se han establecido como políticas, prácticas o planes de seguridad, para los cuales se ha desarrollado un documento específico, se encuentran:

1. Sistema de Gestión de Seguridad de la Información.
2. Política de Seguridad Física.
3. Política de Seguridad de la Información.
4. Plan de Seguridad de Sistemas.
5. Plan de Adminsitración de Claves.

13.1.1 Responsable de la seguridad de la ACCMD

Incode en todo momento se asume como responsable de la seguridad de la información de los procesos relacionados con la emisión de constancias de conservación de mensajes de datos, independientemente de la contratación de procesos que pudiera llevar con terceros. En ese sentido, cualquier actividad realizada por algún proveedor con relación a la Autoridad de Constancias de Conservación de Mensajes de Datos requiere que las responsabilidades que esté asume estén claramente definidas en el contrato de prestación de servicios, no obstante que Incode se mantiene como el responsable ante suscriptores, partes interesadas y autoridades.

13.1.2 Controles de acceso

Las instalaciones de Incode donde se procesa la información para la emisión de constancias de conservación de mensajes de datos implementan controles de acceso que permiten asegurar que la infraestructura tecnológica que soporta la Autoridad de Constancias de Conservación de Mensajes de Datos cuenta con las protecciones y mecanismos de seguridad suficientes para limitar su acceso por terceros no

autorizados. Los controles de acceso son definidos y provistos por los centros de datos arrendados e Incode asume y acepta como propios dichos controles.

El detalle de los controles de acceso a las instalaciones de los centros de datos es consultable en la Política de Seguridad Física de Incode.

13.1.3 Política de seguridad de la información

Incode cuenta con una Política de Seguridad de la Información la cual establece los principios generales de seguridad que son aplicables a la organización, así como los objetivos en materia de seguridad de la información de la empresa. Dicha Política es transmitida a todos los empleados y proveedores como parte de su proceso de integración y forma parte de la concientización que fomenta Incode respecto de la seguridad de la información de conformidad con su Sistema de Gestión de Seguridad de la Información.

13.2 Clasificación y gestión de activos

El Sistema de Gestión de Seguridad de la Información como parte de sus procedimientos requiere que las organizaciones que, sin importar el tipo o característica de los activos, se cuenten con un registro completo y preciso de sus activos. Incode con relación al servicio de emisión de constancias de conservación, que tiene acreditado como Prestador de Servicios de Certificación, pone especial énfasis en el registro de los activos de software y hardware que soportan la operación de su Autoridad de Constancias de Conservación de Mensajes de Datos.

Para ello, ha generado un registro de los componentes de software que son fundamentales para la operación de su Autoridad de Constancias de Conservación de Mensajes de Datos el cual se ha incluido dentro del Plan de Continuidad de Negocio y Recuperación ante Desastres para una mejor identificación de los participantes en la ejecución de dicho Plan. En dicho registro se incluyen las últimas versiones funcionales que se encuentran implementadas, así como las direcciones del repositorio de información en el cual se almacenan o las direcciones de internet a través de las cuales se pueden descargar. Dentro del registro de software se considera especialmente al código fuente de los servicios de la Autoridad de Constancias de Conservación de Mensajes de Datos, el cual se considera activo crítico de la organización y que, para mayor seguridad, se encuentra resguardado en un sistema de control de versionamiento de código.

En el caso de los activos relacionados con el hardware, establece un procedimiento de control de inventarios en el cual se lleva la relación de cada uno de los equipos con los que cuenta la organización, además de tener un procedimiento de control de resguardo de este, donde el colaborador que ocupa el equipo se hace responsable de la seguridad de este, así como de utilizarlo conforme a los lineamientos dictados por la organización. El responsable del equipo, en caso de presencia de algún tipo de falla, deberá realizar los reportes correspondientes a el área de soporte técnico para que se ejecuten los procedimientos de mantenimiento correctivo que se consideren necesarios.

En lo que respecta a la infraestructura de la Autoridad de Conservación de Mensajes de Datos corresponde su resguardo al Profesional Informático y Auxiliar de Apoyo Informático de Seguridad al ser los máximos responsables de la operación, gestión y

administración del servicio de constancias de conservación de mensajes de datos. La gestión de esta infraestructura se lleva a cabo de conformidad con la "Política de administración de infraestructura informática" donde se describen los procedimientos aplicables a estos componentes. Es importante mencionar que, conforme se señala en el "Análisis y Evaluación de Riesgos y Amenazas" todos los componentes de la Autoridad de Constancias de Conservación de Mensajes de Datos están considerados como activos críticos de la organización y cuentan con planes y políticas de seguimiento específicas para garantizar su correcto funcionamiento y mantenimiento.

13.2.1 Clasificación de la información

En Incode se deben implementar los controles y mecanismos necesarios para proteger y hacer un buen uso de la información personal a la que se tiene acceso, así como velar por el cumplimiento de la legislación aplicable.

i. Los responsables del tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la ley.
ii. Los datos personales deben ser recabados y tratados de manera lícita de conformidad con las disposiciones establecidas por estas Leyes y Reglamentos y demás normas aplicables.

El esquema de clasificación de la información del Incode se divide en una jerarquía de tres niveles y es el siguiente:

i. Pública
ii. De uso interno
iii. Confidencial

Esquema de clasificación de la información como Pública**:**

Es toda información que se encuentra disponible fuera de la organización o que se pretende utilizar con fines públicos por parte del propietario de la información.

Esquema de clasificación de la información como de Uso interno:

Es toda la información que comúnmente es compartida por el personal de la organización y no pretende ser distribuida fuera de la empresa, pero no es clasificada como confidencial.

Esquema de clasificación de la información como CONFIDENCIAL:

Es toda la información de datos personales del personal de la organización, clientes, proveedores, socios comerciales e incluso solo de los visitantes, que incluye cualquier información concerniente a una persona física identificada o identificable.

13.3 Seguridad del personal

Incode emplea solo personal calificado en términos de habilidades y comportamientos y es investigado por la organización en cuanto a antecedentes y riesgos. Incode se asegura en todo momento de hacer una revisión de los

antecedentes y referencias que los candidatos proporcionan durante el proceso de reclutamiento.

Documentos relacionados:

- PS – Seguridad del personal
- PL 04 Reglas de Comportamiento – Política de Uso Aceptable

13.3.1 Nuevos empleados y recontrataciones

Uno de los principales controles que se implementan en la contratación y selección de personal es la verificación de credenciales y antecedentes de quienes se postulan para las vacantes, donde se verifica la veracidad de la información que proporciona el interesado tanto a nivel personal como a nivel profesional.

Las siguientes verificaciones requieren ser completadas satisfactoriamente:

- Verificación de referencias (se deben de completar con anterioridad al inicio de labores).
- Revisión formal de historial (donde sea legalmente posible).
    - Debe abarcar al menos los últimos 7 años.
    - Obligatorio para nuevas contrataciones y recontrataciones.
- Consentimiento y aceptación de políticas y procedimientos de seguridad.

Las contrataciones de personal temporal e internos deben de seguir el mismo proceso de verificación.

13.3.2 Competencias para el servicio de CCMD

Como parte del proceso de contratación, principalmente cuando se consideran los puestos del Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, los encargados del proceso de selección y contratación deben considerar las capacidades de los candidatos para mantener la fiabilidad de la operación de la Autoridad de Constancias de Conservación de Mensajes de Datos. Entre las consideraciones que se deben tomar en cuenta en la contratación se encuentran:

1. Cuando se trate de los perfiles de Profesional Informático y Auxiliar de Apoyo Informático de Seguridad se deberá asegurar que los postulantes cuentan con experiencia y conocimientos en criptografía e infraestructura de clave pública.
2. Los postulantes para dichos puestos deberán demostrar que cuentan con conocimiento experto en la administración de procesos criptográficos e infraestructura de clave pública presentando cursos o certificaciones en la materia.
3. Las actividades y responsabilidades de los puestos de seguridad en la operación de la Autoridad de Constancias de Conservación de Mensajes de Datos deberán de estar documentados dentro del perfil de puesto organizacional.
4. Incode deberá de implementar la división de responsabilidades y asignación de privilegios mínimos a efecto de reducir el control operacional de un solo individuo reduciendo el riesgo que esto conlleva.

13.3.3 Revisión de empleados y procesos de capacitación

Los empleados de Incode reciben capacitación en temas de seguridad y se revisan de manera continua. En particular, anualmente se realiza lo siguiente:

- Se establecen planes de desempeño por empleado
- Revisión de desempeño
- Capacitación formal de seguridad
- Revisión de las Políticas de Seguridad de la Información

13.3.4 Sanciones al personal

Incode aborda las violaciones de las reglas de conducta y cualquier otra violación de la política de la empresa de forma individual. De conformidad con la política de empleo a voluntad de la Compañía, Incode se reserva el derecho de imponer cualquier forma de disciplina que elija. La acción disciplinaria puede incluir advertencias orales o escritas, suspensión, descenso de categoría, período de prueba o terminación involuntaria a discreción exclusiva de Incode.

13.3.5 Terminación del empleo

En caso de despidos, Incode garantiza que se tomen las medidas adecuadas en función de procedimientos y listas de verificación. En particular, se asegura que el acceso de los empleados a los sistemas de Incode sea revocado.

13.4 Seguridad física y ambiental

Los sistemas de información, además de contar con medidas de seguridad lógicas, requieren que las organizaciones establezcan medidas de seguridad física que permitan garantizar a sus operadores y usuarios que la información que se genera a partir de sus procesos se mantiene integra al asegurar que sus equipos de infraestructura se mantienen alejados de cualquier manipulación no autorizada.

En ese sentido y en el contexto de la operación de Incode como Prestador de Servicios de Certificación la necesidad de establecer medidas de seguridad físicas cobra mayor relevancia al tratarse de servicios de confianza que impactan en la operación de la organización, así como en las operaciones que sus clientes realizan en medios electrónicos utilizando su servicio de emisión de constancias de conservación de mensajes de datos como evidencia de las transacciones realizadas.

Para dar cumplimiento a estas necesidades de seguridad, Incode implementa una Política de Seguridad Física que está orientada a establecer las medidas de seguridad y controles de acceso que se deberán de implementar en centros de datos y oficinas administrativas a fin de resguardar la seguridad de la información de sus procesos.

En ese sentido, Incode implementa los controles de seguridad que a continuación se enlistan y cuyo detalle se puede consultar dentro de la Política de Seguridad Física.

1. Seguridad física
    a. Instalaciones con perímetros de seguridad sólidos de concreto armado.
    b. Personal de seguridad privada con presencia permanente.
    c. Circuito cerrado de televisión.
    d. Procedimientos de control de acceso.
    e. Mecanismos de doble factor de autenticación para el ingreso a áreas seguras.
2. Seguridad ambiental
    a. Protecciones contra incendios.
    b. Protecciones contra fallas en los servicios eléctricos.
    c. Protecciones contra fallas en telecomunicaciones.
    d. Procesos de protección ante la presencia de sismos.

13.5 Gestión de las operaciones

Una de las principales características de la seguridad de la información es la disponibilidad. Por ello, Incode en su compromiso de mantener en todo momento la seguridad de la información de su proceso de emisión de constancias de conservación implementa medidas que le permiten establecer un servicio de alta disponibilidad que pone a disposición de sus suscriptores y partes interesadas con un diseño de arquitectura tolerante a fallos.

Para lograr este objetivo tiene desplegada la infraestructura tecnológica que soporta la Autoridad de Constancias de Conservación de Mensajes de Datos en dos regiones de procesamiento de datos del proveedor de servicios de cómputo en la nube, en este caso AWS, donde cuenta con una implementación redundante en su región de

procesamiento principal habilitando dos zonas de disponibilidad con una configuración activo-activo donde las peticiones de emisión de una constancia de conservación se distribuyen entre ambas zonas de disponibilidad con la implementación de un balanceador de cargas. En lo que respecta a la región de procesamiento alterna, Incode despliega los mismos recursos presentes en su región principal, aunque los mismos se encuentran habilitados de forma pasiva y no son activados hasta el momento en que pudiera presentarse una contingencia que deje fuera de operación a la región principal.

Ahora bien, para lograr un adecuado funcionamiento del servicio Incode tiene la obligación y compromiso de establecer medidas de seguridad que permitan mantener el nivel de confianza que se tiene sobre su Autoridad de Constancias de Conservación de Mensajes de Datos. Por ello, implementa una serie de medidas de seguridad a nivel físico y lógico que tienen como objetivo mantener la integridad de la información en el proceso. Como parte de las medidas que se implementan a nivel lógico en la Autoridad de Constancias de Conservación de Mensajes de Datos se considera el uso de herramientas antivirus las cuales cuentan con protección antimalware, phishing, ransomware y otro tipo de tecnologías que tienen como objetivo vulnerar la seguridad de los sistemas de información.

Parte importante de la gestión de la operación de la Autoridad de Constancias de Conservación de Mensajes de Datos es la identificación y respuesta a incidentes de seguridad de la información, donde para atender este tipo de incidentes, Incode dentro de su plan de continuidad de negocio y recuperación ante desastres establece los procedimientos que se deben seguir en caso de identificación y presencia de incidentes de seguridad de la información, los cuales incluyen los protocolos de notificación a suscriptores, partes interesadas y autoridades.

Si bien estas medidas de seguridad son preventivas, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad tienen como parte de sus responsabilidades establecer un sistema de monitoreo constante que les permita advertir cualquier desviación en el funcionamiento de los sistemas o servicios para identificar anomalías que puedan poner en riesgo el servicio, así como verificar que el servicio de emisión de constancias de conservación opera dentro de los límites máximos de alerta de su capacidad instalada para asegurar que los sistemas y servicios en todo momento cuentan con las capacidades mínimas de procesamiento y almacenamiento de información.

13.6 Gestión de acceso al sistema

La gestión de la operación de la Autoridad de Constancias de Conservación de Mensajes de Datos está a cargo del Profesional Informático y del Auxiliar de Apoyo Informático de Seguridad, cuyos puestos son considerados por la organización como roles de confianza y, por tanto, son los máximos responsables de la infraestructura y activos críticos de la organización. Como consecuencia, son los únicos colaboradores que se encuentran facultados para acceder a los sistemas y servicios de la Autoridad como parte del servicio de emisión de constancias de conservación.

Para garantizar lo anterior, Incode implementa los controles de gestión de acceso a sistemas que se describen en la declaración de prácticas del Sistema de Gestión de Seguridad de la Información considerando la separación de tareas y asignación de

privilegios mínimos entre todos los colaboradores de la organización incluyendo los señalados roles de confianza. El manejo de los roles y permisos a través de dicha metodología asegura un mayor control en la asignación de accesos, así como mayor eficiencia en las revisiones de seguridad a través de las bitácoras de auditoría.

13.6.1 Seguridad perimetral

Los componentes de la infraestructura de la Autoridad Constancias de Conservación de Mensajes de Datos han sido desplegados con un proveedor de servicios en la nube, en este caso AWS, considerando dos regiones de servicios que cuentan con diversas zonas de disponibilidad para garantizar la continuidad de los servicios. Incode para su Autoridad de Constancias de Conservación de Mensajes de Datos dispone de dos zonas de disponibilidad en la región de procesamiento principal, las cuales cuentan con el mismo despliegue de infraestructura y componentes, a fin de proporcionar un servicio de alta disponibilidad a través de un balanceador de cargas. Adicionalmente, en la segunda región de procesamiento, que se utiliza como DRP también se despliegan componentes e infraestructura conforme las zonas de disponibilidad en la región principal.

Lo anterior resulta relevante dado que la responsabilidad de la seguridad perimetral de las instalaciones donde se encuentra ubicada la Autoridad de Constancias de Conservación de Mensajes de Datos, son responsabilidad de AWS, de acuerdo con el modelo de responsabilidad compartida que rige los servicios de este proveedor de servicios de cómputo en la nube. En ese sentido, AWS implementa diversos controles de acceso a las instalaciones, las cuales cuentan con certificaciones y reportes en materia de seguridad de la información que permiten garantizar que los procedimientos establecidos se cumplen y son coherentes con la información proporcionada a los clientes en materia de seguridad. Es importante mencionar, que los centros de datos de AWS que forman parte de las regiones de procesamiento de datos no autorizan el ingreso de personal ajenos a sus instalaciones, salvo notificación y solicitud expresa de la autoridad que regula los servicios de sus clientes.

13.7 Implementación y mantenimiento de sistemas confiables

Para la implementación de su Autoridad de Constancias de Conservación de Mensajes de Datos, Incode ha seguido las políticas internas de implementación y mantenimiento de sistemas confiables las cuales tienen como finalidad asegurar que los sistemas implementados en la organización cumplen con los requerimientos organizacionales de seguridad de la información.

En el caso de la Autoridad de Constancias de Conservación de Mensajes de Datos, el proceso de implementación incluyó la adquisición del software de dicha Autoridad, así como del servicio de emisión de constancias de conservación de mensajes de datos. Por lo cual Incode realizó un estudio de mercado en el que incluyó y participaron diversos proveedores quienes como primer requisito debieron comprobar experiencia en la implementación de infraestructura de clave pública.

Además de la experiencia, los proveedores requirieron comprobar que dentro sus procesos de desarrollo de sistemas, desde el diseño hasta la implementación de la solución consideran la seguridad de la información como un elemento intrínseco

sobre el cual se construyen los componentes y herramientas a través de los cuales se ejecuta el servicio.

13.8 Compromiso de la Autoridad de Constancias de Conservación de Mensajes de Datos

Se puede afirmar que los datos de creación de firma electrónica avanzada de la Autoridad de Constancias de Conservación de Mensajes de Datos han sido vulnerados cuando se tiene certeza suficiente de que los mismos han sido comprometidos a través de la extracción o robo de dichos datos del módulo criptográfico o cuando han sido eliminados del mismo. Para los Prestadores de Servicios de Certificación es importante conocer en todo momento el estatus que guardan sus datos de creación de firma porque al ofrecer servicios de confianza en medios electrónico su principal activo se vuelven sus datos de creación de firma con los cuales emiten todos y cada uno de los actos que tienen acreditados, en el caso de Incode la emisión de Constancias de Conservación de Mensajes de Datos.

El compromiso de los datos de creación de firma puede presentarse por alguna de las siguientes situaciones:

1. Los Datos de Creación de Firma fueron extraídos del módulo criptográfico por un tercero no autorizado.
2. Los Datos de Creación de Firma fueron eliminados del módulo criptográfico por accidente o de forma intencional.

Para el supuesto de la extracción o robo de los datos de creación de firma conforme a los niveles de seguridad que implementa el módulo criptográfico, podría afirmarse que el único escenario bajo el cual pudiera presentarse este supuesto es cuando el tercero no autorizado tiene acceso físico al módulo criptográfico y cuenta con las credenciales y tarjetas de acceso necesarias para poder extraer la información del certificado.

En cuanto a la eliminación voluntaria o involuntaria de los datos de creación de firma se puede presentar por alguno de los siguientes supuestos:

1. El módulo criptográfico es accesado físicamente y es destapado sin seguir los procedimientos de seguridad que establece el fabricante.
2. Se intenta acceder al módulo criptográfico reiteradamente (ataque de fuerza bruta) sin contar con las credenciales de acceso correspondientes.
3. Eliminación intencional de la llave privada del servicio de constancias de conservación de mensajes de datos por parte del personal de la organización que cuenta con acceso al módulo criptográfico.
4. Eliminación no intencional de la llave privada de la Autoridad de Constancias de Conservación de Mensajes de Datos por parte del Profesional Informático o el Auxiliar de Apoyo Informático de Seguridad.

El proceso que implementará Incode ante el compromiso de los Datos de Creación de Firma Electrónica de su Autoridad de Constancias de Conservación de Mensajes

de Datos forma parte y es consultable en el Plan de Continuidad de Negocio y Recuperación ante Desastres.

13.9 Terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos

La terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos es el proceso en el cual la organización que la administra, por decisión propia o por decisión de la Autoridad que regula la prestación del servicio, determina que no es factible continuar la operación de dicha Autoridad. En caso de presentarse este supuesto, Incode deberá ejecutar el procedimiento que se describe en la Regla 18 de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.

Ahora bien, aun y cuando la Autoridad de Constancias de Conservación de Mensajes de Datos se encuentre en proceso de terminación Incode se asegurará que no se presenten interrupciones potenciales en el servicio de los suscriptores y partes interesadas quienes deberán ser notificados con quince días de anticipación a la notificación que se realice a la Secretaría de Economía con la finalidad de que puedan prever las modificaciones en la integración de sus procesos de negocio. Adicionalmente, Incode se encargará de mantener disponibles los mecanismos que permitan verificar que las constancias de conservación se emitieron de conformidad a la Declaración de Prácticas con anterioridad a la terminación de la Autoridad.

Durante el periodo previo a la terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos, Incode se asegurará de transferir a la Secretaría o al Prestador de Servicios de Certificación que esta determine los archivos de registro de eventos y bitácoras de auditoría que permitan a la Autoridad y a las partes interesadas verificar que la Autoridad de Constancias de Conservación de Mensajes de Datos pero de forma correcta mientas se encontró vigente.

Como parte final del procedimiento de terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos, Incode a través de su Profesional Jurídico deberá solicitar a la Secretaría de Economía la revocación de sus Datos de Creación de Firma Electrónica Avanzada. Este proceso incluye la eliminación segura de los datos de creación de firma de los módulos criptográficos implementando las herramientas que los propios módulos proporcionan con la finalidad de que la información en ellos contenida no pueda ser recuperada por ningún medio.

13.10 Registro de información relativa a la operación del servicio

Para la operación de los servicios de la Autoridad de Constancias de Conservación de Mensajes de Datos resulta relevante para Incode establecer un registro con la información que se genera como parte de la emisión de constancias de conservación, donde se tiene información de los suscriptores como parte del proceso de contratación, misma que se integra en un expediente al que se van relacionando las facturas de consumo conforme a los periodos de cobro que se puedan establecer en cada caso particular. Dicho expediente facilita el seguimiento de la atención a los suscriptores y permite tener a Incode un registro del historial de consumo de cada uno de sus suscriptores.

Además de los expedientes de sus suscriptores, Incode cuenta con un registro de las transacciones relacionadas con la emisión de constancias de conservación que tiene como objetivo contar con la información general relacionada a la emisión de cada una de las constancias de conservación que se generan, la cual pudiera ser requerida por autoridad competente en caso de considerarla necesaria. La información relacionada con las constancias de conservación de mensajes de datos se almacena directamente en la base de datos del sistema donde se incorporan datos como el hash sobre el cual se emite la constancia de conservación, la fecha y hora de petición y respuesta, el usuario que realiza la petición, además de la propia constancia.

13.10.1 Registros generales de auditoría

La Autoridad de Constancias de Conservación de Mensajes de Datos de Incode como parte de sus registros de auditoría almacena la información relacionada con cada uno de los eventos de emisión de una constancia de conservación, incluyendo la siguiente información:

1. Identificador del suscriptor que solicita la constancia de conservación.
2. Hash del mensaje de datos sobre el cual se emite la constancia de conservación.
3. Token la constancia de conservación que se entrega al suscriptor.

Es importante establecer que aún y cuando dichos registros no exponen ningún dato sensible, Incode los cataloga como información confidencial al tratarse de datos generados como parte del servicio que el suscriptor tiene contratado y donde es el único interesado en el contenido de la solicitud y respuesta. Dichos registros podrán ser entregados al suscriptor que lo solicita, a las partes interesadas o autoridades cuando sean requeridos para proporcionar evidencia en procesos legales respecto de la correcta funcionalidad de la Autoridad de Constancias de Conservación de Mensajes de Datos.

13.10.2 Tiempo de resguardo de los registros

Si bien la ley no establece un periodo mínimo de resguardo para las constancias de conservación de mensajes de datos, Incode considera el resguardo de dicha información por al menos los tres años posteriores a su emisión. Esté periodo de tiempo es aplicable a cualquier token de constancia de conservación y se dará cumplimiento al mismo aún y cuando se presente la terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos.

13.11 Proceso de auditoría

Como parte de su operación, Incode realiza procesos de auditoría interna en intervalos anuales que le permiten recabar información respecto del estatus de implementación del SGSI y de las políticas y procedimientos de seguridad relacionados con el servicio de emisión de constancias de conservación de mensajes de datos que tiene acreditado como Prestador de Servicios de Certificación. Las auditorías internas realizadas por Incode tienen como objetivo principal el poder constatar la conformidad de las operaciones con los requerimientos de seguridad de la información de la organización, así como de los requerimientos que establece el presente SGSI.

Incode como parte de sus procesos de auditoria registra eventos significativos para los sistemas de TI según corresponda y mantiene registros de auditoría para análisis y exámenes forenses. Los registros de auditoría pueden generar alertas por anomalías o mediante procesos automatizados basados en reglas. Estas alertas y los registros asociados pueden ser examinados por los administradores del sistema para determinar los niveles de respuesta apropiados.

Incode registra eventos administrativos y de seguridad relevantes lo cual le permite administrar el riesgo y mantener la integridad/mantener la retención del historial de auditoría de la actividad de la red. Cuando el sistema lo permite, los eventos registrados incluyen, entre otros:

- Creación/modificación/eliminación de cuentas de usuario.
- Creación/eliminación de cuentas de equipos de cómputo.
- Habilitación/des habilitación de cuentas.
- Bloqueo/desbloqueo de cuentas.
- Cambio en password de los usuarios.
- Modificaciones a los grupos de usuarios.
- Intentos fallidos de log in.
- Detección de amenazas en los endpoint.
- Conexiones VPN
- Filtros web
- Filtros de correo
- Registro de eventos del Sistema Operativo
- Intentos no autorizados de conexión a los sistemas.
- Cambio en las configuraciones.
- Registro de eventos de acceso físico.

Incode garantiza que los informes de auditoría incluyan información clave cuando sea relevante y técnicamente factible, incluidos, entre otros:

- ID de usuario o ID de proceso.
- Fecha y hora del evento.
- Identificación del sistema/terminal.
- Localización (cuando sea posible).
- Fuente del evento.
- Destino del evento.
- Detalles del evento (proceso, estado del evento antes/después).
- Mensajes del sistema (mensajes de error, alertas, etc.)

Toda la información que se genera como parte del proceso de auditoría deberá de ser considerada como evidencia y, por tanto, en términos del estándar ISO 27001 deberá ser considerada como información documentada por lo cual deberá ser resguardada conforme al proceso establecido. Dicha evidencia deberá ser integrada dentro de la documentación inicial de las auditorías posteriores para que se le pueda dar el seguimiento adecuado.

Concluido el proceso de auditoría se deberá de realizar un informe respecto de los eventos y hallazgos que se derivan del proceso, mismo que será entregado a la Alta Dirección para su análisis y revisión.

Documentos relacionados:

- AU -- Auditoria y responsabilidad

14 Incode

Incode hace conocimiento de suscriptores, partes interesadas y público en general que su Autoridad de Constancias de Conservación de Mensajes de Datos, a través de la cual presta el servicio de emisión de constancias de conservación, es una entidad que opera de una vez que completo el procedimiento de acreditación ante la Secretaría de Economía como Prestador de Servicios de Certificación para el mencionado servicio. Para obtener la acreditación de su Autoridad de Constancias de Conservación de Mensajes de Datos, Incode declara su conformidad con la siguiente normativa:

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

Ahora bien, para mantener su conformidad con la normativa mencionada Incode implementa un Sistema de Gestión de Seguridad de la Información que le permite asegurar que los procesos de negocio y de administración de servicios de la Autoridad de Constancias de Conservación de Mensajes de Datos le ayudarán a cumplir los objetivos organizacionales donde se privilegia la seguridad de la información. Para ello, cuenta con los recursos humanos necesarios con las capacidades técnicas y conocimientos específicos relacionados con la gestión, administración y operación del servicio de emisión constancias de conservación para ofrecer un servicio con calidad y, sobre todo, certeza a sus suscriptores.

14.1 Conformación legal

Incode es una sociedad mexicana constituida de conformidad con la Ley General de Sociedades Mercantiles y cuenta con los siguientes datos:

1. Denominación: Incode S. de R. L. de C.V.
2. Folio Mercantil Electrónico: N-2022062219
3. Registro Federal de Contribuyentes: IPS220825HH4

14.2 Coberturas de responsabilidad

Como parte de su operación y de conformidad con los Elementos Económicos que señalan las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación para el servicio de emisión de constancias de conservación de mensajes de datos, Incode cuenta con un seguro de responsabilidad y una fianza para cobertura del servicio.

La fianza y el seguro de responsabilidad civil permanecerán vigentes por al menos un año con posterioridad a la terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos de Incode.

14.3 Elementos financieros

Incode cuenta con los recursos financieros para soportar la operación continua de la organización como Prestador de Servicios de Certificación de conformidad con la presente Política.

14.4 Recursos humanos

Incode emplea el personal suficiente para el desarrollo de las actividades, procedimientos y procesos relacionados con el servicio de emisión de constancias de conservación, los cuales cuentan con el conocimiento, capacitación y experiencia suficiente para operar la Autoridad de Constancias de Conservación de Mensajes de Datos.

14.5 Relaciones contractuales

Incode mantiene en resguardo los contratos derivados de las relaciones comerciales y contractuales que mantiene con sus suscriptores, los cuales se resguardan dentro de las áreas seguras de las oficinas administrativas y están bajo supervisión y responsabilidad del Profesional Jurídico.

incode psc

Incode PSC

Av. Río San Joaquín 498,

Amp Granada,
Miguel Hidalgo, CP 11529

psc@incode.com

psc.incode.com