ATEB

Manual de políticas del servicio de Constancia de Conservación de Mensajes de Datos

ATEB—BPM

Dirección General

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

Identificador de objeto: 2.16.484.101.10.316.100.9.1.2.1.2

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 políticas del servicio de Constancia de Conservación de Mensajes de Datos
Organización: ATEB Servicios S.A de C. V
Fecha de elaboración del documento: 17/May./2021
Fecha de actualización del documento: 02/May./2022
Administrador: Auxiliar de Apoyo Informático de Seguridad
Patrocinador: Director General
Destinatario / usuario: Público Externo: Aliados de Negocio, Personal Externo (Proveedores), SAT

1.2 Registro de Cambios

Fecha	Autor	Versión	Referencia del Cambio	Estatus del documento
17/May./2021	JDGM	1.0	Elaboración de documento inicial	Definición inicial del documento
18/Ene./2022	JDMG	1.1	Actualización de: - Alcance - Calendario de revisión del documento - Actualización de redacción de Políticas para el Servicio de Constancia de Conservación de Mensajes de Datos	Aprobado
02/May./2022	JDMG	1.2	- Revisión General del documento - Vigencia del documento - Actualización del Calendario de revisión del documento - Actualización del punto 8. Constancia de Conservación de Mensaje de Datos	Aprobado

			- Adición del Punto 8.1 Identificador de Objeto	

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

ATEB Servicios S.A de C.V (en lo sucesivo ATEB), es una razón social que brinda soluciones de negocio y diferentes servicios como el de Constancia de Conservación de Mensajes de Datos ofreciendo un servicio de calidad que respeta y cumple con lo requisitado por las Reglas Generales para los Prestadores de Servicio de Certificación (PSC), la NOM-151-SCFI-2016, el Código de Comercio y demás leyes aplicables.

ATEB como empresa de servicios, está enfocada en brindar a sus clientes diferentes ventajas y oportunidades en el campo de las tecnologías, automatizando sus procesos y brindando la optimización de sus recursos.

Este documento establece las responsabilidades y obligaciones de las partes interesadas en el servicio de Constancia de Conservación de Mensajes de Datos, así como definir los términos, condiciones y las 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 Mensajes de Datos con base en la NOM-151-SCFI-2016, el Código de Comercio y Medidas de Seguridad establecidas

en el SGSI de ATEB, proporcionando los elementos humanos, económicos, materiales y tecnológicos establecidos para brindar un servicio de calidad como PSC.

2.3 ALCANCE

Este Manual de Políticas aplica para todos aquellos usuarios (Personas Físicas o Morales) que soliciten el servicio de Constancia de Conservación de Mensajes 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 de Constancia de Conservación de Mensajes de Datos, 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)

Certificado: Todo mensaje de datos u otro registro que confirme el vínculo entre el firmante y los datos de creación de firma electrónica.

Constancia de Conservación de Mensajes 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.

FIPS: Federal Information Processing Standard (Estándares Federales de Procesamiento de la Información).

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

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

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 Mensajes 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): Persona o institución pública o privada 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 de Economía.

RFC 3161/3628: (Request For Comments). Estándares internacionales donde se estable el protocolo para garantizar el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

S.A de C.V: Sociedad Anónima de Capital Variable.

3. Responsable del manual de políticas del servicio de Constancia de Conservación de Mensajes de Datos

El ISO es la persona responsable de mantener permanentemente actualizado y documentado el presente manual de políticas de del servicio de Constancia de Conservación de Mensajes de Datos, así como las reglas que lo fundamentan.

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

3.1 ACREEDORES DE CONSTANCIAS DE CERTIFICACIÓN

Personas físicas que, a nombre propio o representando legalmente a un tercero, solicitan la emisión de Constancias de Conservación de Mensajes de Datos, 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.

3.2 PARTES INTERESADAS

Autoridad de Constancias de Conservación de Mensajes de Datos de ATEB (ACCMD ATEB): Organización acreditada por la Secretaría de Economía para ofrecer los servicios de emisión de constancias de conservación de mensajes de datos a las personas que así lo requieran.

Comerciantes – Usuarios: Personas físicas o morales que necesitan los servicios otorgados por la ACCMD de 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).

4. Vigencia del documento

El período de vigencia del presente documento es de 6 meses, por lo que la fecha en que entran en vigor la presente declaración de prácticas y políticas 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

4.1 Calendario de revisión del manual de políticas del servicio de Constancia de Conservación de Mensajes 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.

5. Matriz RACI

INFORMACIÓN SOBRE LOS PARTICIPANTES DEL SERVICIO					
#	**Puesto**	**Responsable**	**Aprobador**	**Consultado**	**Informado**
1.	Director General	—	*	*	*
2.	Auxiliar de Apoyo Informático de Seguridad	*	*	*	*
3.	Profesional Informático	—	*	*	*
4.	Profesional Jurídico	—	*	*	*

Nota: (*) Participa; (—) No participa

6. Obligaciones y responsabilidades de la ACCMD ATEB y el comerciante – usuario

6.1 Obligaciones de la ACCMD ATEB

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 de Constancias de Conservación de Mensajes de Datos.

b) Brindar los servicios de emisión de Constancias de Conservación de Mensajes 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 emisión 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 autorizado por el mismo.

e) Aclarar los términos y condiciones para la emisión de Constancias de Conservación de Mensajes de Datos dentro del contrato entre ambas partes.

f) Verificar que la infraestructura con que se cuenta soporte el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

g) Proteger la confidencialidad y asegurar la disponibilidad e integridad de la información que los comerciantes - usuarios le proporcionan para la emisión de las Constancias de Conservación de Mensajes 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 Constancias de Conservación de Mensajes de Datos emitidas de conformidad con la NOM-151-SCFI-2016.

i) Brindar a los comerciantes – usuarios el medio adecuado y de fácil acceso, para que pueda 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.

6.2 Obligaciones del comerciante – usuario

Los usuarios deberán cumplir con sus obligaciones:

a. Resguardar sus llaves de acceso al servicio de emisión de Constancias de Conservación de Mensajes de Datos.
b. Asegurar la vigencia de la constancia.
c. Verificar que las constancias estén relacionadas con los documentos para los que se solicitaron.
d. Cumplir con lo estipulado en el contrato y/o documentos adicionales pactados entre ATEB y el comerciante – usuario.

6.3 Responsabilidades de la ACCMD ATEB

ATEB es responsable de brindar el servicio de emisión de Constancias de Conservación de Mensajes de Datos de acuerdo con lo establecido en el presente documento y en relación con las Políticas de Constancias de Conservación de Mensajes de Datos.

1. Dar a conocer por medio de la página oficial de ATEB, la información relacionada con el servicio de emisión de Constancias de Conservación de Mensajes de Datos.
2. Garantizar que el certificado con el que se emiten las Constancias de Conservación de Mensajes de Datos es íntegro y auténtico.

ATEB no se hace responsable de:

1. Cualquier daño que pudieran sufrir los comerciantes – usuarios al realizar el mal uso de las Constancias de Conservación de Mensajes de Datos emitidas por ATEB.
2. Cualquier daño que pudieran sufrir sus comerciantes – usuarios por el incumplimiento de sus obligaciones.
3. Malas interpretaciones por parte de los comerciantes – usuarios al usar el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

4. Emisión de Constancias de Conservación de Mensajes de Datos errónea debido a una entrega incorrecta de documentos por parte del comerciante - usuario.
5. Por la interrupción de la emisión de las Constancias de Conservación de Mensajes de Datos debido a causas ajenas a ATEB incluso con la activación de los respectivos planes de contingencia.

6.4 RESPONSABILIDADES DE LOS COMERCIANTES – USUARIOS

El comerciante – usuario es el responsable de:

1. Conservar las llaves de acceso al servicio de Constancias de Conservación de Mensajes de Datos al igual que las Constancias de Conservación de Mensajes de Datos ya emitidas y la debida gestión de los Mensajes de Datos por los que se solicitó el servicio.
2. Controlar y administrar el almacenamiento de las Constancias de Conservación de Mensajes de Datos y los documentos digitalizados por medios propios o mediante la contratación de un tercero.

7. Políticas de Constancias de Conservación de Mensajes de Datos

7.1 ANTECEDENTES

ATEB brinda diversos servicios relacionados con las Tecnologías E-Business, en este concepto y derivado de la alta competitividad que se tiene a nivel nacional e internacional, es que se necesita avanzar más allá de los servicios básicos de Firma Electrónica; teniendo como objetivo entre otros; la Emisión de Sellos Digitales de Tiempo, Constancias de Mensajes de Datos y Digitalización de documentos en Soporte Físico, todo de Conformidad con la NOM151-SCFI-2016, en términos y con los requisitos que establece el Código de Comercio.

Estos planes no deben interferir, afectar o disminuir en el servicio de las funciones mínimas para cumplir con los objetivos de negocio, regulatorios, técnicos, administrativos y operativos de la organización. Estos requerimientos deben considerar la infraestructura tecnológica requerida para su funcionamiento sin que se vea afectada la principal operación de ATEB.

En esta política se establece el cumplimiento de los requerimientos humanos, económicos, materiales y tecnológicos necesarios para poder emitir las Constancias de Conservación de Mensajes de Datos que prueban, con fecha y hora de emisión, que el contenido de los documentos enviados por el cliente se conserva íntegro desde su emisión original y está disponible para las partes interesadas y autorizadas. De igual manera, estas políticas son la base para la creación y desarrollo del Manual de Declaración de Prácticas del servicio de Constancia de Conservación de Mensajes de Datos.

Cualquier cambio que se haga en este documento que implique un impacto para la emisión de las Constancias de Conservación de Mensajes de Datos se podrá hacer siempre y cuando cuente con la respectiva notificación a la Secretaría de Economía.

7.2 Políticas Generales para el servicio de Constancia de Conservación de Mensajes de Datos

• Política de Seguridad de la Información

1. La Seguridad de la Información es un asunto que está directamente relacionado al riesgo de la operación de los negocios.

2. El área asignada al servicio de Constancia de Conservación de Mensajes de Datos debe incorporar un procedimiento de Seguridad de la Información que asegure el cumplimiento de estas políticas al desarrollar e instrumentar aplicaciones, sistemas y servicios para el desarrollo e implementación de este servicio.

3. Las tareas asociadas a la administración de Seguridad de la Información para este tipo de servicio no deben ser realizadas por proveedores externos.

   • Los proveedores externos únicamente deben brindar asesorías y soporte técnico relacionadas a la Seguridad de la Información.

   • Los proveedores externos que participen en la asesoría de Seguridad de la Información deben firmar un convenio de confidencialidad y no divulgación de información.

4. La Normatividad y Legislación aplicable a la generación de este servicio deben ser con base en las leyes y reglamentos y demás relacionadas a la Seguridad de la Información, entre las que se encuentran Ley Federal de Protección de Datos Personales en Posesión de Particulares, y las Leyes Federal y General de Acceso a la Información Pública Gubernamental y las internacionales aplicables.

• Política sobre los responsables de Seguridad de la Información

1. Debido a las características de negocio y del manejo de información de nuestros clientes, debe existir un grupo responsable de la Seguridad de la Información en la organización formado por al menos dos personas:

   • Un responsable de establecer y supervisar la implementación de un programa de Seguridad de la Información, así como de la verificación y cumplimiento de este (ISO).

   • Un coordinador de la administración de la seguridad responsable de la instrumentación del día a día del programa de seguridad informático, del programa de divulgación y capacitación a los demás colaboradores de las políticas y estándares de Seguridad de la Información (ISA).

2. Debe haber una persona responsable de la Seguridad de la Información con el título “Oficial de Seguridad de la Información” (Information Security Officer (ISO)) para establecer y mantener actualizado y documentado el presente manual de políticas y los estándares para asegurar la protección y salvaguardar los activos informáticos para el desarrollo e implementación de este servicio.

7.3 POLÍTICAS ESPECÍFICAS PARA EL SERVICIO DE CONSTANCIA DE CONSERVACIÓN DE MENSAJES DE DATOS

• 7.3.1 Políticas de administración de la Seguridad

- Política de confidencialidad de la información

1. Se entiende como “Confidencialidad de la información” el que la información involucrada en el servicio de Constancia de Conservación de Mensajes de Datos esté protegida en todo momento de su revelación no autorizada, ya sea a personal interno o externo a la organización.

2. Seguridad de la Información es un asunto que está directamente relacionado al riesgo de la operación de los negocios.

Para poder asegurar de una manera efectiva la información, por lo que el área asignada para la gestión del servicio de Constancia de Conservación de Mensajes de Datos debe poder responder las siguientes preguntas fundamentales para la confidencialidad de la información involucrada:

- **Confidencialidad:**

¿Podemos asegurar la confidencialidad de la información?

¿Podemos asegurar que los requerimientos apropiados de privacidad estén satisfechos?

¿Podemos asegurar que los datos estén disponibles únicamente para aquellos que tienen la necesidad y la autorización para utilizarla?

- **Responsabilidad:**

¿Podemos garantizar el no repudio de una operación?

¿Podemos saber y probar quién hizo qué?

¿Se puede demostrar la responsabilidad de cada usuario por sus actividades en los sistemas?

- Política de integridad de la información

1. Se entiende como “Integridad de la información” el que la información manejada en el servicio de Constancia de Conservación de Mensajes de Datos sea en todo momento confiable, esté completa y esté protegida de modificaciones no intencionales, no anticipadas y no autorizadas por la propia organización.

2. Seguridad de la Información es un asunto que está directamente relacionado al riesgo de la operación de los negocios.

Para poder asegurar de una manera efectiva la información, por lo que el área asignada para la gestión del servicio de Constancia de Conservación de Mensajes de Datos debe poder responder las siguientes preguntas fundamentales para la Seguridad de la Información:

- **Integridad:**

¿Podemos prevenir cambios no autorizados a la información manejada, ya sean estos deliberados o accidentales?

¿Podemos asegurar la fiabilidad de esta información y podemos confiar en la misma?

- **Responsabilidad:**

¿Podemos garantizar el no repudio de una operación?

¿Podemos saber y probar quién hizo qué?

¿Se puede demostrar la responsabilidad de cada usuario por sus actividades en los sistemas?

- **Especificaciones de la Política**

El área de Sistemas debe instalar productos antivirus, antispam, antispyware, etc., en los equipos utilizados para el servicio de Constancia de Conservación de Mensaje de Datos.

El área de Sistemas junto con Seguridad de la Información deben ser los responsables de actualizar, mantener y monitorear la operación apropiada en todos los equipos de cómputo, así como en los servidores de red utilizados para brindar el servicio de Constancia de Conservación de Mensaje de Datos.

- Política de disponibilidad de la información

1. Se entiende como “Disponibilidad de la información” el que la información, así como todos los recursos informáticos requeridos para brindar el servicio de Constancias de Conservación de Mensajes de Datos estén disponibles cuando se les necesite para alcanzar los requerimientos del negocio y evitar pérdidas substanciales por su ausencia.

2. Por las características de las aplicaciones sensitivas del servicio de Constancias de Conservación de Mensajes de Datos, la ausencia de datos y/o de información, puede poner en riesgo la implementación de este servicio, al negocio de sus clientes o de los contribuyentes.

- **Especificaciones de la Política**

1. Para las aplicaciones sensitivas y de misión crítica se debe elaborar un plan de alta disponibilidad que incluya los siguientes aspectos:

   a. El centro de cómputo y todos sus servicios asociados como las instalaciones eléctricas, de aire acondicionado, de emergencia para prevención y detección de incendios, etc.
   b. Las telecomunicaciones.
   c. La protección permanente de los sistemas, aplicaciones y los datos que se registran y manejan en los mismos, de tal manera que permita la restauración inmediata de los mismos al procurar en lo posible que no se afecte la operación del servicio de Constancias de Conservación de Mensajes de Datos.
   d. Controles de acceso físico, como seguridad policial, CCTV, señalización, bitácoras de entrada y salida del espacio asignado al servicio de Constancias de Conservación de Mensajes de Datos.

e. Equipo de cómputo de tecnología no obsoleta, que tenga servicio de mantenimiento por el fabricante del equipo, monitoreo de la capacidad operativa y de crecimiento de los equipos, administración del retiro de los medios de almacenamiento, etc.
f. Definir e instrumentar una arquitectura de la plataforma tecnológica que evite tener elementos que sean considerado con puntos únicos de falla “Single Point of Fail (SPF)” que la sola ausencia de alguno de ellos afecte la operación del servicio.

- Política de no repudio de la información

1. Se entiende como “no repudio de la información” al ejercicio que protege a cualquiera de las partes involucradas de la negación de la transacción de información; el no repudio debe ser eficaz en los mecanismos de seguridad implementados para validar, mantener y poner a disposición de los involucrados las pruebas irrefutables de evidenciar la veracidad de las transacciones de la información y su contenido.

   - No repudio de origen: Este servicio proporciona al receptor de un objeto digital una prueba infalsificable del origen de dicho objeto, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

   - No repudio de recepción: Proporciona al emisor la prueba de que el destinatario legítimo de un mensaje u objeto digital genérico, realmente lo recibió, evitando que el receptor lo niegue posteriormente y consiga sus pretensiones. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

2. Debido a la amenaza de Seguridad de la Información que puede presentar la organización en la manipulación de transacciones tales como documentos digitales, el servicio de no repudio es el procedimiento que debe proteger a cualquiera de las partes involucradas, sin embargo la manipulación no autorizada y sin conocimiento de los documentos generados a través del servicio de Constancias de Conservación de Mensajes de Datos pueden originar graves problemas derivados de falsificaciones, modificaciones accidentales o intencionadas, pérdidas o retrasos, e incluso disputas sobre el momento exacto de envió o recepción. Tras estos comportamientos ilegítimos se deben de implementar mecanismos de no repudio que sirvan para generar evidencia irrefutable.

   - **Especificaciones de la Política**

1. El no repudio debe estar relacionado con la autenticación para identificar al emisor de un mensaje, el creador de un documento o dispositivo conectado a un servicio.
3. Debe autorizar el sistema de información o persona con responsabilidades funcionales sobre el servicio de Constancias de Conservación de Mensajes de Datos para controlar el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber validado el proceso de autenticación.
4. Debe verificar el correcto funcionamiento de las políticas o medidas de seguridad establecidas para el servicio de Constancias de Conservación de Mensajes de Datos.

- Política de consistencia de la información

1. Se entiende como “Consistencia de la información” el que la información involucrada en el desarrollo e implementación del servicio de Constancia de Conservación de Mensajes de Datos y los sistemas requeridos se comporten de manera estable, coherente, con estabilidad y solidez a lo largo de su vida útil.

2. La información debe mantener la consistencia entre la información interna en la computadora y los sistemas con la realidad del mundo exterior.

- Política de auditorías y revisiones de cumplimiento

1. En la empresa se deben realizar auditorías y revisiones de cumplimiento del servicio de Constancias de Conservación de Mensajes de Datos.

2. Las auditorías y revisiones de cumplimiento deben ser efectuadas por personal independiente al encargado de brindar el servicio de Constancias de Conservación de Mensajes de Datos y estás deberán hacerse de manera semestral.

3. El personal que dirija las auditorías y revisiones de cumplimiento debe ser personal calificado, que sustente certificaciones vigentes en materia de Seguridad de la Información.

4. El área de Seguridad de la Información realizará revisiones físicas de manera aleatoria en el área asignada para la implementación del servicio de Constancias de Conservación de Mensajes de Datos.

- **Especificaciones de la Política**

Se deben realizar auditorías internas de cumplimiento.

1. Los resultados de las auditorías se deben clasificar como CONFIDENCIAL.
2. Los resultados de las auditorías deben tener una vigencia máxima de 12 meses.
3. Las observaciones de las auditorías se deben subsanar por prioridades de acuerdo con el nivel de riesgo de cada observación.
4. Mientras el nivel de riesgo o el impacto sea más alto se atenderán y resolverán primero.
5. Todas las observaciones atendidas y resueltas deben estar sustentadas en evidencias físicas verificables.

- Política de propiedad de los activos informáticos

1. Todos los activos informáticos como son los equipos físicos y virtuales, las aplicaciones y los datos deben tener un responsable único de su protección y salvaguarda.

2. Estos activos deben estar debidamente identificados en el inventario de activos que soportan el servicio de Constancias de Conservación de Mensajes de Datos.

- **Especificaciones de la Política**

1. A todos los activos de la información del servicio de Constancias de Conservación de Mensajes de Datos como son los equipos físicos y virtuales, las aplicaciones y los datos se les debe asignar un “Dueño” o último responsable de proteger dichos activos.

2. Todos los equipos físicos o lógicos del servicio de Constancias de Conservación de Mensajes de Datos para el manejo de sus aplicaciones sensitivas y de misión crítica deben ser responsabilidad directa de la organización.

3. La protección de todos los equipos físicos y virtuales debe ser responsabilidad del Gerente de Sistemas de la organización.

4. La protección de las aplicaciones sensitivas y de misión crítica debe ser responsabilidad del Gerente de Sistemas de la organización.

5. La protección de las bases de datos que manejan información sensitiva y de misión crítica debe ser responsabilidad del Gerente de Sistemas de la organización.

• 7.3.2 Políticas de Seguridad Física y Tecnológica

- Política para resguardar la seguridad física

1. Las oficinas centrales y/o los centros de cómputo donde residan y se ejecute el servicio de Constancias de Conservación de Mensajes de Datos, deben estar en lugares seguros, libres de amenazas de alto impacto y con controles de protección perimetrales y señalizaciones de seguridad.

2. Las oficinas centrales y/o los centros de cómputo donde se ejecute el servicio de Constancias de Conservación de Mensajes de Datos, deben contar con una infraestructura de seguridad, instalación eléctrica y monitoreo que minimice la posibilidad de detener las operaciones de las aplicaciones críticas de estos servicios.

3. Las oficinas centrales y/o los centros de cómputo deben contar con sus propios planes de DRP para garantizar la continuidad del servicio de Constancias de Conservación de Mensajes de Datos.

4. Se deben proteger el área asignada al servicio de Constancias de Conservación de Mensajes de Datos mediante controles de entrada (tarjetas de proximidad) apropiados para asegurar que sólo se permita acceso al personal autorizado.

Por el tipo de información que se maneja en el servicio de Constancias de Conservación de Mensajes de Datos, el área asignada a la prestación de este servicio debe considerarse como área restringida.

- **Especificaciones de la Política**

1. Ubicación física. Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos en los cuales operen las aplicaciones críticas, no críticas y sensibles, de ATEB deben seleccionarse con una ubicación física segura y libre de riesgos de alto impacto como son:

- Estar alejado como mínimo 100 m de lugares de alto riesgo como:
  - Gasolineras
  - Bancos
  - Gaseras
  - Minas
  - Acometidas de cableado de luz
  - Gas, etc.

2. Estructura. Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con protección perimetral adecuada que impida el acceso fácil desde el exterior y de ser posible, debe tener algún elemento adicional de protección como malla de picos, malla eléctrica, etc., debe contar con paredes de concreto, puerta blindada,

piso falso acceso ya sea por sistema biométrico o tarjeta de proximidad, o mínimo con acceso por teclado.

3. Infraestructura. Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con sistema contra incendios (Gas FM200), detectores de humo, equipo contra incendios, específicos para cada tipo de incendio que se pueda presentar.

- Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con cableado estructurado que cubra la necesidad de continuidad en el servicio de Telecomunicaciones.
- Para las oficinas centrales deben contemplar seguridad de interconectividad.
- Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con un adecuado sistema de aire acondicionado para evitar problemas de sobrecalentamiento en los equipos.
- Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con restricción de acceso de medios de almacenamiento al personal externo e interno que tenga acceso a esta área.
- Revisiones periódicas por parte de la Unidad Verificadora de Instalaciones Eléctricas u otro órgano de revisión deben validar que el sistema de tierra de seguridad mantiene valores menores a 2 ohms.
- El sistema eléctrico debe ser monitoreado en línea por un sistema automatizado integrado al sistema de monitoreo general de las oficinas centrales y los centros de cómputo.
- Medidas de detección de humedad y líquidos para evitar inundaciones.

4. Instalación eléctrica. Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con equipamiento eléctrico que permita mantener la continuidad del servicio.

5. Mantenimiento. Las oficinas centrales y el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos deben contar con un plan de mantenimiento para los equipos, cableado, sistemas contra incendio, plantas, etc.

6. Planes de continuidad y de recuperación en caso de desastres.

- Las oficinas centrales deben contar con la documentación necesaria de BCP que consideran las aplicaciones e infraestructura requerida para garantizar la continuidad de la operación.
- Los planes de continuidad de las oficinas centrales deben ser probados al menos anualmente para verificar su efectividad y eficiencia y las desviaciones son atendidas de manera inmediata, las desviaciones son solventadas en menos de 3 meses.

- Política de criptografía

1. Para la administración y protección de las constancias, llaves de encriptación y passphrases se deben llevar registros de los hashes de control para cada una de las llaves, constancias y otros elementos de criptografía para asegurar la integridad de estos.

2. La solución implementada debe cumplir con los controles de criptografía, independientemente del tipo de solución o arquitectura implementada.

3. Los mecanismos de criptografía deben estar alineados a mejores estándares de seguridad y deberán prevenir el descifrado de llaves.

- Política de encriptación

1. Toda la información sensible involucrada en el servicio de Constancias de Conservación de Mensajes de Datos debe estar encriptada de conformidad con los estándares de encriptación de datos con el fin de evitar su posible conocimiento por personal no autorizado.

2. Las contraseñas de acceso (*Passwords* y *Passphrases*) deben estar encriptadas para evitar su posible conocimiento por personal no autorizado.

- **Especificaciones de la Política**

1. Las contraseñas de acceso (*Passwords* y *Passphrases*) deben estar encriptadas para evitar su posible conocimiento por personal no autorizado.

2. La información clasificada como CONFIDENCIAL, debe estar encriptada para evitar su posible conocimiento por personal no autorizado.

Este requerimiento debe incluir todos los medios de almacenamiento usados como bases de datos, discos, unidades NAS y/o SAN, cintas, respaldos en sitio y fuera de sitio, etc.

• 7.3.3 Políticas de Seguridad en las operaciones de la organización

- Política de responsabilidad en el manejo de Seguridad de la Información

1. Todo el personal responsable de brindar el servicio de Constancia de Conservación de Mensajes de Datos debe conocer y aceptar de manera formal sus responsabilidades con respecto al manejo de la información.

2. Todo el personal responsable de brindar el servicio de Constancia de Conservación de Mensajes de Datos debe manejar de manera correcta y adecuada la información con la que operan el servicio de Constancia de Conservación de Mensajes de Datos, manteniendo siempre la Seguridad de la Información como elemento clave.

- **Especificaciones de la Política**

1. El Área de Jurídico debe de tener las medidas necesarias para poder sancionar a los colaboradores que incurran en un mal manejo de la información y por consecuencia haya sido violada la Seguridad de la Información. Estas medidas pueden ser desde una llamada de atención hasta la separación de su cargo.

2. La Gerencia de Sistemas debe de contar con los mecanismos suficientes y sustentables para poder realizar verificaciones de No Repudio y control de cambios a la información a la que tienen accesos los colaboradores de **ATEB**.

- Política de ética en ATEB

1. Los colaboradores de ATEB designados al área de Constancia de Conservación de Mensajes de Datos, deben asegurar que las actividades realizadas dentro de la organización estén apegadas a los valores, ética, políticas, procedimientos, leyes y normativas, aplicables en la organización.

2. ATEB, en todos los niveles jerárquicos, debe tener un trato responsable, ético y transparente con las entidades de gobierno, no deben aceptar ni hacer, ningún tipo de ofrecimiento de cualquier índole por parte de o hacia éstas, evitando así malas interpretaciones por parte de nuestros grupos de interés.

3. Los colaboradores de ATEB deben cumplir expresamente con las leyes aplicables a todos los ciudadanos, ser partícipes de los usos y costumbres de la sociedad, deben ejercer sus profesiones con ética, realizar actos seguros que no pongan en riesgo su salud o la de sus compañeros dentro de la empresa, promover la calidad de vida con su familia, con la empresa y con el país.

- Política para la definición de una línea estratégica mínima de Seguridad de la Información

1. Las áreas administrativas, operativas y técnicas del servicio de Constancia de Conservación de Mensajes de Datos, deben instrumentar un mecanismo para la protección de la información mediante una línea estratégica mínima de Seguridad de la Información basada en un proceso de gestión de riesgos de negocio asociados con los temas de:

a) Los centros de cómputo que utiliza la organización para brindar el servicio de Constancia de Conservación de Mensajes de Datos.

b) Las telecomunicaciones.

c) El control de accesos físicos al área de Constancia de Conservación de Mensajes de Datos.

d) La protección física de los equipos de cómputo y su nivel de actualización tecnológica.

e) Los ambientes de operación.

f) Desarrollo y adecuación de aplicaciones propietarias.

g) La custodia de la información.

h) Administración de la seguridad, e implementación de los controles necesarios para asegurar el cumplimiento de una línea mínima de seguridad.

- **Especificaciones de la Política**

1. Postura de la empresa sobre la Seguridad de la Información:

- Aseguramiento del compromiso institucional con la protección de la información.
- Seguridad en el manejo de la documentación sensitiva impresa.
- Seguridad en los procesos y manuales.

2. Seguridad en el Personal

- Seguridad en el manejo de personal previo a la contratación.
- Seguridad en el manejo de personal previo a la separación de este.

3. Gestión de los Activos

4. Seguridad Física

- En las oficinas.
- En el área asignada para el servicio de Constancias de Conservación de Mensajes de Datos.

5. Gestión de la Seguridad

- Manejo de incidentes y respuestas a los mismos.
- Control de auditorías, atención, observaciones y respuestas a las mismas
- Medición y métricas de Seguridad de la Información
- Mecanismos de no repudio como pueden ser:
  - Administración de los dispositivos de hardware de seguridad (HSM)
  - Información cifrada
  - Firmas digitales y manuscritas
  - Copias de seguridad
  - Logs de seguridad
- Pruebas y monitoreo permanentes de seguridad a la plataforma tecnológica, aplicaciones y a las bitácoras de auditorías y trazabilidad de las operaciones.

6. Seguridad de la Plataforma Tecnológica

- Plan y pruebas de continuidad del negocio:
  - Manejo de contingencias
  - Manejo de continuidad de negocios (BCP)
  - Manejo del plan ante desastres (DRP)
  - Preparación de los planes ante desastres
  - Pruebas de escritorio, reales y no anunciadas
  - Mantenimiento de los planes BCP y DRP
  - Activación de los planes ante desastres
  - Recuperación de los planes ante desastres
  - Desactivación del plan ante desastres (DRP)

- Manejo de recuperación de datos (Data Recovery)

- Criptografía
  - Administración de criptografía y llaves criptográficas

- Administración de los dispositivos de hardware de seguridad (HSM)

• Protección Contra Código Malicioso

- Manejo y operación de programas *antivirus, antispam y antispyware*
- Manejo y control de sistemas de detección y prevención de intrusos

• Manejo y control de las licencias de software
• Control de cambios en las aplicaciones
• Control de cambios en la plataforma tecnológica
• Control de cambios en las configuraciones de los equipos, sistemas operativos y servidores virtuales.
• Control de capacidades de la plataforma tecnológica

7. Cumplimiento Legal y Regulatorio

- Administración y actualización de los acuerdos y convenios de confidencialidad con autoridades.
- Administración y actualización de los acuerdos de confidencialidad previos a la contratación de personal interno.
- Administración y actualización de los acuerdos de confidencialidad en la separación de personal interno.

- Política de identificación y autentificación de usuarios

La presente política describe una serie de requisitos necesarios y de recomendaciones encaminadas a mejorar la seguridad y robustez en la identificación y autentificación mediante el uso de contraseñas personales para el acceso a los servicios o tecnologías ofrecidos a través del Servicio de Constancia de Conservación de Mensajes de Datos.

1. El uso de contraseñas se define como el uso de una combinación de caracteres alfanuméricos que realizan la autentificación como medida de seguridad para la autorización de acceder a los recursos de la información o de la información del activo, el uso de ésta debe ser confidencial para los colaboradores autorizados.

2. Todos los sistemas de información y software contemplado en el inventario de activos del Servicio de Constancia de Conservación de Mensajes de Datos deben de autentificar la identidad de los usuarios antes de iniciar una sesión de trabajo o una transacción (incluyendo otros sistemas y aplicaciones que tengan acceso a estas plataformas), a menos que la información a la que se va a tener acceso esté clasificada como PÚBLICA.

3. Todos los usuarios deben estar identificados para ingresar a las plataformas del servicio de por al menos:

• Una clave de usuario única (USER ID).
• Una metodología de autenticación como es un password estático o dinámico.

4. Los usuarios deben ser directamente responsables de toda actividad asociada con su USER ID y password.
5. Sobre los passwords estáticos:

• Nunca se deben compartir, dar a conocer o escribir en ningún lugar.
• Consistirán en un mínimo de 10 (diez) caracteres alfanuméricos en el caso de cuentas de usuario estándar y en el caso de las cuentas de usuario administrador deberá ser mayor a los 10 (diez) caracteres alfanuméricos.
• Nunca se deben desplegar en la pantalla.
• Nunca se deben almacenar en ningún dispositivo en texto claro.

6. Los USER ID asociados a *passwords* estáticos y administrador se deben deshabilitar después, no más, de 3 intentos fallidos de *login*.

- **Especificaciones de la Política**

1. Cada usuario debe contar con una clave de acceso única denominada como “Clave de Usuario” (USER ID).
2. Las claves de los usuarios deben ser de fácil definición para que estas puedan ser fácilmente identificadas y asociadas al usuario.
3. El sistema de información no debe permitir que los usuarios o los procesos cambien dinámicamente su identificación sin una autorización expresa.

Política de línea base de seguridad para las aplicaciones

1. Las aplicaciones sensitivas y de misión crítica deben contar con la definición de líneas base de seguridad, documentadas e implementadas que consideren e incluyan como mínimo:

- Implementación de autenticación de los usuarios.
- Implementación de mecanismo de no repudio.
- Protección contra inyección de código malicioso.
- Inicio de sesión seguro.
- Validación de datos de entrada/salida para evitar errores en el procesamiento de la información.
- Manejo de errores.

- **Especificaciones de la Política**.

Las líneas base de seguridad de las aplicaciones sensitivas y de misión crítica deben considerar los siguientes elementos:

1. Implementación de autenticación de los usuarios (internos y clientes).
2.Implementación de mecanismo de no repudio de las transacciones mediante bitácora respectivas.

3. Inicio de sesión seguro.

• Conexión encriptada
• Proceso de identificación y autentificación mediante credenciales
• No despliegue de las contraseñas de las credenciales

4. Validación de datos de entrada / salida para evitar errores en el procesamiento de la información.
5. Manejo de errores.

- Política de control de acceso a las aplicaciones

1. Todas las aplicaciones sensitivas y de misión crítica deben seguir los siguientes requerimientos para poder ser usadas por los usuarios del servicio de Constancia de Conservación de Mensajes de Datos:

- Controles de acceso a las aplicaciones del servicio de Constancia de Conservación de Mensajes de Datos
- Manejo de las claves de usuarios y sus contraseñas de autenticación
- Manejo de seguridad por roles y actividades
- Manejo obligado de segregación de funciones

- **Especificaciones de la Política**.

1. Todas las aplicaciones sensitivas y de misión crítica deben ser iniciadas mediante un proceso de identificación de credenciales I-A-A (Identificación, Autentificación y Autorización de permisos).

7.4 ESTÁNDARES

1. Todo aquel que solicite una Constancia de Conservación de Mensaje de Datos estará aceptando los términos y condiciones establecidas en este documento.
2. La solicitud y obtención de la Constancia de Conservación de Mensajes de Datos se efectuará a través del Web Service correspondiente.
3. ATEB permite a las partes interesadas identificar la Constancia de Conservación de Mensajes de Datos mediante Web Service.
4. Se deben mantener los estándares de la información en la emisión de las Constancias de Conservación de Mensajes de Datos (integridad, disponibilidad y confidencialidad) mediante un proceso de emisión seguro y confiable.
5. ATEB establece roles de confianza para poder llevar a cabo las operaciones de emisión de Constancias de Conservación de Mensajes de Datos, los cuales son:
    a. Profesional Jurídico o Agente Certificador
    b. Profesional Informático
    c. Information Security Officer (ISO)
    d. Auxiliar de apoyo Informático de Seguridad
    e. Auxiliar de apoyo Informático de Administrador de Redes
    f. Auxiliar de apoyo Informático de Operador de Sistemas
    g. Auxiliar de apoyo Informático de Administrador de Sistemas
    h. Auxiliar de apoyo Informático de Administrador de Bases de Datos

6. En caso de que se requieran llevar a cabo cambios que afecten el nivel de seguridad deben ser aprobados por el ISO, el Profesional Jurídico y el Profesional Informático y en caso de requerirse de deberá ejecutar el procedimiento de control de cambios.

7. En el caso de que ATEB quiera dejar de prestar el servicio de emisión de Constancias de Conservación de Mensajes de Datos de manera voluntaria deberá cumplir con el pago correspondiente de derechos e informar a la Secretaría de Economía los motivos del cese de funciones con 45 días de anticipación para asegurarse de que se cuenta con una copia de cada Constancia de Conservación de Mensajes de Datos generada y se puedan compartir con otro PSC que cumpla con las características al que llevaba ATEB para evitar que las partes interesadas se vean afectadas con el cese de funciones de ATEB.

8. ATEB se respalda por medio de las fianzas y el seguro de responsabilidad civil solicitados por la Secretaría de Economía, que cubren a ATEB por los daños que cause y que deba responder en materia civil.

9. El ISO además de fungir como auditor líder dentro de las auditorías internas, se encarga también de analizar los informes de las auditorías, internas y externas realizadas a ATEB, así como de llevar a cabo el seguimiento de los planes de remediación y acciones correctivas para corregir las no conformidades en caso de haberlas.

8. Constancia de conservación de mensaje de datos

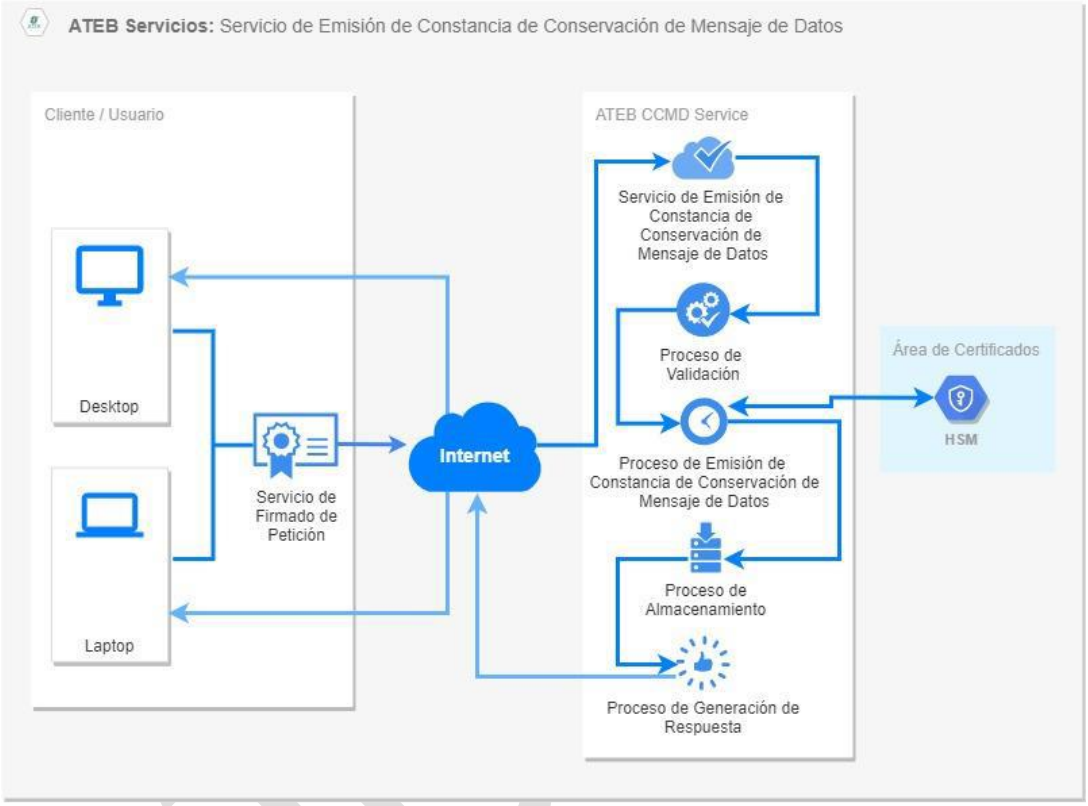
Emisión:

1.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.
2.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.

3. Se emite la Constancia de Conservación de Mensaje de Datos
4. Se genera la respuesta
5. Se almacena la Constancia de Conservación de Mensaje de Datos para su futura verificación
6. 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:

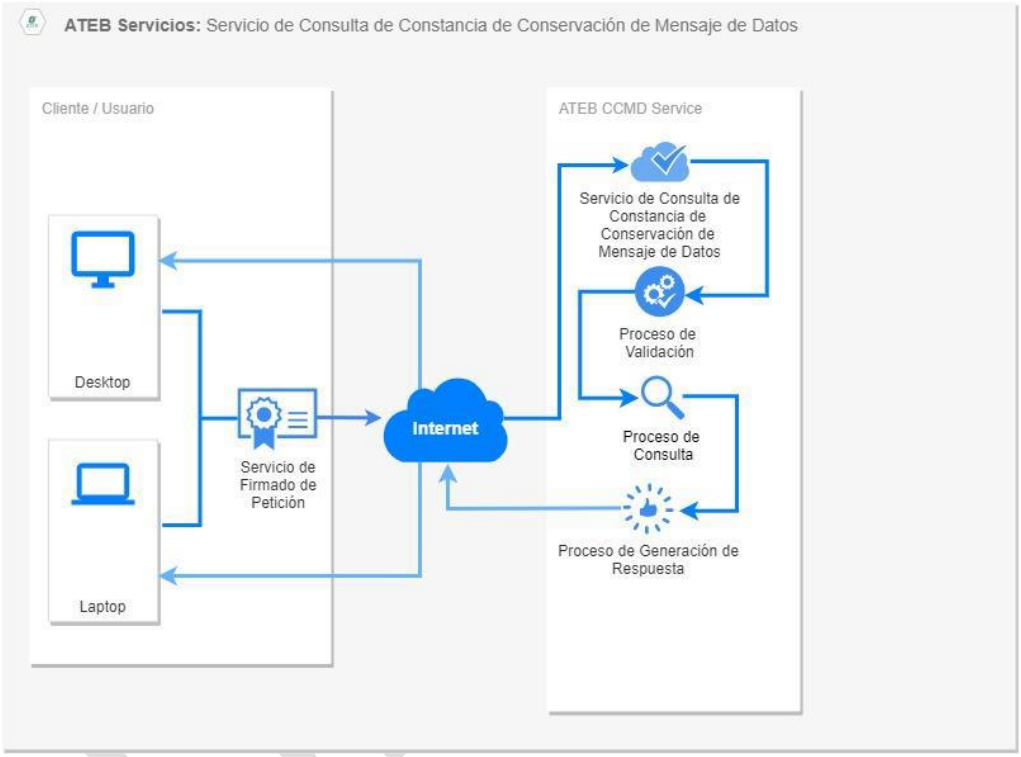
1. Recibe la solicitud de validación de Constancia de Conservación de Mensaje de Datos con extensión .ccq con el estándar ASN.1 que contiene la llave pública y la petición firmada con la firma electrónica del cliente.

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.

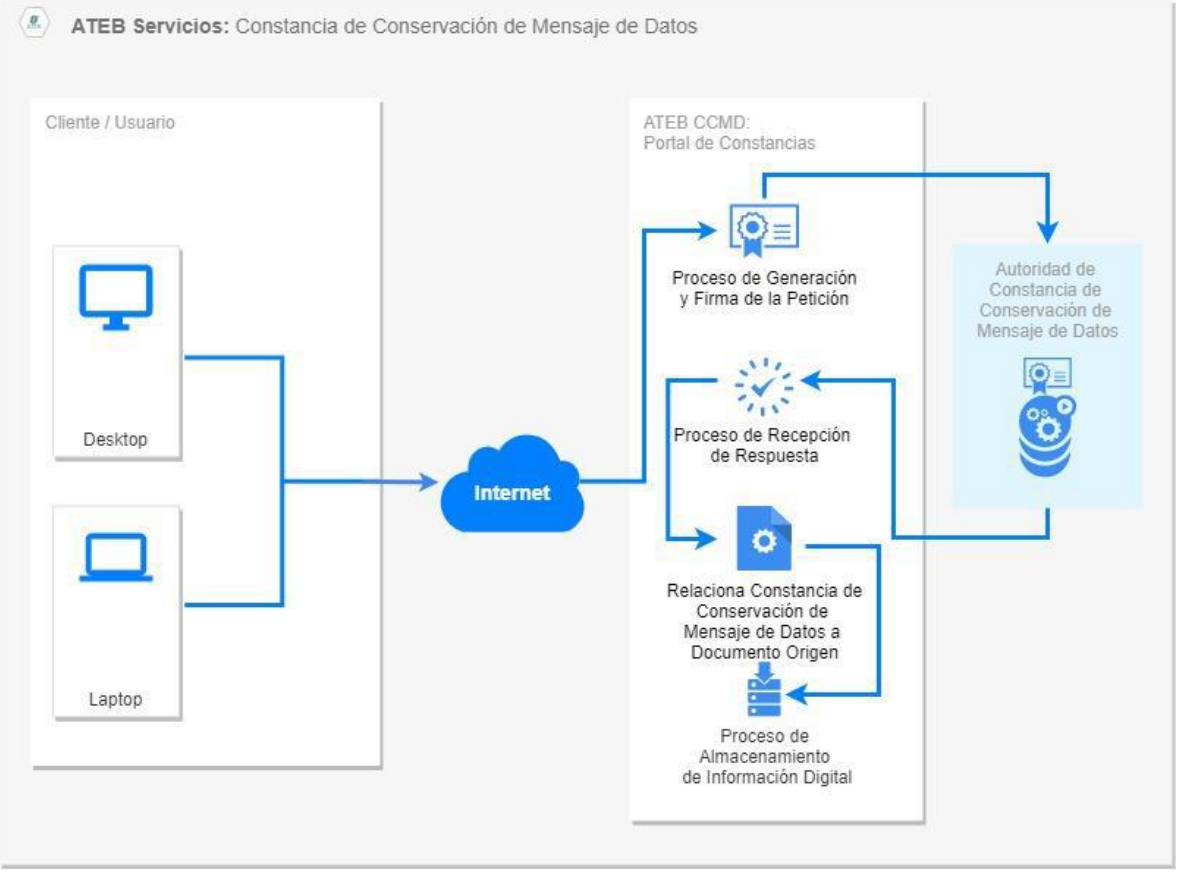
Solicitar Constancia de Conservación de Mensaje de Datos, de los documentos cargados al portal.

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 muestra el diagrama de generación de Constancia de Conservación de Mensaje de Datos:



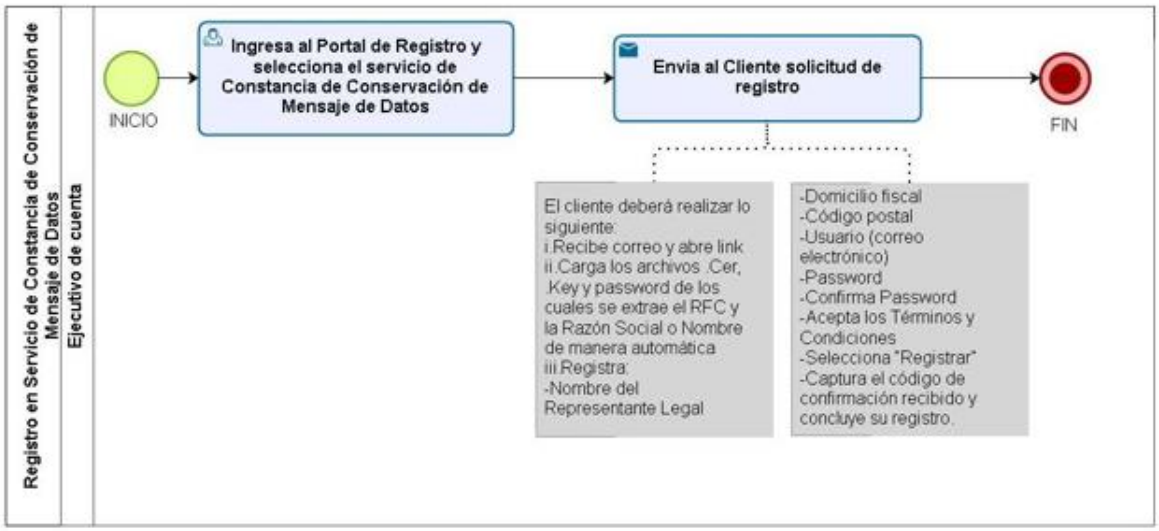
8.1 IDENTIFICADOR DE OBJETO

El identificador proporcionado por la Secretaría de Economía para el servicio de Constancia de Conservación de Mensajes de Datos es: 2.16.484.101.10.316.100.9.1.2.1.2

9. 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

9.1 PROCEDIMIENTO 1: REGISTRO EN SERVICIO DE CONSTANCIA DE CONSERVACIÓN DE MENSAJES DE DATOS

- Diagrama General del procedimiento



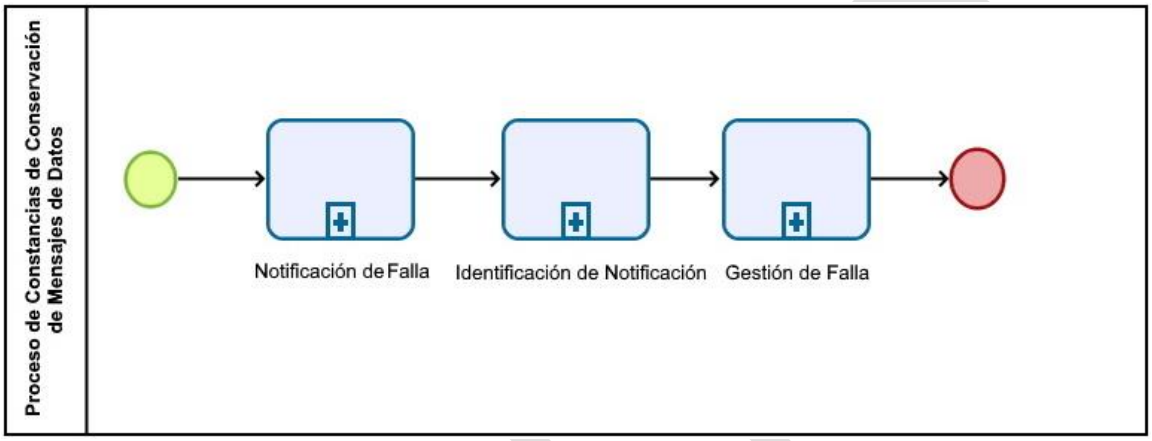
- Descripción del procedimiento

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					

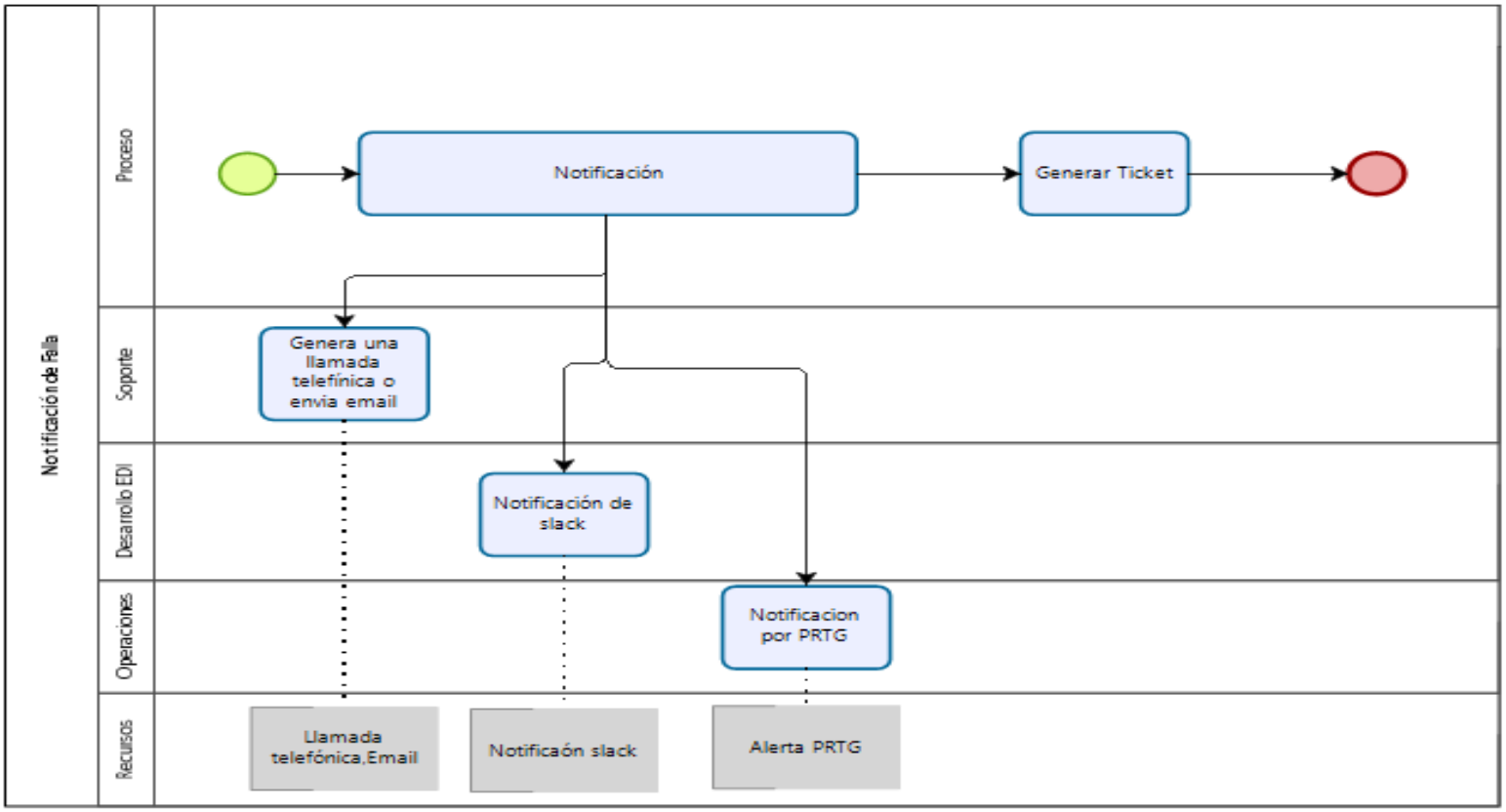
9.2 PROCEDIMIENTO 2: GESTIÓN DE FALLAS DURANTE EL FUNCIONAMIENTO DE LOS SERVICIOS CON EL CLIENTE

Cada servicio provisto por el área de Prestador de Servicios de Certificación cuenta con un procedimiento a seguir para poder detectar las fallas que puedan poner el riesgo el buen funcionamiento de este; el cual se detalla a continuación:

- Diagrama general del procedimiento



- Subprocedimiento 1: Notificación de Falla

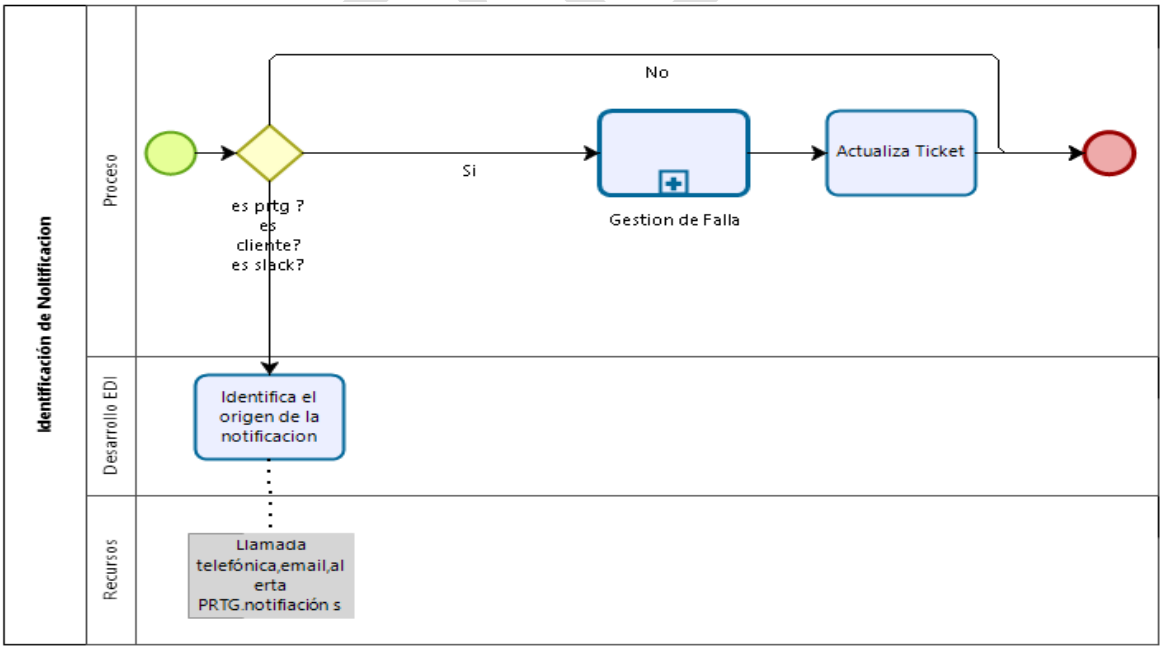


- Descripción del procedimiento

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					

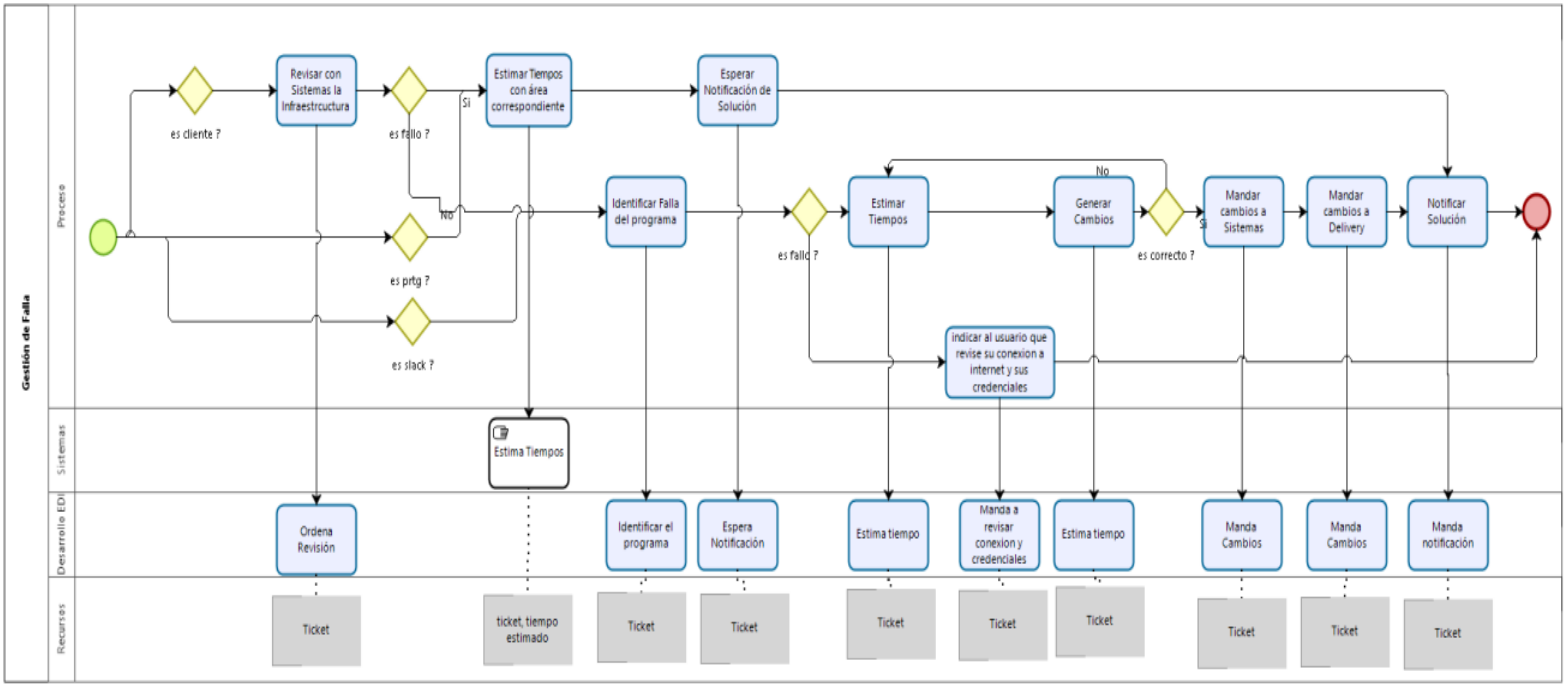
- Subprocedimiento 2: Identificación de Notificación



- Descripción del procedimiento

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 DEL PROCEDIMIENTO					
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					

- Subprocedimiento 3: Gestión de Falla



- Descripción del procedimiento

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 ir 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					