ATEB

Manual de Declaración de Prácticas del servicio de Constancia de Conservación de Mensaje de Datos

ATEB—BPM

Dirección General

Fecha de inicio de operaciones: 15/Sep./2022

Identificador de Objeto: 2.16.484.101.10.316.100.9.1.2.2.3

Contenido

1. Información inicial

1.1 Información del documento

Información del documento
Denominación formal del Documento: Plan Estratégico de Negocios en ATEB 2021-2025
Descripción: Manual de Declaración de Prácticas del servicio de Constancia de Conservación de Mensaje de Datos
Organización: ATEB Servicios S.A de C.V.
Fecha de elaboración del documento: 20/May./2021
Fecha de actualización del documento: 02/May./2022
Administrador: Auxiliar de Apoyo Informático de Seguridad
Patrocinador: Director General
Destinatario / usuario: Público Externo: Secretaría de Economía

1.2 Registro de Cambios

Fecha	Autor	Versión	Referencia del Cambio	Estatus del documento
20/May./2021	JDGM	1.0	Elaboración de documento inicial	Definición inicial del documento
03/Ago./2021	JDGM	1.1	- Especificar archivo que recibirá el solicitante y la respuesta obtiene al solicitar la Constancia - Corrección de HSM - Se anexa columna al calendario de revisión debido a la segunda revisión semestral del documento - Inclusión de la URL donde se publicará el documento	Aprobado
19/Ene./2022	JDGM	1.2	Actualización de: - Alcance del documento -Calendario de revisión y actualización del documento	Aprobado

			- Punto 8 “Constancia de Conservación de Mensaje de Datos” - Descripción del procedimiento	
02/May./2022	JDMG	1.3	- Vigencia del presente documento - Actualización del Calendario de revisión del documento - Adición del punto 8.1 Identificador de Objeto	Aprobado

1.3 RESPONSABLES DE AUTORIZACIÓN

Autorizado

Profesional Jurídico

Lic. Luisa María Pastrán Llanes

Autorizado

Profesional Informático

Lic. Alberto Toledo Torres

Autorizado

Auxiliar de Apoyo Informático de Seguridad

Ing. Jesús David Guerrero Martínez

Autorizado

Director General

Ing. Jesús Miguel Pastrán Rodríguez

1.4 CLASIFICACIÓN DE LA INFORMACIÓN DEL DOCUMENTO

De conformidad con la política de confidencialidad de la información y la clasificación ahí establecida, el presente documento se clasifica como **Público.**

Bajo el esquema de clasificación de información, la contenida en el presente documento se clasifica como:

-Pública: Es toda aquella información que está disponible fuera de la organización o que su intención es la de ser usada con fines públicos por el dueño de la misma.

Además, y de conformidad con la LFPDPPP, con excepción de la información reservada o confidencial prevista en la ley, los sujetos obligados deben poner a disposición del público los términos del reglamento y los lineamientos, así como las actualizaciones que expida el instituto o la instancia equivalente a que se refiere el Artículo 61 de la citada ley y toda la información que no esté clasificada como reservada, confidencial y que contravenga la protección de datos personales.

ESTE ES UN PROCESO CÍCLICO, EVOLUTIVO Y DE MEJORA CONTINUA, QUE ESTÁ EN REVISIÓN Y ACTUALIZACIÓN PERMANENTE

2. Introducción

2.1 ANTECEDENTES

En el presente documento se estipula la Declaración de Prácticas necesarias para la prestación del servicio de Constancia de Conservación de Mensaje de Datos, esto con base en las Reglas Generales No.163 fracción I a VII y 164 a las que deben sujetarse los Prestadores de Servicio de Certificación (PSC) y con fundamento en lo dispuesto en el RFC 3628 y el RFC 3161, la NOM-151-SCFI-2016, el Código de Comercio y demás leyes aplicables.

Este documento establece las responsabilidades y obligaciones de las partes interesadas en el servicio de Constancia de Conservación de Mensaje de Datos, así como la definición de los términos, condiciones y características que se deben cumplir para la prestación de este servicio.

2.2. OBJETIVO

Establecer las normas, lineamientos, condiciones y procedimientos para el cumplimiento de las políticas aplicables a la Prestación del servicio de Constancia de Conservación de Mensaje de Datos, proporcionando los elementos humanos, económicos, materiales y tecnológicos requeridos para brindar un servicio de calidad como autoridad de Constancia de Conservación de Mensaje de Datos.

2.3. ALCANCE

Este Manual de Declaración de Prácticas aplica para todos aquellos usuarios (Personas Físicas o Morales) que soliciten el servicio de Constancia de Conservación de Mensaje de Datos, siempre y cuando estén acorde a las leyes y normativas existentes aplicables y se encuentren establecidos en el presente documento.

Así mismo, para todas las personas de las áreas involucradas en el desarrollo e implementación del servicio, estas son EDI, Desarrollo y Sistemas, así como para la correcta preservación de la confidencialidad, integridad y disponibilidad de la información manejada en los procesos de solicitud, ejecución y verificación de cada uno de los servicios que ATEB provee como autoridad.

2.4. DEFINICIONES

ASN.1: Versión 1 del Abstract Sintax Notation (Notación de Sintaxis Abstracta).

BCP: Business Continuity Plan (Plan de Continuidad de Negocio).

CFDI´s: Comprobante Fiscal Digital por Internet.

CENAM: Centro Nacional de Metrología.

Constancia de Conservación de Mensaje de Datos (CCMD): Mensaje de datos emitido por un prestador de servicios de certificación, conforme a lo establecido en la Norma Oficial Mexicana NOM-151-SCFI-2016.

Criptografía: Conjunto de técnicas matemáticas para cifrar información.

DRP: Disaster Recovery Plan (Plan de Recuperación ante Desastres).

HSM: Hardware Security Module (Módulo de Seguridad Hardware).

ISO: Information Security Officer (Oficial de Seguridad de la Información).

ISO/IEC: International Organization for Standardization /International Electrotechnical Commission (ISO/IEC 27001:2013).

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de Particulares.

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

NOM/SCFI: Norma Oficial Mexicana / Secretaría de Comercio y Fomento Industrial (NOM-151-SCFI-2016).

Política de Constancia de Conservación de Mensaje de Datos : Conjunto de directrices que establecen las características y requerimientos para la emisión de Constancias de Conservación de Mensajes de Datos por parte de ATEB.

Prestador de Servicios de Certificación (PSC): De acuerdo con el Art. 89 del Código de Comercio, es la persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el

sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría**.**

RFC 3161/3628: Request For Comments. Documento donde se estable el protocolo para garantizar el servicio de Constancia de Conservación de Mensaje de Datos.

SGSI: Sistema de Gestión de Seguridad de la Información.

TSAs: Time-Stamping Authorities (Autoridades de Sello de Tiempo).

2.5. PARTES INTERESADAS

Autoridad del servicio de Constancia de Conservación de Mensaje de Datos: Organización acreditada por la Secretaría de Economía para ofrecer los servicios de emisión de constancias de conservación de mensajes de datos a las personas físicas o morales que así lo requieran.

Comerciantes – Usuarios: Personas físicas o morales que solicitan los servicios otorgados por ATEB y que aceptan por ende los términos y condiciones que rigen su emisión.

Secretaría de Economía: Organismo responsable de la aplicación del marco normativo en materia de Comercio Electrónico, que, a través del cumplimiento de los requisitos establecidos por la ley, acredita a las Personas Jurídicas como Prestadores de Servicios de Certificación (PSC).

3. Vigencia del presente documento y de las Constancias de Conservación de Mensajes de Datos

El período de vigencia del presente documento es de 6 meses, por lo que la fecha en que entra en vigor la presente declaración de prácticas es a partir de la fecha de actualización.

De esta manera se resume la vigencia del presente documento:

Vigencia	Fechas
Inicio	02 de Mayo de 2022
Término	01 de Noviembre de 2022

Para poder identificar el inicio de la vigencia de la Constancia se agregan dos elementos, cuya definición se expresa mediante el formato ASN.1:

1) id-nom-ini-time OBJECT IDENTIFIER:: = {2 16 484 101 10 316 20 37 1117}
2) NOM151IniTime:: = GeneralizedTime

La vigencia de la Constancia de Conservación de Mensaje de Datos será mínima de 10 años a partir de su emisión y el comerciante-usuario podrá decidir si requiere la extensión de dicha vigencia según la naturaleza de la información de acuerdo con las leyes aplicables.

Así mismo se debe llevar un seguimiento de la vigencia de las normas y algoritmos empleados para la generación de las constancias y su validación, así como seguir los procedimientos necesarios para casos de contingencia cuando se descubran debilidades en los algoritmos empleados incluso ante de los 10 años.

3.1 Calendario de revisión del Manual de Declaración de Prácticas de Constancia de Conservación de Mensaje de Datos

	Calendario de revisión		
Día / ***Año***	Martes 02 de Mayo	***Día*** / ***Año***	Martes 01 de Noviembre
2022	Actualización	**2022**	Actualización
	Viernes 28 de Abril		Viernes 27 de Octubre
2023	Actualización	**2023**	Actualización
	Viernes 26 de Abril		Viernes 25 de Octubre
2024	Actualización	**2024**	Actualización
	Jueves 24 de Abril		Jueves 23 de Octubre
2025	Por definir	**2025**	Por definir

*Se anexa el calendario para los próximos 3 años sin embargo las fechas de actualización podrían ser modificadas con base en las necesidades del negocio y requerimientos solicitados por la Secretaria de Economía.

4. Matriz RACI

INFORMACIÓN SOBRE LOS PARTICIPANTES DEL SERVICIO					
#	**Puesto**	**Responsable**	**Aprobador**	**Consultado**	**Informado**
1.	Director General	**I**	*	*	*
2.	Auxiliar de Apoyo Informático de Seguridad	*	*	*	*

3.	Profesional Informático	—	*	*	*
4.	Profesional Jurídico	—	*	*	*
5.	Oficial de Seguridad	*	*	*	—
6.	Administrador del sistema	*	—	*	*
7.	Operador del sistema	*	—	*	*
8.	Auditor del Sistema	—	*	*	*

Nota: (*) Participa; (—) No participa

5. Declaración de Prácticas y su relación con las Políticas de Constancias de Conservación de Mensaje de Datos

El ISO es la persona responsable de mantener permanentemente actualizada y documentada la presente declaración de prácticas de certificación, así como su relación con las políticas que la fundamentan.

Todas las dudas y sugerencias sobre esta declaración se deben dirigir al ISO directamente.

Para que una empresa pueda operar de manera correcta y en óptimas condiciones necesita contar con procedimientos, procesos y políticas que sean la base de las operaciones que se han de realizar en cualquier empresa.

ATEB cuenta con un SGSI implementado lo que implica, entre otras cosas, garantizar el servicio que se proporciona como PSC, ya que adicional al centro de datos principal se cuenta con dos centros adicionales que tienen redundancia entre ellos, siendo así que la infraestructura tecnológica no se ve interrumpida o afectada en caso de que ocurriera algún incidente de cualquier tipo y de ser así se cuenta con los planes de continuidad y de recuperación del negocio, dependiendo de la gravedad de este, para continuar con las operaciones del mismo.

5.1 ESTÁNDARES

1. Los algoritmos criptográficos y la longitud de las llaves soportadas y utilizadas por ATEB cumplen con el estándar FIPS 140-2 nivel 3 y ETSI TS 102 042.
2. Se deben emplear en los procesos de generación de Constancias de Conservación de Mensajes de Datos, los algoritmos criptográficos que la Secretaría de Economía publica en su portal de internet y tener en cuenta las características mencionadas.
3. La disponibilidad del servicio brindado por ATEB es del 99.3%
4. Se utilizarán llaves con una longitud mínima de 4096 bits para los PSC y para los usuarios.
5. En caso de algún incidente, que afecte en cualquier medida la seguridad de cualquiera de los servicios de certificación emitidos por ATEB, serán comunicados a través de la página oficial de ATEB y medios de comunicación autorizados para conocimiento de los interesados.
6. Todos los eventos e incidentes deben ser registrados con la fecha y hora exacta en que se presentaron.

7. Todos los eventos e incidentes deben ser reportados y notificados a la Secretaría de Economía en cuanto se detectan para que se lleven a cabo las acciones correctivas y se reduzca el impacto negativo que pudieran tener.
8. ATEB asegura la exactitud de ±3 milisegundos, tiempo con el que se emiten los Sellos Digitales de Tiempo correspondientes a las Constancias de Conservación de Mensajes de Datos, ya que se encuentra sincronizado al servidor de tiempo Cronos del CENAM.
   En el caso de que se detecte la existencia de una variación en el tiempo se dejará de brindar cualquiera de los servicios de certificación brindados por ATEB, y se llevarán a cabo las acciones correctivas hasta asegurar que la sincronización es correcta.
9. ATEB mantiene evidencia de la trazabilidad de la sincronización de tiempo con el servidor de CENAM.
10. No se limita el uso de ninguno de los servicios de certificación emitidos por ATEB, sin embargo, se excluye a ATEB de todo uso malintencionado que los comerciantes - usuarios les den a estos.
11. ATEB mediante el SGSI implementado se asegura de mantener toda la información que maneja confidencial, íntegra y disponible.
12. Las operaciones de ATEB y todo lo expresado en el presente documento se rigen por las legislaciones y normativas nacionales e internacionales que así lo apliquen, manifestando por ende que para cualquier actualización que se realice a las normas aplicables deberá ATEB apegarse a las mismas.
13. ATEB declara que permitirá a las autoridades relevantes la realización de las investigaciones que correspondan a sus facultades, siempre y cuando éstas sean debidamente fundamentadas y que quienes las realicen, se acrediten como autorizados para llevarlas a cabo.
14. En caso de presentarse alguna queja sobre cualquiera de los servicios de certificación brindados por ATEB se deberá seguir el procedimiento de atención a clientes tal como se realiza para cualquiera de los otros servicios brindados por ATEB.
15. La emisión de la Constancia de Conservación de Mensaje de Datos se realizará una vez completado el procedimiento de ventas establecido para todos los servicios brindados por ATEB.
16. Se deben cumplir los requisitos para la emisión de Constancias de Conservación de Mensaje de Datos cuando éstos sean utilizados por ATEB en actos de comercio que estén relacionados con sus negocios.
17. Se deben mantener los estándares de la información en la emisión de las Constancias de Conservación de Mensaje de Datos (integridad, disponibilidad y confidencialidad).
18. Las Constancias de Conservación de Mensaje de Datos serán otorgadas para todas aquellas personas físicas o morales que emitan CFDI´s.
19. Una vez otorgada la acreditación por parte de la Secretaría de economía, el PSC podrá iniciar las operaciones como autoridad en el servicio de Constancia de Conservación de Mensaje de Datos.

6. Aplicabilidad

El presente Manual de Declaración de Prácticas del servicio de Constancia de Conservación de Mensaje de Datos cumple con las Reglas Generales para PSC, el Código de Comercio, la NOM-151-SCFI-2016 y el Reglamento del Código para PSC, en los cuales se establecen los requisitos para que toda organización que quiera brindar el servicio de Constancia de Conservación de Mensaje de Datos pueda ofrecer sus servicios como Prestador de Servicios de Certificación (PSC).

Este servicio se encuentra disponible para las personas físicas y morales que necesitan los servicios otorgados por ATEB y que aceptan por ende los términos y condiciones que rigen su emisión.

Estos servicios que ofrece ATEB se encuentran sincronizados con el servidor de tiempo Cronos del CENAM para contar con un tiempo de respuesta óptimo y con ello asegurar la correcta aplicación de estos.

6.1 Acreedores del servicio de Constancia de Conservación de Mensaje de Datos

Personas físicas o morales que a nombre propio o representando legalmente a un tercero de manera legal, solicitan la emisión de una constancia, siempre y cuando se especifique que el responsable se compromete a custodiar los datos de creación de la firma sin otorgar el uso a cualquier persona y bajo ningún concepto.

7. Obligaciones y Responsabilidades

7.1 Obligaciones de la autoridad del servicio de Constancia de Conservación de Mensaje de Datos

Las obligaciones de ATEB respecto de la emisión de las Constancias de Conservación de Mensajes de Datos acreditado por la Secretaría de Economía como Prestador de Servicios de Certificación son:

a) Asegurarse de la implementación de los requisitos descritos en el presente documento y en relación con las Políticas del servicio de Constancia de Conservación de Mensaje de Datos.
b) Brindar el servicio de Constancia de Conservación de Mensaje de Datos con la disponibilidad aquí señalada, en el formato establecido (ASN.1) y por el mismo medio por el que fue solicitada.
c) Atender las solicitudes de Constancias de Conservación de Mensajes de Datos bajo los lineamientos establecidos con el comerciante – usuario en el contrato establecido entre ambas partes.
d) Cerciorarse de que la solicitud se está haciendo por la persona correcta y con quien se establece el contrato o alguien destinado por el mismo.
e) Aclarar todos los términos y condiciones para el servicio de Constancia de Conservación de Mensaje de Datos dentro del contrato entre ambas partes.
f) Verificar que la infraestructura con que se cuenta soporte el servicio de Constancia de Conservación de Mensaje de Datos.
g) Proteger la confidencialidad y asegurar la disponibilidad e integridad de la información que los clientes le proporcionan para el servicio de Constancia de Conservación de Mensaje de Datos.
h) Cumplir con todos los elementos humanos, económicos, materiales y tecnológicos solicitados por la Secretaría de Economía para fungir como Prestador de Servicios de Certificación en el servicio de Constancia de Conservación de Mensaje de Datos emitidas de conformidad con la NOM-151-SCFI-2016.
i) Brindar a los comerciantes – usuarios el web service adecuado para que puedan identificar y/o validar las constancias generadas.

j) Implementar controles para reducir el riesgo del mal uso, el uso no autorizado de los datos personales de los comerciantes – usuarios y de su pérdida o destrucción, comprometiéndose así bajo acuerdo de confidencialidad y/o contrato, a mantener la información proporcionada por el cliente como confidencial, cumpliendo así con el Sistema de Gestión de Seguridad de la Información bajo el que se rige ATEB.

7.2 Obligaciones del comerciante – usuario

Los usuarios deberán cumplir con sus obligaciones:

a. Resguardar sus llaves de acceso al servicio de Constancia de Conservación de Mensaje de Datos.
b. Asegurar la vigencia del certificado.
c. Cumplir con lo estipulado en el contrato y/o documentos adicionales pactados entre ATEB y el comerciante – usuario.

7.3 Responsabilidades de la autoridad del servicio de Constancia de Conservación de Mensaje de Datos

ATEB es responsable de brindar el servicio de Constancia de Conservación de Mensaje de Datos de acuerdo con lo establecido en el presente documento y en relación con las Políticas del servicio de Constancia de Conservación de Mensaje de Datos.

1. Dar a conocer por medio de la página oficial de ATEB, la información relacionada con el servicio de Constancia de Conservación de Mensaje de Datos.
2. Garantizar que las Constancias de Conservación de Mensaje de Datos emitidas por la organización sean íntegras y auténticas.

ATEB no se hace responsable de:

1. Cualquier daño o perjuicio al que puedan estar expuestos los comerciantes – usuarios al hacer uso inadecuado de las Constancias de Conservación de Mensajes de Datos emitidas por ATEB.
2. Cualquier daño o perjuicio al que puedan estar expuestos los comerciantes – usuarios debido al incumplimiento de sus obligaciones.
3. Cualquier daño o perjuicio ocasionado por las malas interpretaciones por parte de los comerciantes – usuarios al hacer uso del servicio de Constancia de Conservación de Mensaje de Datos.
4. La emisión errónea de una Constancia de Conservación de Mensaje de Datos ocasionada por la entrega de documentos apócrifos por parte del comerciante - usuario.

7.4 Responsabilidades del comerciante – usuario

El comerciante – usuario es el responsable de:

1. Guardar las llaves de acceso al servicio de Constancia de Conservación de Mensaje de Datos al igual que las constancias emitidas y la debida gestión de los Mensajes de Datos por las que solicitó el servicio.

2. Administrar el almacenamiento de las Constancias de Conservación de Mensaje de Datos por medios propios o mediante la contratación de un tercero.

8. Constancia de Conservación de Mensaje de Datos

Garantizan la integridad de los mensajes de datos en el transcurso del tiempo.

El servicio se proporciona a través de una autoridad de Constancia de Conservación de Mensaje de Datos para la emisión de constancias y un portal web para la creación de solicitudes y administración de documentos:

8.1 Identificador de Objeto

El identificador de Objeto proporcionado por la Secretaría de Economía para el servicio de Constancia de Conservación de Mensajes de Datos es: 2.16.484.101.10.316.100.9.1.2.2.3

8.2 Autoridad de Constancia de Conservación de Mensaje de Datos

La emisión de Constancia de Conservación de Mensaje de Datos cumple con lo establecido por el RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) y el RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).

El certificado utilizado para la emisión de Constancia de Conservación de Mensaje de Datos es almacenado en un HSM con certificación FIPS140-2 nivel l 3.

Cuenta con sincronización del tiempo con el Centro Nacional de Metrología (CENAM).

Este servicio se proporciona a través de un web service con los métodos de Emisión y Consulta que se detallan a continuación:

NOTA**:**
En el servicio de emisión de Constancia de Conservación de Mensaje de Datos y la Consulta de éstas, la solicitud va firmada utilizando el certificado privado de firma electrónica del solicitante con el objetivo de asegurar la confidencialidad, disponibilidad, integridad y no repudio de la información enviada en los mensajes de datos.

Emisión:

Se recibe la solicitud de la Constancia de Conservación de Mensaje de Datos con extensión .ccq con el estándar ASN.1 que contiene la llave pública y la petición firmada con la firma electrónica del cliente.

1. Se validan los siguientes elementos:

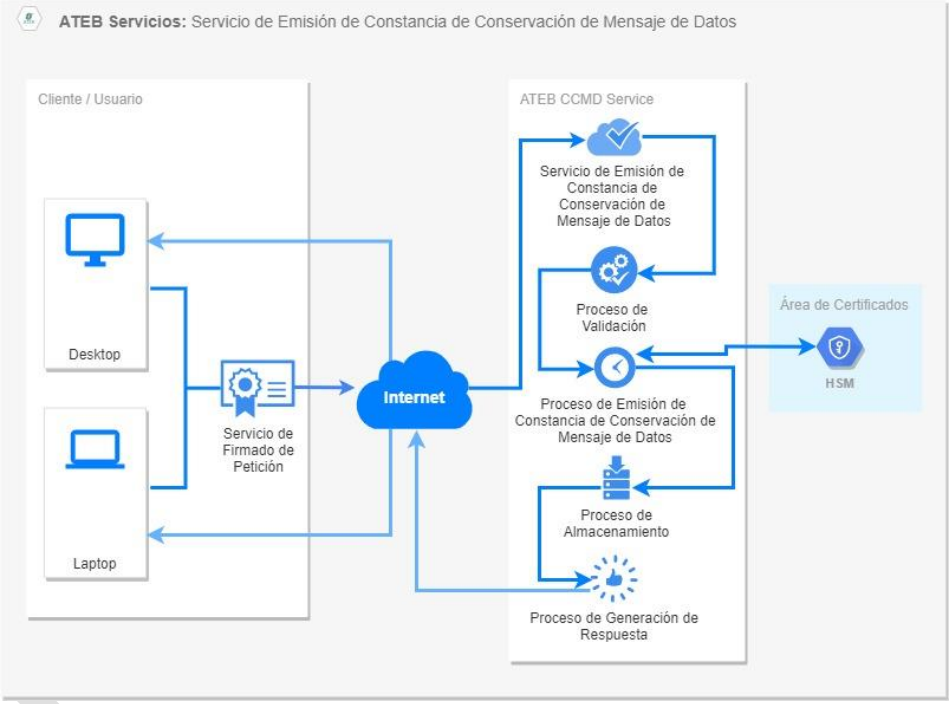
   - **RFC**. Se verifica consultando el certificado público de firma electrónica del cliente contra la información almacenada en la base de datos.
   - **Vigencia**. Se verifica consultando los datos del certificado público de firma electrónica del cliente.

- **Firma Electrónica** de la solicitud de la Constancia de Conservación de Mensaje de Datos. Se validan en conjunto la petición firmada y el certificado público de firma electrónica del cliente para asegurar que la petición proviene del par de llaves con la que se firmó.

2. Se emite la Constancia de Conservación de Mensaje de Datos.

3. Se genera la respuesta
4. Se almacena la Constancia de Conservación de Mensaje de Datos para su futura verificación
5. Se envía la respuesta a la solicitud de Constancia de Conservación de Mensaje de Datos que contiene un archivo con extensión .ccr con el formato ASN.1 del RFC 3161

A continuación, se muestra el diagrama del proceso de emisión de Constancia de Conservación de Mensajes de Datos:



Consulta:

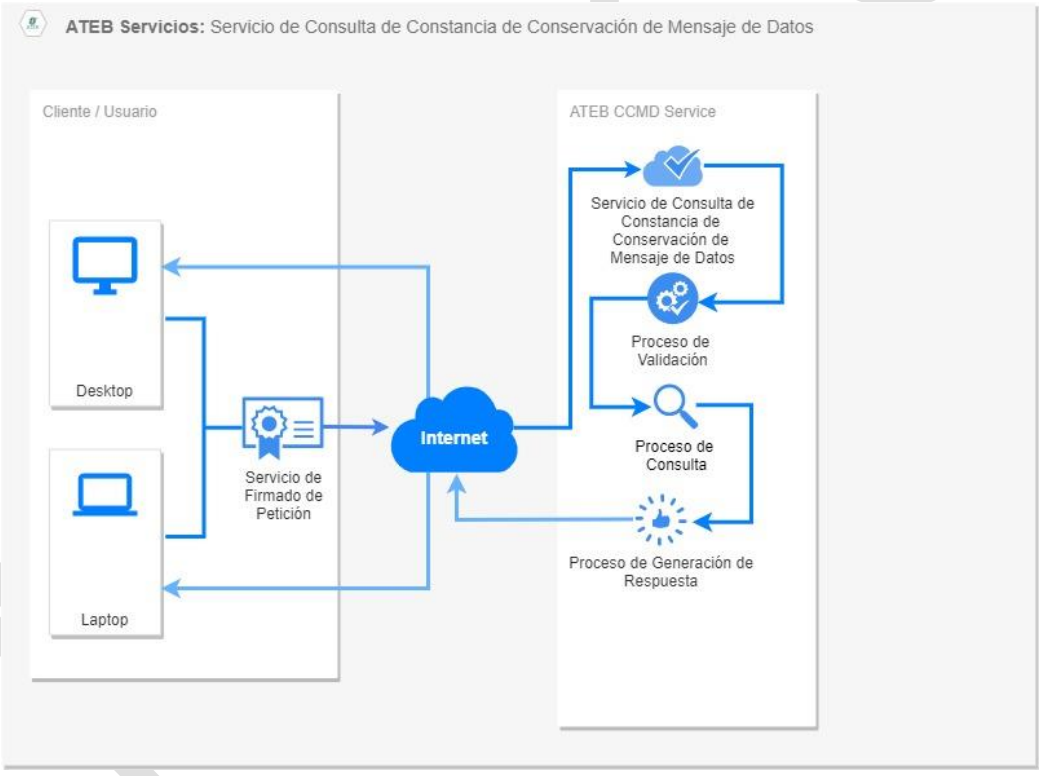
1. Recibe la solicitud de validación de Constancia de Conservación de Mensaje de Datos con extensión .ccq con el estándar ASN.1 que contiene la llave pública y la petición firmada con la firma electrónica del cliente.

2. Se validan los siguientes elementos:

a. **RFC**. Se verifica consultando el certificado público de firma electrónica del cliente contra la información almacenada en la base de datos.
b. **Vigencia.** Se verifica consultando los datos del certificado público de firma electrónica del cliente.
c. **Firma** de la petición de la Constancia de Conservación de Mensaje de Datos. Se validan en conjunto la petición firmada y el certificado público de firma electrónica del cliente para asegurar que la petición proviene del par de llaves con la que se firmó.

3. Realiza la búsqueda de la Constancia de Conservación de Mensaje de Datos y envía la respuesta a la solicitud, dicha respuesta, contiene una estructura de error en caso de no encontrar un resultado a su búsqueda, en caso de ser exitosa se envía un archivo con extensión .ccr con el formato ASN.1.del RFC 3161.

A continuación, se muestra el diagrama de consulta de Constancia de Conservación de Mensaje de Datos:



Portal web

El portal web cuenta con los siguientes módulos:

- **Administración del portal:** La administración incluye entre otras cosas, la configuración de los usuarios que tendrán acceso al sistema; creación de áreas para organizar los

documentos y la asignación de permisos de visualización de usuarios a las áreas correspondientes.

- **Documentos:** En donde se realiza el manejo de documentos electrónicos:

  Carga de documentos, se puede realizar de forma manual desde la interfaz web o de forma automática con interfaces de integración con aplicaciones que generan documentos electrónicos.

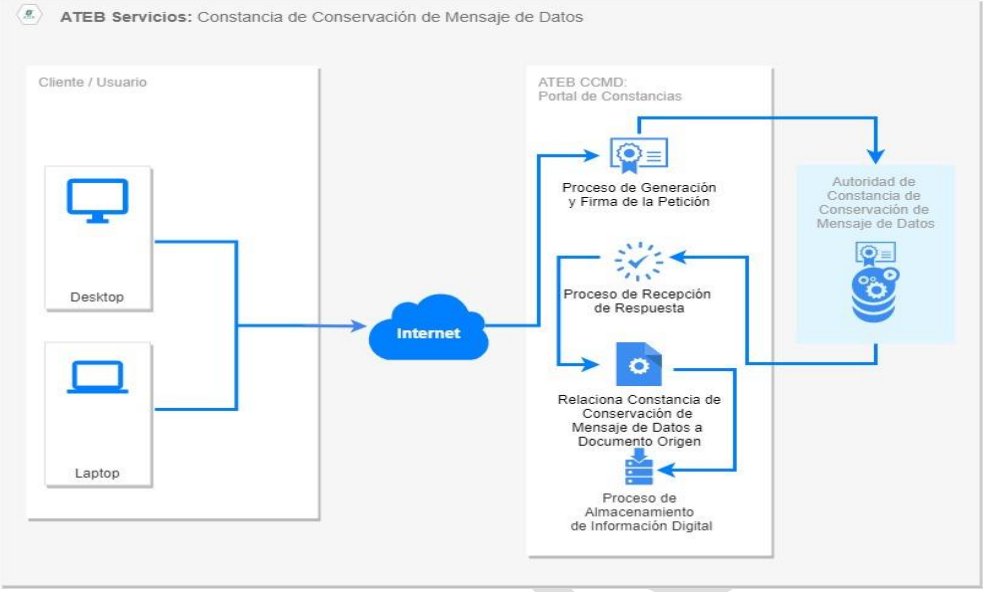
  Solicitar Constancia de Conservación de Mensaje de Datos, de los documentos cargados al portal.

  Cuando el usuario solicita una constancia para un documento, el portal genera la solicitud, la envía a la autoridad de Constancia de Conservación de Mensaje de Datos, recibe la constancia y la asocia al documento permitiendo la consulta o descarga del documento junto con su constancia.

Emisión de Constancia de Conservación de Mensaje de Datos desde el portal:

1. Usuario ingresa al portal.
2. Selecciona archivo a procesar y solicita Constancia de Conservación de Mensaje de Datos.
3. El portal genera solicitud de Constancia de Conservación de Mensaje de Datos y la firma electrónicamente con las llaves del cliente.
4. El portal envía la solicitud a la autoridad de emisión de Constancia de Conservación de Mensaje de Datos.
5. Recibe respuesta.
6. Almacena la Constancia de Conservación de Mensaje de Datos, asociándola al documento origen para su posterior consulta.

A continuación se muesra el diagrama de generación de Constancia de Conservación de Mensaje de Datos:



9. Seguridad en las aplicaciones

Los servicios de Prestador de Servicios de Certificación de ATEB utilizan los siguientes elementos de seguridad para garantizar un entorno seguro para la información digital del cliente:

Almacenamiento de contraseñas cifradas:

Las contraseñas de cada uno de los usuarios serán cifradas bajo el método de cifrado MD5 con el cual aseguramos que solo sea el cliente quien sepa su contraseña, siendo imposible para cualquier otra persona conocerla.

Método o función de autenticación:

El método “Authenticate” utiliza un sistema de petición por token. Siempre y cuando las credenciales del usuario sean correctas, se le otorgará un primer token que estará ligado a la información del cliente que hace la petición y con el cual podrá inicializar el servicio de Constancia de Conservación de Mensaje de Datos y poder obtener un nuevo token para realizar el consumo de este; cabe mencionar que cada token permitirá la ejecución de una sola transacción y luego será desechado.

Credenciales a bases de datos cifradas:

Las credenciales de acceso a las bases de datos se encuentran cifradas con el fin de no exponerlas en texto plano dentro de sus documentos de configuración.

Almacenamiento de Constancia de Conservación de Mensaje de Datos cifrado:

Cada Constancia de Conservación de Mensaje de Datos que se genera es almacenada de forma cifrada en bases de datos con la finalidad de poder tener control sobre las diferentes constancias emitidas y que estas no puedan ser generadas nuevamente.

Almacenamiento de información digital cifrada:

Cada documento digital, Constancia de Conservación de Mensaje de Datos, solicitud y respuesta a los servicios de Prestador de Servicios de Certificación de ATEB, son almacenados de forma cifrada en bases de datos con la finalidad de cumplir con los principios de la Seguridad de la Información.

Antivirus:

El análisis y monitoreo de seguridad de los componentes informáticos de los servicios de Prestador de Servicios de Certificación de ATEB para la protección antimalware es el software Bit Defender

10. Administración de la seguridad

Para el servicio de Constancia de Conservación de Mensaje de Datos, ATEB cuenta con un documento denominado Políticas de Seguridad de la Información en el cual se detallan los lineamientos a los cuales las partes interesadas deben apegarse para poder realizar las funciones laborales de la organización, un Sistema de Gestión de Seguridad de la Información para este servicio en donde se detallan los procesos, procedimientos y demás documentos que le permiten a ATEB implementar controles para preservar la Seguridad de la Información del servicio en cuanto a la disponibilidad, confidencialidad e integridad de este, así mismo el área de Seguridad de la Información se encarga de realizar un Plan Anual de Seguridad en el cual se detallan las actividades y fechas programadas de ejecución.

ATEB realiza anualmente un Análisis de Evaluación de Riesgos con el objetivo de definir los controles preventivos, de detección y correctivos, así como las medidas de implementación técnicas, administrativas y operativas que se instrumenten en la empresa.

La Declaración de Prácticas establecida en el presente documento regula el servicio de Constancia de Conservación de Mensaje de Datos, la cual se debe auditar periódicamente ya sea interna o externamente para determinar las mejoras por realizar y efectuar los cambios requeridos tanto a nivel documental como de infraestructura. ATEB se asegura de que las prácticas declaradas se implementen adecuadamente mediante la revisión periódica de su funcionalidad.

ATEB cuenta con diversos procedimientos referenciados en el SGSI para el servicio de Constancia de Conservación de Mensaje de Datos, los cuales le dan la pauta para la implementación de los diferentes controles necesarios para afianzar la Seguridad de la Información y la disponibilidad en el servicio de Constancia de Conservación de Mensaje de Datos, de igual manera se tienen documentados los procedimientos y demás documentación solicitada por las Reglas Generales para a las que deben sujetarse los Prestadores de Servicio de Certificación en los cuales se establecen las medidas y controles de seguridad para el resguardo de la información y lo relacionado al servicio de Constancia de Conservación de Mensaje de Datos.

Al igual que los procedimientos que permiten a ATEB brindar el servicio de Constancia de Conservación de Mensaje de Datos de manera ininterrumpida, se deben tener presentes las medidas correspondientes en el tema de la seguridad física, para lo cual ATEB cuenta con la Política de Seguridad Física para este servicio.

Debido al tipo de información que se maneja en la organización se deben segregar las áreas restringidas mediante controles de accesos físicos, guardias para el edificio en general, personal de vigilancia propio para la empresa capacitado y calificado para el desempeño de sus funciones y circuitos cerrados de televisión o CCTV, también se debe utilizar bloqueos visuales en ventanas y puertas para no dejar a la vista las actividades que en ella se desarrollan, tanto en las oficinas centrales como en los diferentes centros de datos con que ATEB cuenta para soportar los diferentes servicios que ofrece, las oficinas centrales están en la ciudad de México en la Alcaldía Cuauhtémoc, el primer centro de datos es TRIARA y se encuentra en la ciudad de Querétaro, el segundo centro de datos es MCM ubicado en la ciudad de México en la Alcaldía Miguel Hidalgo, ambos centros de datos cuentan con los medios, servicios e instalaciones necesarios para el desarrollo de las actividades que ATEB ejerce, así mismo ambos cuentan con las medidas y controles de seguridad solicitados por las normas nacionales e internacionales en Seguridad de la Información, garantizando así la disponibilidad tanto de la información como de los servicios brindados por ATEB.

Estas medidas y controles incluyen por ende el acceso físico y lógico del personal a las oficinas centrales y los centros de datos para lo cual se deben llevar a cabo los debidos Procedimientos de reclutamiento y selección y contratación de personal del área de Capital Humano, ya que el personal encargado de los servicios relacionados con la Constancia de Conservación de Mensaje de Datos debe cumplir con el perfil y los requisitos solicitados por la Secretaría de Economía en las Reglas Generales a las que deben sujetarse los Prestadores de Servicios de Certificación.

ATEB adicional al personal solicitado por la Secretaría de Economía, requiere de personas que cumplan con el requisito de conocimiento y experiencia, a través de una formal capacitación y experiencia real sobre los temas para poder brindar el servicio de Constancia de Conservación de Mensaje de Datos.

Los colaboradores confiables incluyen roles que involucran las siguientes responsabilidades:

- Oficiales de seguridad: Responsabilidad general de administrar la implementación de las prácticas de seguridad.

- Administradores del sistema: Instalar, configurar y mantener los sistemas confiables de la ASDT.

- Operadores del sistema: Operar el sistema de Constancia de Conservación de Mensaje de Datos de manera confiable y hacer copias de seguridad y recuperación día a día.

- Auditores del sistema: Revisar archivos y registros de auditoría de los sistemas confiables del servicio de Constancia de Conservación de Mensaje de Datos.

El personal ejercerá procedimientos administrativos y de gestión, y procesos que están en línea con la Seguridad de la Información de la ASDT.

11. Controles para asegurar auditorías

ATEB cuenta con un Procedimiento de Auditoría Interna (PRO-SEG-AUI-003) y otro Procedimiento de Auditoría Externa (PRO-SEG-AUE-003) los cuales tienen como objetivo el determinar los lineamientos y bases para establecer la forma correcta de realizar auditorías y emitir los resultados correspondientes e informarlos a Dirección General junto con las partes interesadas.

Estos documentos aplican para:

a) Todas las auditorías internas que se requieran hacer en la organización a fin de encontrar mejoras en los procesos y actividades actuales e implementarlas para una mejor eficacia en la operación del negocio.
b) Las normas ISO/IEC 27001:2013 y ISO/IEC 27002:2013.
c) El seguimiento de la remediación de observaciones (Necesidad de Mejora y No Conformidades) realizadas en otras auditorías.

Con base en estos procedimientos se realizarán las auditorías correspondientes para asegurar la revisión semestral del Manual de Declaración de Prácticas para el servicio de Constancia de Conservación de Mensaje de Datos .

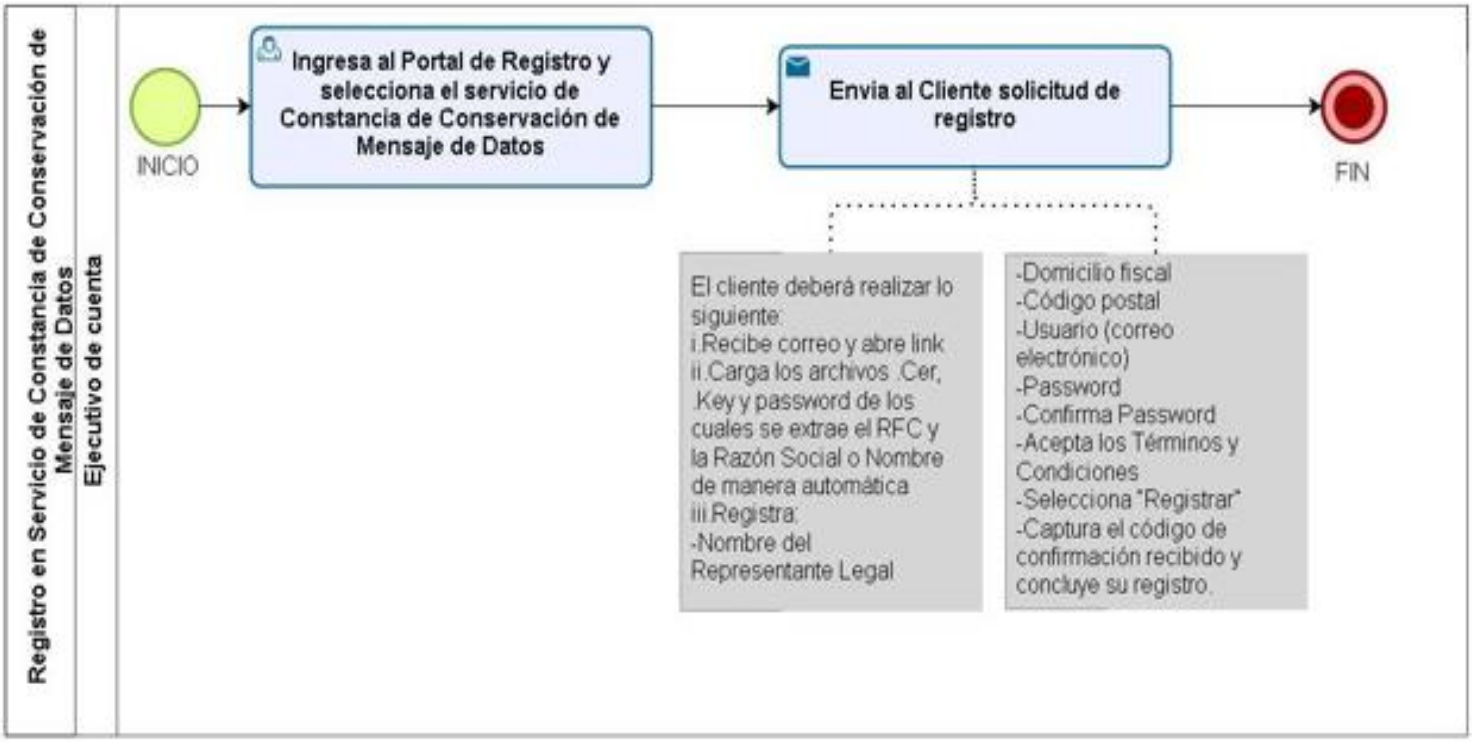
Los resultados de las auditorías se integrarán en un Reporte de Auditoría de PSC (REP-SEG-PSC-068) en el cual se desglosará cada uno de los documentos revisados y se verificará si se cumplió o no con cada uno de los controles requeridos por el auditor, con este documento se verificarán las áreas de oportunidad y se garantizará el cumplimiento de los controles en posteriores auditorías.

Esta documentación será compartida por los involucrados a través de un repositorio SVN asignado para este fin.

12. Procedimientos de Registro en servicio de constancias de conservación de mensajes de datos y gestión de fallas durante el funcionamiento de los servicios con el cliente

12.1 Procedimiento 1: Registro en Servicio de Constancia de Conservación de Mensaje de Datos

- Diagrama General del procedimiento



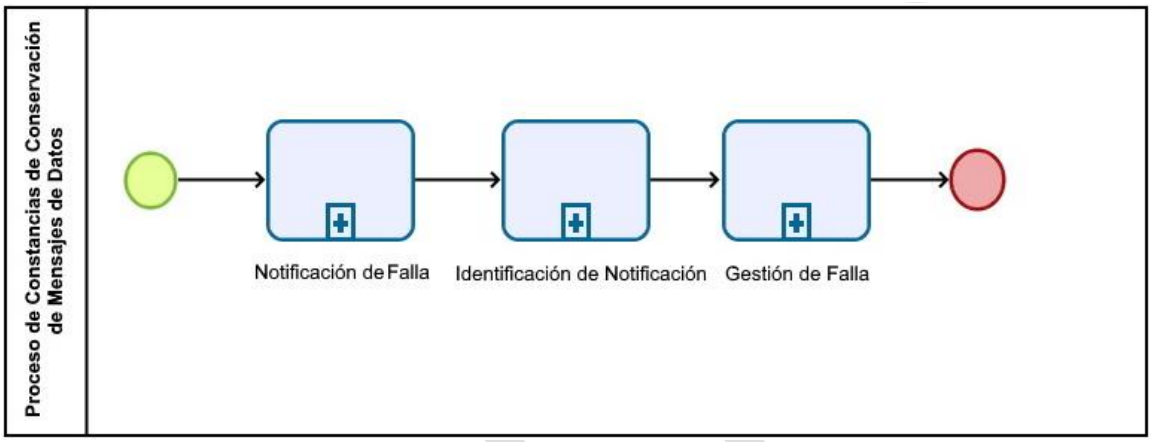
- Descripción del proceso

No.	Actividad	Descripción	Responsable	Entrada	Salida
1	Ingresar al Portal de Registro y seleccionar el servicio de Constancia de Conservación de Mensaje de Datos	Ingresa al portal de registro y selecciona el servicio de Constancia de Conservación de Mensaje de Datos	Ejecutivo de cuenta	Contrato firmado de prestación del servicio	Selección de servicio contratado por el cliente
2	Enviar al Cliente solicitud de registro	● Envía al Cliente la Solicitud de Registro al capturar su correo electrónico en el portal de Registro ● El Cliente deberá realizar lo siguiente: ● Recibe correo y abre link ● Carga los archivos .Cer, .Key y password de los cuales se extrae el RFC y la Razón Social o Nombre de manera automática ● Registra: ● Nombre del Representante Legal ● Domicilio fiscal ● Código postal ● Usuario (correo electrónico) ● Password ● Confirma Password ● Acepta los Términos y Condiciones ● Selecciona “Registrar” ● Captura el código de confirmación recibido y concluye su registro.	Ejecutivo de cuenta	Selección de servicio contratado por el cliente	Correo con Solicitud de Registro enviado y registro realizado
FIN DEL PROCEDIMIENTO					

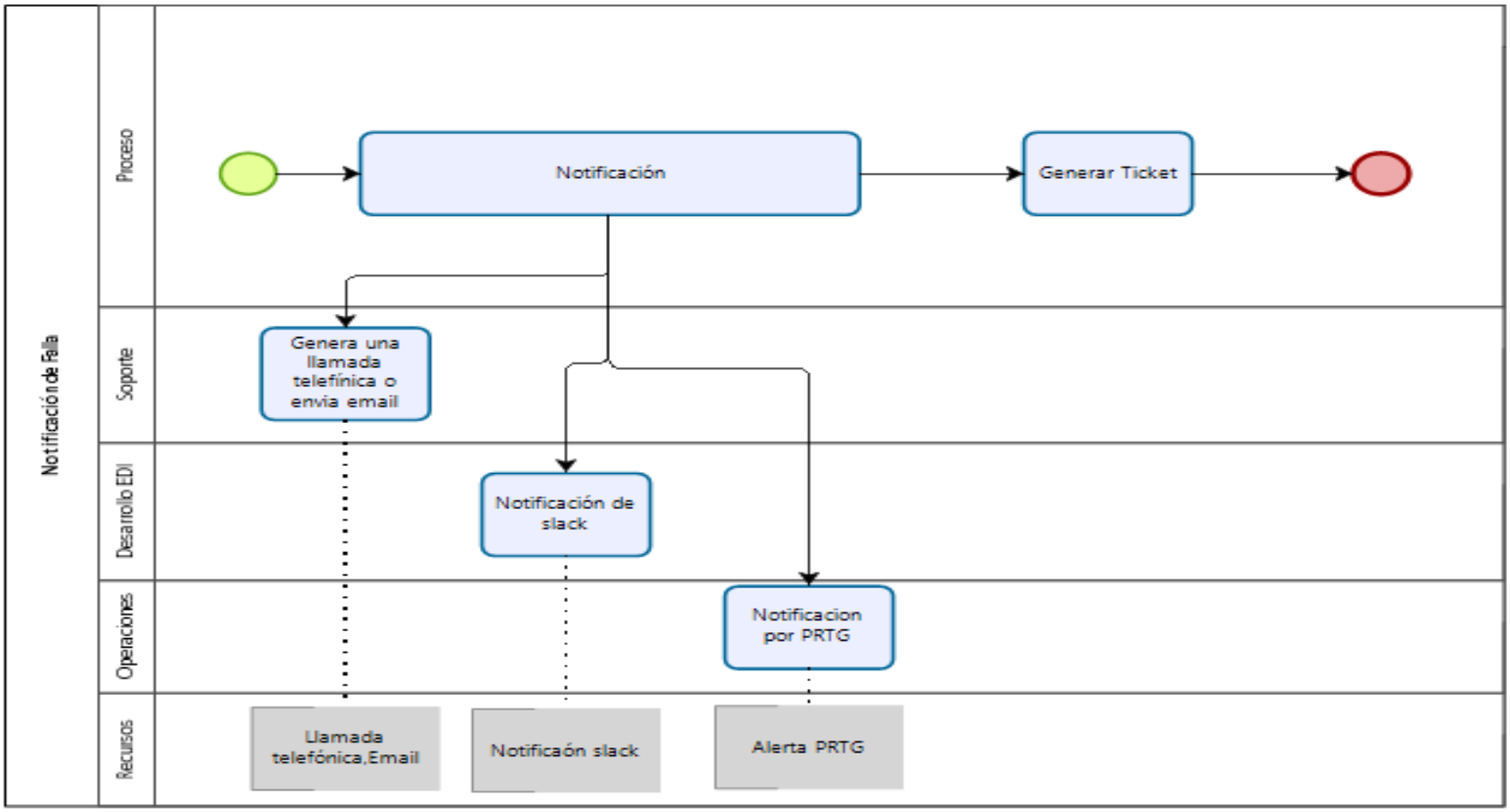
12.2 Procedimiento 2: Gestión de Fallas durante el Funcionamiento de los Servicios con el Cliente

Cada servicio provisto por el área de PSC cuenta con un procedimiento a seguir para poder detectar las fallas que puedan poner el riesgo el buen funcionamiento de este; se detallan a continuación.

- Diagrama general del procedimiento



- Subproceso 1: Notificación de Falla

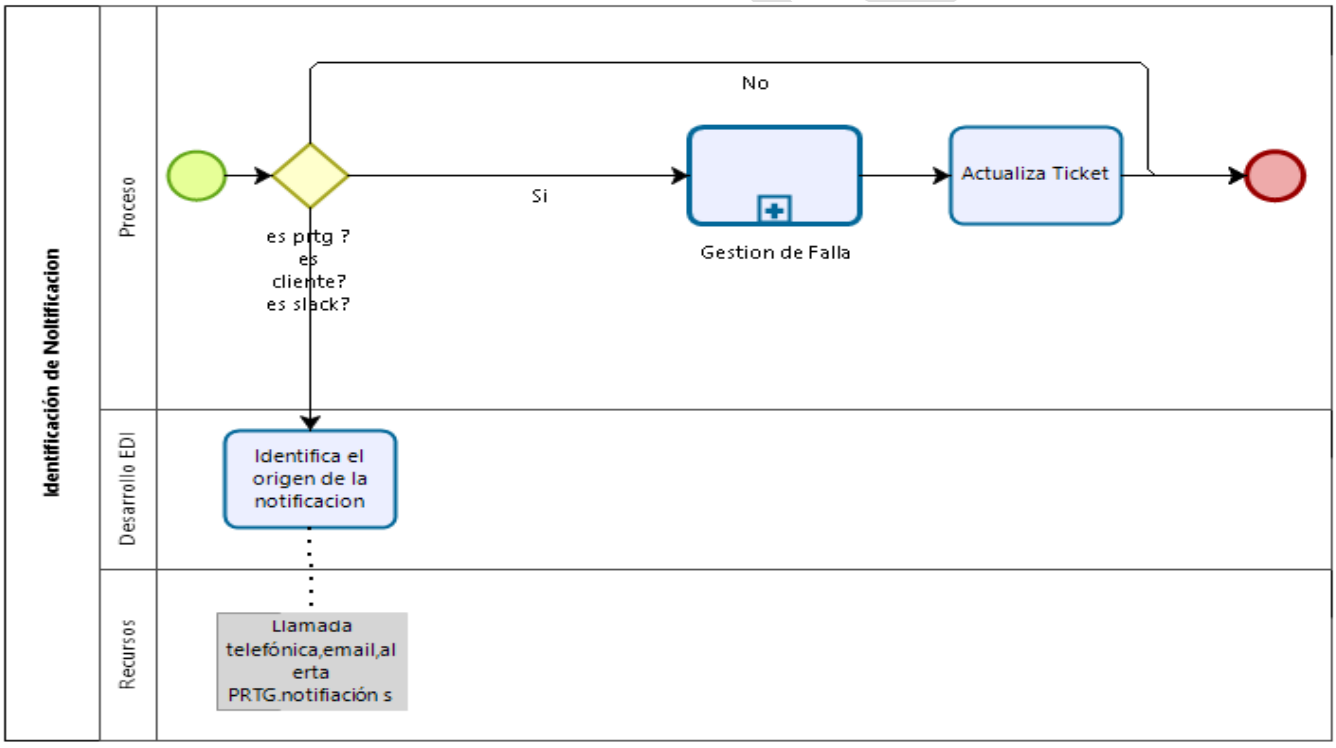


- Descripción del subproceso

No.	Actividad	Descripción	Responsable	Entrada	Salida
1	Notificación	Se genera un reporte de falla que posteriormente sirve para crear una notificación	Producto o Servicio de ATEB, Cliente	Falla	Reporte de Falla
2	Generación de Notificación	Se genera una notificación que puede ser atendida de diferente forma dependiendo del caso	Producto o Servicio de ATEB, Cliente	Reporte de Falla	Notificación de Falla
Si es PRTG pasar a la actividad 3, **Si es Slack pasar a la actividad 4,** **Si es notificación del Cliente, pasar a la actividad 5**					

3	Notificación PRTG	Se genera una Alerta a través de alerta PRTG	Operaciones	Llamada telefónica/Presencial	Ticket Generado
FIN DEL PROCEDIMIENTO					
4	Notificación Slack	Se genera una Alerta a través de una notificación Slack	Desarrollo EDI	Notificación por Slack	Ticket Generado
FIN DEL PROCEDIMIENTO					
5	Notificación del Cliente	Se genera una Alerta a través de llamada telefónica / Presencial	Soporte	Llamada telefónica/Correo Electrónico	Ticket Generado
FIN DEL PROCEDIMIENTO					

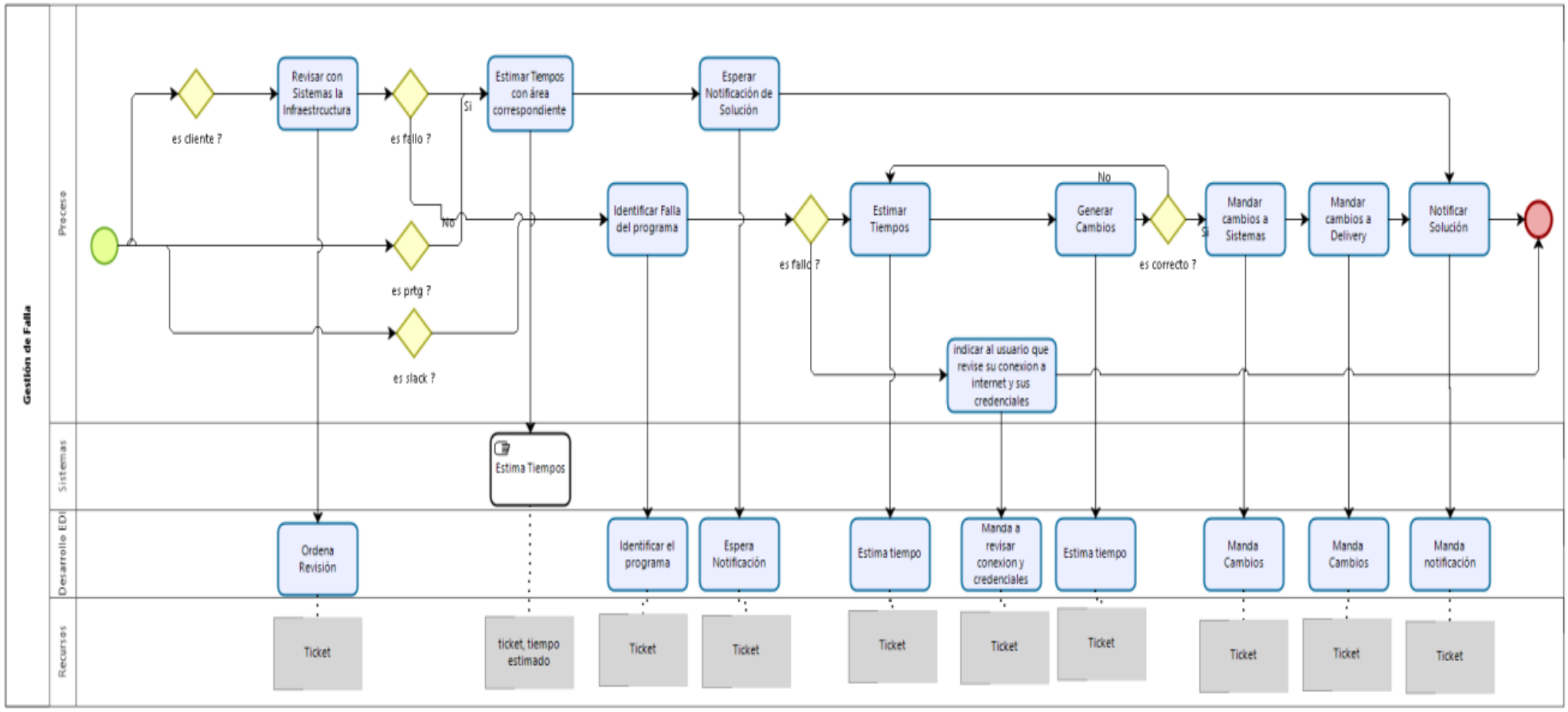
- Subproceso 2: Identificación de Notificación



- Descripción del subproceso

No.	Actividad	Descripción	Responsable	Entrada	Salida
Si es una notificación del Cliente, PRTG o Slack, pasar a la actividad 1, de lo contrario pasar a FIN					
1	Gestión de Falla	Ejecuta el procedimiento de Gestión de Falla	Operaciones / Desarrollo EDI	Ticket	Ticket canalizado al área correspondiente
2	Actualizar Ticket	Se actualiza la información del ticket, ya sea para su reasignación, comentario o cierre	Operaciones / Desarrollo EDI	Ticket canalizado al área correspondiente	Ticket Actualizado
FIN DEL PROCEDIMIENTO					

- Subproceso 3: Gestión de Falla



- Descripción del proceso

No.	Actividad	Descripción	Responsable	Entrada	Salida
Si es Notificación del Cliente pasar a la actividad 1, Si es Notificación de PRTG pasar a la actividad 2, Si es Notificación de Slack pasar a la actividad 5,					
1	Revisar con Sistemas la Infraestructura	Verificar con Sistemas todos aquellos puntos de conexión que podrían afectar al funcionamiento del servicio.	Desarrollo EDI	Ticket	Ticket Actualizado
Si es falla de Sistemas pasar a la actividad 2, de lo contrario ir a la actividad 4					
2	Estimar Tiempos con Área Correspondiente	Sistemas deberá revisar con el área correspondiente, los tiempos estimados para la solución de la falla.	Sistemas	Ticket / Tiempo Estimado	Ticket Actualizado
3	Esperar Notificación de Solución	El ticket debe quedar en espera hasta que se dé solución a la falla.	Desarrollo EDI	Ticket	Ticket Actualizado
Pasar a la actividad 10					
4	Identificar falla del programa	Se busca la razón de ocurrencia de la falla dentro del software.	Desarrollo EDI	Ticket	Ticket Actualizado
Si es falla del programa, pasar a la actividad 5, de lo contrario ir a la actividad 10					
5	Estimar Tiempos	Se estiman los tiempos de desarrollo para la solución.	Desarrollo EDI	Ticket	Ticket Actualizado
6	Generar Cambios	Se hacen las modificaciones pertinentes para solucionar la falla.	Desarrollo EDI	Ticket	Ticket Actualizado
Si los cambios fueron correctos, pasar a la actividad 7, de lo contrario regresar a la actividad 5					
7	Mandar Cambios a Sistemas	Se mandan los cambios del programa a sistemas.	Desarrollo EDI	Ticket	Ticket Actualizado
8	Mandar Cambios a Delivery	Se mandan los cambios del programa a Delivery.	Desarrollo EDI	Ticket	Ticket Actualizado
Pasar a la actividad 10					

9	Indicaciones al Usuario	Indicar al usuario que revise su conexión a Internet y sus credenciales, así como los puntos de conexión a los que apunta (si es que los hay).	Desarrollo EDI	Ticket	Ticket Actualizado
10	Notificar Solución	Una vez con la solución, esta se le notifica al cliente.	Desarrollo EDI	Ticket	Ticket Actualizado
FIN DEL PROCEDIMIENTO					

13. Gestión de las claves privadas y públicas de la autoridad del servicio de Constancia de Conservación de Mensaje de Datos

13.1 Generación de la clave

La generación de las claves utilizadas para el servicio de Constancia de Conservación de Mensaje de Datos se realiza a 4096 bits y un algoritmo de firma SHA256RSA en equipos HSM, de la marca FutureX, modelo Vectera Plus 100, los cuales cuentan con la Certificación FIPS140-2 nivel l 3.

13.2 Segregación de funciones de seguridad de las llaves de acceso al HSM

La descripción detallada de las responsabilidades de los recursos que resguardarán las llaves y tarjetas del HSM, juegan un papel muy importante en la seguridad de la información de la empresa, de aquí se delimitan las responsabilidades que cada uno de los involucrados deberán cubrir y ejecutar.

La información es resguardada bajo 3 niveles:

- 1er Nivel Llave de acceso
- 2do Nivel Tarjeta inteligente
- 3er Nivel Contraseña

El modo Administrador en el HSM requiere tener 2 de 3 tarjetas inteligentes con contraseñas presentes.

Tarjetas Inteligentes

Cada HSM tiene 3 juegos de 3 tarjetas inteligentes.

13.3 NIVELES DE SEGURIDAD

- 1er. Nivel

Dirección General resguarda un juego de tarjetas de cada HSM.

- 2º. Nivel

El segundo juego de tarjetas se almacena con el 1er juego resguardadas en el mismo lugar físico con diferente contraseña.

- 3er. Nivel

Contraseñas de acceso asociada a la llave inteligente que es definida por cada responsable.

13.4 RESPONSABLES DE RESGUARDO

Cada juego de tarjetas tiene asociada una contraseña de seguridad. Los juegos de tarjetas están asignados a los siguientes recursos:

Juego de Tarjetas Inteligentes para HSM Productivo (Administrator Card)

# Set	Responsable	Tipo de tarjeta
1°.	DIRECCIÓN GENERAL	Administrator Card
2°.	DIRECCIÓN GENERAL EDI	Administrator Card
3°.	DIRECCIÓN GENERAL COLOMBIA	Administrator Card

Juego de Tarjetas Inteligentes para HSM Productivo (Custodian Card)

# Set	Responsable	Tipo de tarjeta
1°.	Gerencia Ventas	Custodian Card
2°.	Gerencia Delivery	Custodian Card
3°.	Gerencia Sistemas	Custodian Card

Juego de Tarjetas Inteligentes para HSM Productivo (Masterkey Card)

# Set	Responsable	Tipo de tarjeta
1°.	Dirección General	MasterKey Card
2°.	Dirección General	MasterKey Card
3°.	Dirección General	MasterKey Card

La asignación y responsabilidad será registrada dentro de las **Cartas compromiso de asignación**

13.4.1 Lugar de resguardo de las llaves de encendido

Tipo de llaves	Lugar de resguardo
Administrator Card	Las resguardan cada responsable en sitio seguro
Custodian Card	Las resguardan cada responsable en sitio seguro
Masterkey Card	Se resguarda en la oficina de ATEB en la caja fuerte

13.5 ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE LA CLAVE

Incluyendo las llaves administrativas, el HSM Vectera Plus 100 de Futurex puede guardar hasta 25000 llaves, las cuales se guardan en compartimientos o SLOTS. Estas llaves se encuentran encriptadas en la base de datos a través de la MFK, por lo que se almacenan de manera segura en el servidor, las cuales se borran en caso de que el servidor detecte algún intento de intrusión no autorizada.

13.5.1 Llaves operativas

Este tipo de llaves son las que se utilizan para las operaciones criptográficas en las diferentes aplicaciones que se requieran. Dependiendo de la herramienta a utilizar, se necesita ya sea un usuario administrador o un usuario criptográfico para poder crearlas, sin embargo, el único que puede usarlas para la operación correspondiente es el usuario criptográfico.

Estas llaves se almacenan en la base de datos del HSM y se encuentran en todo momento encriptadas por la MFK. También se pueden encriptar ya sea con la llave BAK o la KEK para la operación que sea necesaria en cada caso. El personal de Cega Security recomienda que la contraseña del usuario criptográfico sea lo suficientemente segura pues es la que utilizarán las aplicaciones que se conecten al HSM para realizar las operaciones criptográficas.

En los siguientes apartados se explica el procedimiento para la administración de llaves a través del Excrypt Manager.

13.5.2 Generación de llaves desde un requerimiento específico

La generación de las claves criptográficas se realizará a partir de un requerimiento específico proporcionado por la Secretaría de Economía y será celebrado con la presencia del siguiente personal:

#	Personal	Entidad
1	Dirección General	ATEB
2	Dirección PSC	ATEB
3	Profesional informático	ATEB

4	Auxiliar Informático de Seguridad	ATEB
5	Personal Secretaría de Economía	Secretaría Economía
6	Personal de implementación	CEGASecurity

13.5.3 Requerimientos

1. HSM Futurex.
2. HSM instalado y operativo.

13.5.4 Respaldo y restauración de llaves

El HSM Vectera Plus cuenta con la capacidad de realizar respaldos de la configuración actual y las llaves almacenadas. Estos respaldos se encriptan con la llave BAK lo que permite la manipulación segura de la información fuera del servidor. El tener estos archivos de respaldo nos permite poder replicar la configuración para una arquitectura de múltiples HSM o para recuperar la información en caso de que haya sido necesario borrar la información o se haya comprometido la integridad de ésta.

El personal del proveedor Cega Security recomienda realizar un respaldo al terminar la configuración inicial del HSM, y cada vez que se genera una nueva llave para evitar la pérdida de información.

Al terminar el procedimiento es importante definir el lugar o la persona que se hará responsable de guardar los archivos correspondientes.,

Para poder cargar un respaldo, es necesario que el HSM se encuentre en un número de firmware igual o superior al que se usó cuando se generó el archivo.

Generación de respaldo

1. Seleccionar la opción de “Maintenance”.
2. En la sección de “Backup/Restore” seleccionar el botón de “Backup Config” o “Backup Keys” para realizar el respaldo correspondiente.
3. Cargar la llave BAK en caso de que no se haya realizado la carga previamente.
4. Seleccionar la ruta y el nombre del archivo donde se guardará el respaldo.
5. Se mostrará una barra de progreso de la exportación, encriptado con la llave BAK. Al finalizar seleccionar “Finish” y se podrá encontrar el archivo en la ruta asignada.

Restauración/replicación de respaldo

1. Seleccionar la opción de “Maintenance”
2. En la sección de “Backup/Restore” seleccionar el botón de “Restore Config” o “Restore Keys” para realizar la replicación correspondiente
3. Cargar la llave BAK en caso de que no se haya realizado la carga previamente
4. Seleccionar la ruta y el nombre del archivo desde donde se cargará el respaldo

5. Se mostrará una barra de progreso de la replicación. Al finalizar seleccionar “Finish” y se podrá encontrar el archivo en la ruta asignada

13.6 DISTRIBUCIÓN DE LA CLAVE PÚBLICA

Para la emisión de Constancia de Conservación de Mensaje de Datos, la distribución de la llave pública del Prestador de Servicio de Certificación se envía en la respuesta (tsr) de la solicitud de Constancia de Conservación de Mensaje de Datos (tsq), por lo que verificamos que estos dos elementos tengan relación entre sí.

Además, se dispondrán las claves públicas vigentes para el servicio emisión de Constancia de Conservación de Mensaje de Datos en el sitio web de ATEB Servicios https://www.ateb.mx/psc.html.

Adicionalmente dichas claves son publicadas por la Secretaría de Economía en el portal www.firmaelectronica.gob.mx.

13.7 FIN DEL CICLO DE VIDA DE LA CLAVE

Al concluir el periodo de validez de las claves, se realiza el borrado de estas en el dispositivo HSM.

14. Suspensión temporal o definitiva de actividades de ATEB como autoridad del servicio de Constancia de Conservación de Mensaje de Datos

A continuación, se detallan las diferentes circunstancias de la suspensión con base en los siguientes reglamentos:

14.1 DE LAS REGLAS GENERALES A LAS QUE DEBERÁN SUJETARSE LA AUTORIDAD DEL SERVICIO DE CONSTANCIA DE CONSERVACIÓN DE MENSAJE DE DATOS

La autoridad que en términos del artículo 104 fracción VI del Código de Comercio, quiera cesar de manera voluntaria su actividad, previo pago de derechos, tiene que informar a la Secretaría, el motivo de dicho cese con un término de cuarenta y cinco días de anticipación, a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16o. del Reglamento, así como con lo estipulado en los TÍTULOS, SEXTO, SÉPTIMO y OCTAVO de las Reglas. En este supuesto los registros y archivos pasarán a otro Prestador de Servicios de Certificación que cumpla con las características similares al que llevaba dicho servicio.

14.2 DEL CÓDIGO DE COMERCIO

Tomando como referencia el artículo 97, cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante.
II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante.
III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

De acuerdo con el artículo 100, podrán ser Prestadores de Servicios de Certificación previa acreditación ante la Secretaría:

I. Los notarios y corredores públicos.
II. Las personas morales de carácter privado, y
III. Las instituciones públicas, conforme a las leyes que les son aplicables.

Las facultades de expedir certificados o de prestar servicios relacionados con la conservación de mensajes de datos, así como fungir en calidad de tercero legalmente autorizado conforme a lo que se establezca en la norma oficial mexicana, no conllevan fe pública por sí misma, así, los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel o mensajes de datos.

Quien aspire a obtener la acreditación como prestador de servicios de certificación, podrá solicitarla respecto de uno o más servicios, a su conveniencia.

En referencia al artículo 102, cuando haya obtenido la acreditación de la Secretaría deberá notificar a ésta la iniciación de la prestación de los servicios a que haya sido autorizados, dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

a) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual podrá otorgarse para autorizar la prestación de uno o varios servicios, a elección del solicitante, y no podrá ser negada si éste cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar los servicios, a efecto de garantizar la seguridad de la información y su confidencialidad.
II. Contar con procedimientos definidos y específicos para la prestación de los servicios, y medidas que garanticen la seguridad de los Certificados, la conservación y consulta de los registros, si es el caso.
III. Quienes operen o tengan acceso a los sistemas de certificación ATEB no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

IV. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y
V. Registrar su Certificado ante la Secretaría.

Así mismo y de acuerdo con el artículo 110, al incumplir con las obligaciones que se le imponen en el mencionado Código, el reglamento o la norma oficial mexicana sobre conservación de mensajes de datos que para tal efecto emita la Secretaría, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

14.3 DEL REGLAMENTO DEL CÓDIGO PSC

ATEB de acuerdo con el artículo 12, deberá mantener la fianza vigente y actualizada en los casos siguientes:

I. Durante todo el período que comprenda su acreditación y el año siguiente a su término, cese o revocación.
II. Cuando sea sancionado con suspensión temporal, y
III. Si se hubiere iniciado procedimiento administrativo o judicial en su contra hasta que concluya el mismo.

Lo anterior deberá consignarse expresamente en la póliza de fianza.

Conforme al artículo 26 la Secretaría sancionará con suspensión temporal de cinco y hasta seis meses en el ejercicio de sus funciones a ATEB si:

a) Reincide en cualquiera de las conductas a que se refiere el artículo 25.
b) No cuenta con fianza vigente por el monto y condiciones que se determinan en forma general en el Reglamento y en las Reglas Generales que expida la Secretaría.
c) Provoca la nulidad de un acto jurídico por su negligencia, imprudencia o dolo, en la expedición de un Certificado, u
d) Omite notificar a la Secretaría cualquier cambio que pretenda efectuar respecto de los datos a que se refiere el artículo 17 del Reglamento.

De acuerdo con el artículo 27, la Secretaría sancionará con suspensión definitiva en el ejercicio de sus funciones a ATEB si:

a) Reincide en cualquiera de las conductas a que se refiere el artículo 26.

b) No comprueba la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un Certificado, en los términos establecidos por el Código de Comercio, el Reglamento y las Reglas Generales.
c) Proporciona documentación o información falsa para obtener la acreditación como Prestador de Servicios de Certificación.
d) Altera, modifica o destruye los Certificados que emita sin que medie resolución de la Secretaría o de autoridad judicial que lo ordene.
e) Emite, registra o conserva los Certificados que expide, fuera del territorio nacional.
f) Impide a la Secretaría efectuar las auditorías a que se refiere el Código de Comercio y el Reglamento.
g) Revela los Datos de Creación de Firma Electrónica que correspondan a su propio Certificado.
h) Difunde sin autorización la información que le ha sido confiada o realiza cualquier otra conducta que vulnere la confidencialidad de esta.

En el caso de que la Secretaría suspenda a ATEB en sus funciones, deberá revocar su correspondiente Certificado, de acuerdo con el artículo 27 del reglamento, ya sea de manera temporal o definitiva, y lo agregará al listado de certificados revocados en el dominio que establezca para tal efecto y publicará un extracto de la resolución en el **Diario Oficial de la Federación**, a efecto de que cualquier usuario verifique en todo momento si un Prestador de Servicios de Certificación puede o no ejercer su función. En el caso de suspensión definitiva la Secretaría deberá además revocar la acreditación.

15. Consulta del documento

La información correspondiente a las presentes Declaraciones de Prácticas para el servicio de Constancia de Conservación de Mensaje de Datos es de carácter público y estará publicada en la página: **https://www.ateb.mx/psc.html** para su consulta

16. Referencias

ATEB como Prestador de Servicios de Certificación acreditado por la Secretaría de Economía ofrece los servicios de emisión de Constancias de Conservación de Mensajes de Datos.

Esta declaración se fundamenta en las Políticas Corporativas de Seguridad de la Información implementadas en ATEB, estructuradas de acuerdo con el *Knowledge Database* KDB del International *Information Systems Security Certification Consortium*, (ISC^2) y están expresadas para ser mapeadas fácilmente para el cumplimiento de los objetivos y controles manejados por el estándar ISO/IEC 27001:2013 y de los procesos y objetivos de control del estándar CobiT versión 4.1.

Para que ATEB pueda fungir como un Prestador de Servicios de Certificación se necesitan cumplir diferentes estándares y requerimientos legales tanto nacionales como internacionales tales como:

a) Estándar FIPS 140-2 nivel 3
b) Estándar ETSI TS 102 042 en sus secciones de:
    a. 7.2 Public key infraestructure- Key management life cycle
    b. 7.4.4 Physical and environmental security

c. 7.4.8 Business continuity management and incident handling

c) RFC 3161, Internet X.509 Public Key Infraestructure Time-stampl Protocol (TSP)
d) RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs)
e) ISO/IEC 27001:2013
f) Ley Federal del Procedimiento Administrativo
g) Código de Comercio
h) NOM-151-SCFI-2016 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.
i) Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.
j) Reglamento del Código de Comercio en materia de Prestadores de Servicio de Certificación.