ATEB

# Manual de Políticas para el servicio de Emisión de Sellos Digitales de Tiempo

## ATEB—BPM

## Dirección General

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

**Identificador de objeto: 2.16.484.101.10.316.100.9.1.3.1.3**

# 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 Políticas para el servicio de Emisión de Sellos Digitales de Tiempo |
| **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<br>Externo: Aliados de Negocio, Personal Externo (Proveedores) |

## 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 |
| 03/Ago./2021 | JDGM | 1.1 | -Especificar archivo que recibirá el solicitante y la respuesta obtiene al solicitar el Sello Digital emitido<br>- Homologar definición de Sellos Digitales de Tiempo<br>- Incluir Matriz RACI con personal adicional mencionado en Manual de Declaración de Prácticas<br>- Replantear políticas descritas del servicio de emisión de Sello de Tiempo<br>- Se anexa columna al calendario de revisión debido a la segunda revisión semestral del documento | Aprobado |

| | | | | |
|---|---|---|---|---|
| 18/Ene./2022 | JDMG | 1.2 | - Actualización del alcance<br>- Actualización del Calendario de revisión del documento<br>- Actualización de redacción de Políticas para el Servicio de Emisión de Sellos Digitales de Tiempo | Aprobado |
| 02/May./2022 | JDMG | 1.3 | - Vigencia del documento<br>- Actualización del Calendario de revisión del documento<br>- Adición del punto 5.3 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 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 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 estipulan las Políticas de Seguridad necesarias para la prestación del servicio de Emisión de Sellos Digitales de Tiempo, esto con base en la Regla General No.97 fracción IV a la que deben sujetarse los Prestadores de Servicio de Certificación (PSC), con fundamento en lo dispuesto en el estándar ISO/IEC 27001:2013 y el proceso Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST)

Este documento establece las responsabilidades y obligaciones de las partes interesadas en el servicio de Emisión de Sellos Digitales de Tiempo, 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 Emisión de Sellos Digitales de Tiempo, proporcionando los elementos humanos, económicos, materiales y tecnológicos requeridos para brindar un servicio de calidad como autoridad de Emisión de Sellos Digitales de Tiempo.

## 2.3 ALCANCE

Este Manual de Políticas aplica para todos aquellos usuarios (Personas Físicas o Morales) que soliciten el servicio de Emisión de Sello Digital de Tiempo, 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 Emisión de Sellos de Digitales de Tiempo, 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

**ASDT:** Autoridad de Sellos Digitales de Tiempo.

**CENAM:** Centro Nacional de Metrología.

**Firmante:** Persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

**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.

**Política de Emisión de Sellos Digitales de Tiempo:** Conjunto de directrices que establecen las características y requerimientos para la emisión del Emisión de Sellos Digitales de Tiempo por parte de ATEB.

**Prestador de Servicios de Certificación:** 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: RFC (Request For Comments).** Estándar internacional donde se estable el protocolo para el desarrollo e implementación del servicio de Emisión de Sellos Digitales de Tiempo.

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

**Sellos Digitales de Tiempo:** Los sellos digitales de tiempo son mensajes de datos que demuestran la existencia de la información al momento de su emisión.

**UTC:** Tiempo universal coordinado.

## 2.5 OBLIGACIONES Y RESPONSABILIDADES DE LA ASDT Y EL COMERCIANTE - USUARIO

### 2.5.1 Obligaciones de la ASDT

ATEB al ofrecer el servicio de Emisión de Sellos Digitales de Tiempo de acuerdo con las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, está obligado a cumplir lo siguiente:

a) Asegurar que la declaración de prácticas se cumpla y esté acorde a las políticas de Emisión de Sellos Digitales de Tiempo.
b) Brindar un servicio de calidad, eficaz y eficiente en cuanto a la Emisión de Sellos Digitales de Tiempo, que permitan preservar la confidencialidad, integridad y disponibilidad de la información.
c) Cumplir la Emisión de Sellos Digitales de Tiempo conforme a lo establecido en los términos y condiciones de la Declaración de Prácticas y el contrato de servicio firmado entre las partes interesadas.
d) Contar con un control de accesos que apoye a validar la identidad de los usuarios que utilizan los servicios y salvaguardar la integridad de los datos suministrados.
e) Otorgar un servicio de Emisión de Sellos Digitales de Tiempo eficaz y eficiente.
f) Asegurar la correcta sincronización con el servidor del CENAM.
g) Contar con los elementos humanos, tecnológicos, materiales y económicos necesarios para brindar el servicio de Emisión de Sellos Digitales de Tiempo con la disponibilidad declarada en el presente documento.

### 2.5.2 Obligaciones del comerciante - usuario

a) Resguardar las llaves de acceso al servicio de Emisión de Sellos Digitales de Tiempo.
b) Verificar que los sellos digitales estén relacionados con los documentos para los que se solicitaron.
c) Asegurar la vigencia del sello digital.
d) Cumplir con lo estipulado en el contrato y/o documentos adicionales pactados entre ATEB y el comerciante – usuario.
e) Asegurar que la firma de los Sellos Digitales de Tiempo coincida con la de la autoridad ATEB.
f) Aceptar los términos y condiciones bajo los que se emitirán los Sellos
g) Digitales de Tiempo.
h) Utilizar únicamente los medios establecidos por ATEB para la solicitud de la Emisión de los Sellos Digitales de Tiempo.
i) Otorgar la información, datos o documentos correctos y completos para la Emisión de los Sellos Digitales de Tiempo y asegurarse que sean capturados correctamente para su posterior utilización.

### 2.5.3 Responsabilidades de la ASDT

a) Brindar el servicio de Emisión de Sellos Digitales de Tiempo conforme a lo establecido en el presente documento.
b) Dar respuesta por cualquier falla en el servicio que sea derivado de malas prácticas o cualquier otra irregularidad que sea imputado a ATEB.
c) Garantizar la disponibilidad del servicio.

d) Realizar auditorías de cumplimiento periódicas y ser igualmente auditado previa notificación.
e) Trabajar bajo el SGSI para mantener la información confidencial, disponible e íntegra.

ATEB por otro lado no se hace responsable en caso de lo siguiente:

a) Incidentes relacionados con la falta de cumplimiento de las obligaciones de los comerciantes-usuarios.
b) Del mal uso del servicio de Emisión de Sellos Digitales de Tiempo.
c) Daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que lleguen los comerciantes-usuarios del servicio de Emisión de Sellos Digitales de Tiempo.
d) De la entrega de datos erróneos o falsos para la Emisión de los Sellos Digitales de Tiempo.

## 3. 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 |

### 3.1 Calendario de revisión del Manual de Políticas para el servicio de Emisión de Sellos Digitales de Tiempo

| | 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 | — | * | * | * |
| **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. Emisión de Sellos Digitales de Tiempo

El servicio de Emisión de Sellos Digitales de Tiempo ofrecido por ATEB se encuentra disponible en un 99.3 % de funcionalidad ininterrumpida, asegurando que la fecha y hora de los Sellos Digitales de Tiempo están acordes al servidor de tiempo Cronos del CENAM (Centro Nacional de Metrología). Cada Emisión de Sellos Digitales de Tiempo debe contener:

a) El identificador de objeto correspondiente al algoritmo de hash utilizado para obtener la huella digital del mensaje de datos.
b) Los datos del Emisión de Sellos Digitales de Tiempo encriptados.
c) Un número de folio para cada sello digital.
d) ATEB se asegura de estar sincronizado en todo momento con el servidor de CRONOS para evitar sellos digitales a destiempo, cada sincronización o ajuste que se le haga al servidor se registrará dentro de una herramienta de monitoreo para tener un histórico de los movimientos realizados al mismo.
e) El formato de tiempo utilizado en los Sellos Digitales de Tiempo será el de 24 horas, sincronización con el CENAM
f) El sello digital deberá contener el nombre del emisor.

## 5.1 Objetivo de la Emisión de Sellos Digitales de Tiempo

Vincular una fecha y hora a mensajes de datos en particular para obtener evidencia de que dichos mensajes de datos demuestran la existencia de información al momento de su emisión.

## 5.2 Propósito

Contar con una evidencia que permita la existencia y legalidad de mensajes de datos a partir de la fecha y hora en que son emitidos.

## 5.3 Identificador de Objeto

El identificador proporcionado por la Secretaría de para el servicio de Emisión de Sellos Digitales de Tiempo es: 2.16.484.101.10.316.100.9.1.3.1.3

## 5.4 Información de los Sellos Digitales de Tiempo

La ASDT debe asegurar que los Sellos Digitales de Tiempo sean emitidos a través de un proceso seguro y que contengan la fecha y hora correctas.

Particularmente:

- Deben incluir un valor representativo del dato que será sellado de manera digital, tal y como fue proporcionado por el Comerciante- usuario.
- El tiempo plasmado en el Sello Digital debe estar sincronizado con el Tiempo Universal Coordinado (UTC).
- Los Sellos Digitales deben tener un número de folio único.
- Deben contar con valores de tiempo rastreables.
- Los Sellos Digitales de Tiempo deben incluir un identificador representativo del ASDT.
- El tiempo incluido en cada Emisión de Sellos Digitales de Tiempo debe estar sincronizado de acuerdo con la exactitud mencionada en este apartado.
- Los Sellos Digitales de Tiempo serán firmados con una clave generada únicamente para este propósito.
- Si existe una desviación en la exactitud de la sincronización con respecto al UTC, la ASDT no deberá expedir los Sellos Digitales de Tiempo.

## 5.5 Sincronización del Reloj con el UTC

ATEB, como ASDT, debe cerciorarse que el reloj utilizado en el servicio de Emisión de Sellos Digitales de Tiempo se encuentre sincronizado con el UTC y este tenga un rango de exactitud de ± 3 milisegundos.

Específicamente:

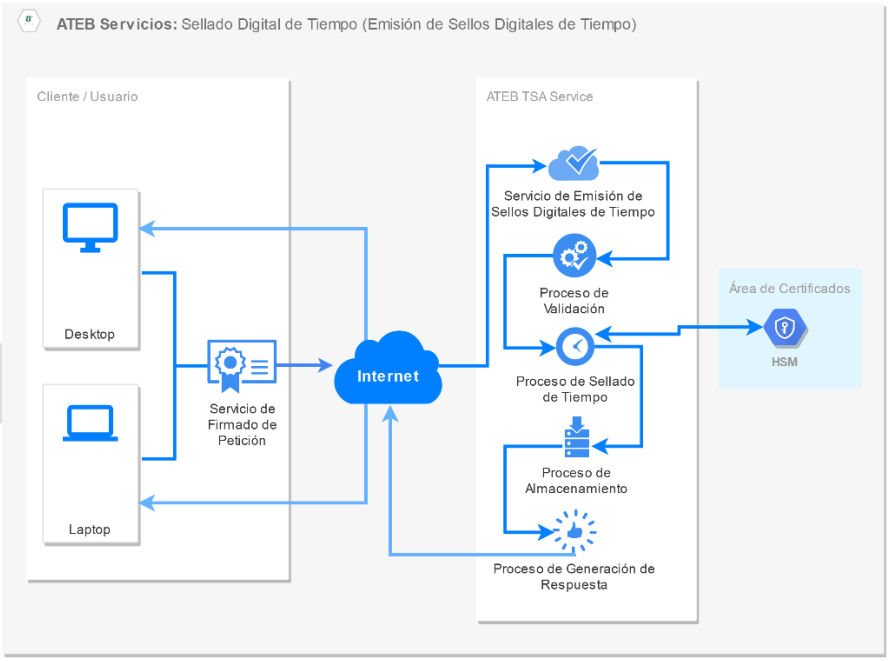
- Deberán estar protegidos contra amenazas que pudieran derivar un cambio no detectado que modifique su calibración, lo que podría ocasionar un cambio en la exactitud del servicio.
- ATEB debe asegurar que la sincronización del reloj se mantenga constante cuando ocurra un segundo intercalar, cuando este sea notificado por un organismo autorizado. El segundo intercalar ocurrirá en el último minuto de la última hora del día, siempre y cuando el segundo intercalar esté programado para ocurrir. El registro de un Sello Digital de Tiempo debe mantener el tiempo exacto (±3 milisegundos) cuando ocurra este cambio.
- La ASDT debe asegurar que, si el tiempo que debe indicarse en la Emisión de Sellos Digitales de Tiempo varía o se desvía de la sincronización con el UTC, este será detectado y dejará de expedir Sellos Digitales de Tiempo hasta que se re-sincronice con el UTC provisto por el CENAM o por lo Secretaría de Economía.

## 5.6 EMISIÓN Y CONSULTA DE LOS SELLOS DIGITALES DE TIEMPO

**Emisión:**

1. Se recibe la solicitud del Sello Digital de Tiempo 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 consultado los datos del certificado público de firma electrónica del cliente.
   - **Firma Electrónica** de la petición del Sello Digital de Tiempo. 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 el Sello Digital de Tiempo.
4. Se genera la respuesta
5. Se almacena el Sello Digital de Tiempo para su futura verificación y
6. Se envía la respuesta a la solicitud del Sello Digital de Tiempo que contiene un archivo con extensión. tsr con el formato ASN.1 del RFC 3161

A continuación, se muestra el diagrama del proceso de Emisión de Sellos Digitales de Tiempo:

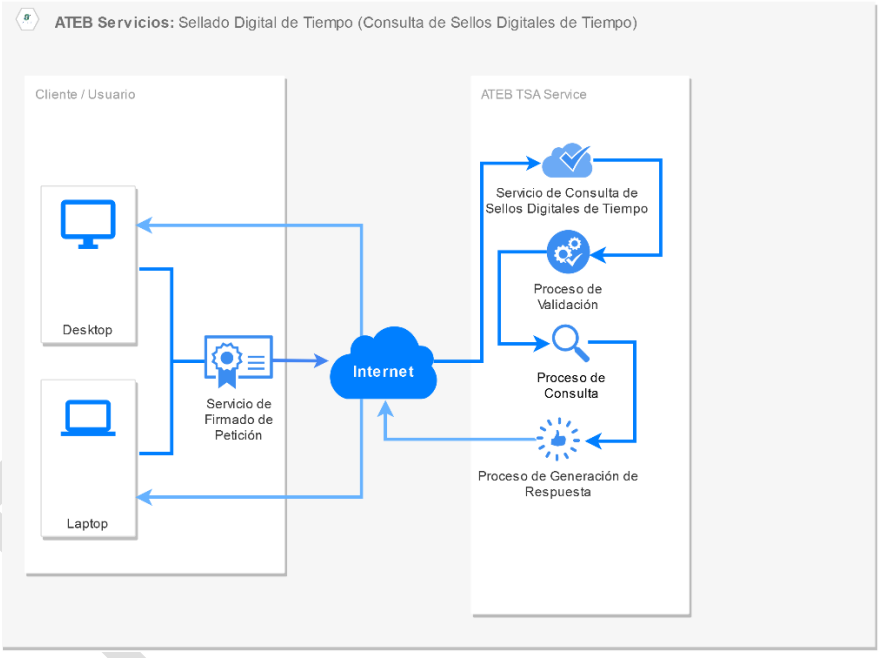


**Consulta:**

1. Recibe la solicitud de validación del Sello Digital de Tiempo 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 del Sello Digital de Tiempo. 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 del Sello Digital de Tiempo 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. tsr con el formato ASN.1.del RFC 3161.

   A continuación, se muestra el diagrama de consulta de Sellos Digitales de Tiempo:




# 6. Políticas del servicio de Emisión de Sellos Digitales de Tiempo

En estas políticas se establece el cumplimiento de los requerimientos humanos, económicos, materiales y tecnológicos necesarios para poder emitir los sellos digitales de tiempo y en las que estarán basadas las Declaraciones de Prácticas del servicio de Emisión de Sellos Digitales de Tiempo.

## 6.1 Políticas generales para el servicio de Emisión de Sellos Digitales de Tiempo

### • Política de Seguridad de la Información

1. La Seguridad de la Información es un asunto que está directamente relacionado al riesgo de la operación del servicio de Emisión de Sellos Digitales de Tiempo.

2. El área asignada al servicio de Emisión de Sellos Digitales de Tiempo debe incorporar un procedimiento de Seguridad 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 el servicio de Emisión de Sellos Digitales de Tiempo no deben ser realizadas por proveedores externos.

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

   • 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 relacionados con la Seguridad de la Información para este servicio, entre las que se encuentran Ley Federal de Protección de Datos Personales en Posesión de Particulares, la Ley Federal y General de Acceso a la Información Pública Gubernamental y las Reglas Generales a las que deben sujetarse los Prestadores de Servicios de Certificación.

### • Política sobre los responsables de Seguridad de la Información

1. 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 del servicio de Emisión de Sellos Digitales de Tiempo.

## 6.2 Políticas específicas para el servicio de Emisión de Sellos Digitales de Tiempo

### • 6.2.1 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 Emisión de Sellos Digitales de Tiempo esté protegida en todo momento de su revelación no autorizada, ya sea a personal interno o externo a la organización.

2. La Seguridad de la Información es un asunto que está directamente relacionado al riesgo de la operación del servicio de Emisión de Sellos Digitales de Tiempo.

Para poder asegurar de una manera efectiva la información, por lo que el área asignada para la gestión del servicio de Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo.

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 Emisión de Sellos Digitales de Tiempo.

## - 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo, 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 Emisión de Sellos Digitales de Tiempo.
d. Controles de acceso físico, como seguridad policial, CCTV, señalización, bitácoras de entrada y salida del espacio asignado al servicio de Emisión de Sellos Digitales de Tiempo.
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 Emisión Sello Digital de Tiempo 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.
2. Debe autorizar el sistema de información o persona con responsabilidades funcionales sobre el servicio de Emisión de Sellos Digitales de Tiempo para controlar el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber validado el proceso de autenticación.
3. Debe verificar el correcto funcionamiento de las políticas o medidas de seguridad establecidas para el servicio de Emisión de Sellos Digitales de Tiempo.

## - 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo.

2. Las auditorías y revisiones de cumplimiento deben ser efectuadas por personal independiente al encargado de brindar el servicio de Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo.

- **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.

   a) Mientras el nivel de riesgo o el impacto sea más alto se atenderán y resolverán primero.

4. 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 Emisión de Sellos Digitales de Tiempo.

- **Especificaciones de la Política**

1. A todos los activos de la información del servicio de Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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.

## • 6.2.2 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 Emisión de Sellos Digitales de Tiempo, 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 Emisión de Sellos Digitales de Tiempo, 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 Emisión de Sellos Digitales de Tiempo.

4. Se deben proteger el área asignada al servicio de Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo, 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 y el área asignada para el servicio de Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo 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 la información del servicio de Emisión de Sellos Digitales de Tiempo se deben llevar registros de los hashes de control para cada una de las llaves 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 Emisión de Sellos Digitales de Tiempo 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.

## • 6.2.3 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 Emisión de Sellos Digitales de Tiempo 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 Emisión de Sellos Digitales de Tiempo debe manejar de manera correcta y adecuada la información con la que operan este servicio, 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 Emisión de Sellos Digitales de Tiempo, 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 participantes del Servicio de Emisión de Sellos Digitales de Tiempo, 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 Sello Digital de Tiempo, 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 Sello Digital de Tiempo.

b) Las telecomunicaciones

c) El control de accesos físicos al área de Sello Digital de Tiempo

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 Emisión de Sellos Digitales de Tiempo

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 Sello Digital de Tiempo.
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 Sello Digital de Tiempo 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, y 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”
2. (USER ID).
3. Las claves de los usuarios deben ser de fácil definición para que estas puedan ser fácilmente identificadas y asociadas al usuario.
4. 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 Sello Digital de Tiempo:

- Controles de acceso a las aplicaciones del servicio de Sello Digital de Tiempo
- Manejo de las claves de usuarios y sus contraseñas de autenticación
- Manejo de seguridad por roles y actividades

- **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).

## 6.3 ESTÁNDARES

1. Todo aquel que solicite la Emisión de Sellos Digitales de Tiempo estará aceptando los términos y condiciones establecidas en este documento.

2. ATEB no se hace responsable por el uso que se le dé al Sello Digital de Tiempo emitido por cualquier solicitante, deslindándose así de toda responsabilidad del mal o indebido uso de estos.

3. ATEB es el responsable de cumplir con todo lo estipulado en el presente documento referente a la prestación del servicio de Emisión de Sellos Digitales de Tiempo, siendo así que permite la auditoría e investigación pertinentes por parte de las autoridades relevantes para verificar el buen y correcto funcionamiento del servicio, siempre y cuando estén debidamente fundamentadas y que quienes las realicen se acrediten como autorizados para llevarlas a cabo.

4. Cada vez que se actualice el presente documento se hará pública la última versión que se esté manejando, siendo así que en todo momento la Declaración de Prácticas y Políticas de Certificación se encontrará vigente en su última versión en la página web antes mencionada.

5. El acceso únicamente de lectura del presente documento es de uso público, siendo que cualquier modificación, actualización, sustitución o borrado de información será únicamente realizada por ATEB o por quien ATEB autorice previamente, estableciendo de esta manera, controles de acceso para evitar su modificación no autorizada, para más detalle revisar las Políticas Corporativas de Seguridad de la Información de ATEB.

6. Permitir las auditorías correspondientes al ejercicio de la Prestación de Servicios de Certificación por parte de la Secretaría de Economía en todo momento.

7. Aplicar la política de No repudio en el envío de Mensaje de Datos.

## 6.4 SEGURIDAD DEL SERVICIO DE EMISIÓN DE SELLOS DIGITALES DE TIEMPO

El servicio de Emisión de Sellos Digitales de Tiempo utiliza 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 nosotros el 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 Emisión de Sellos Digitales de Tiempo 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 Sellos Digitales de Tiempo cifrado:**

Cada Sello Digital de Tiempo que se genera es almacenado de forma cifrada usando el algoritmo AES en bases de datos, con la finalidad de proteger la información digital.

**Almacenamiento de certificado para servicio de Emisión de Sellos Digitales de Tiempo:**

El dispositivo utilizado para almacenar el certificado del servicio de Emisión de Sellos Digitales de Tiempo es un HSM con certificación FIPS140-2 nivel l 3.

**Modulo criptográfico:**

Este módulo está conformado por un dispositivo HSM con certificación FIPS140-2 nivel l 3, el cual contempla los siguientes algoritmos de cifrado:

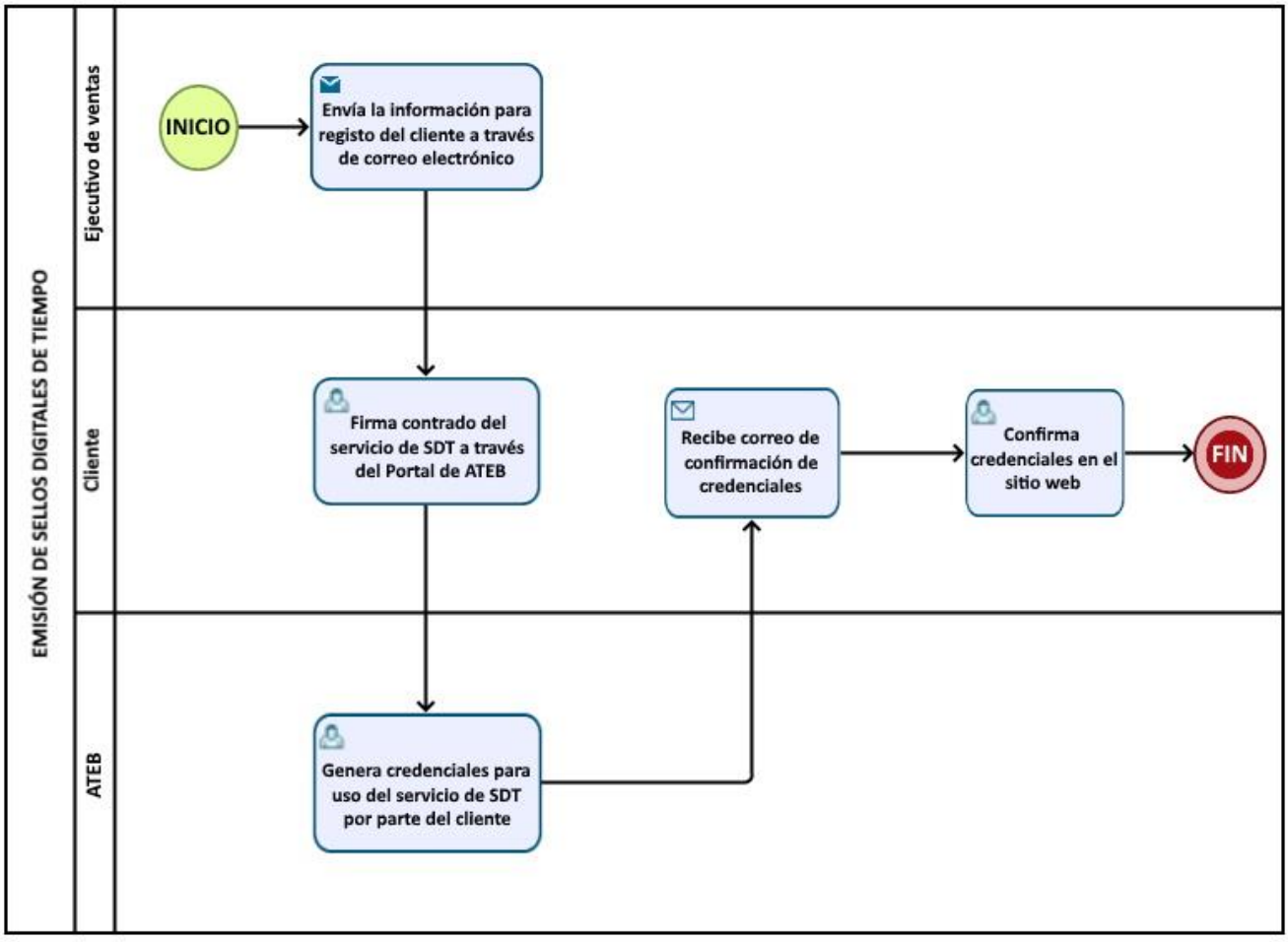
- SHA256
- SHA384
- SHA512

*Nota: Para la Emisión de Sellos Digitales de Tiempo, se utiliza el algoritmo SHA256.

# 7. Procedimientos de registro en servicio de Emisión de Sellos Digitales de Tiempo y gestión de fallas durante el funcionamiento con el cliente

## 7.1 Proceso 1: Registro en Servicio de Emisión de Sellos Digitales de Tiempo

### - Diagrama general del procedimiento

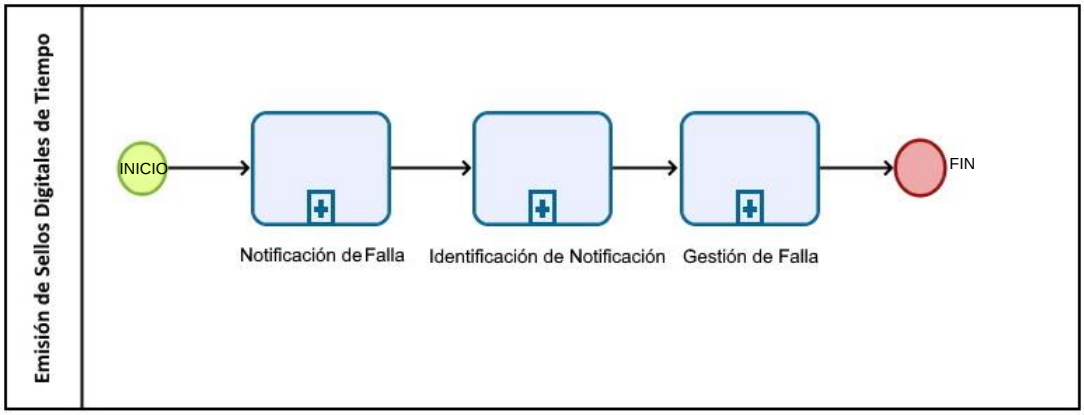


## - Descripción del procedimiento

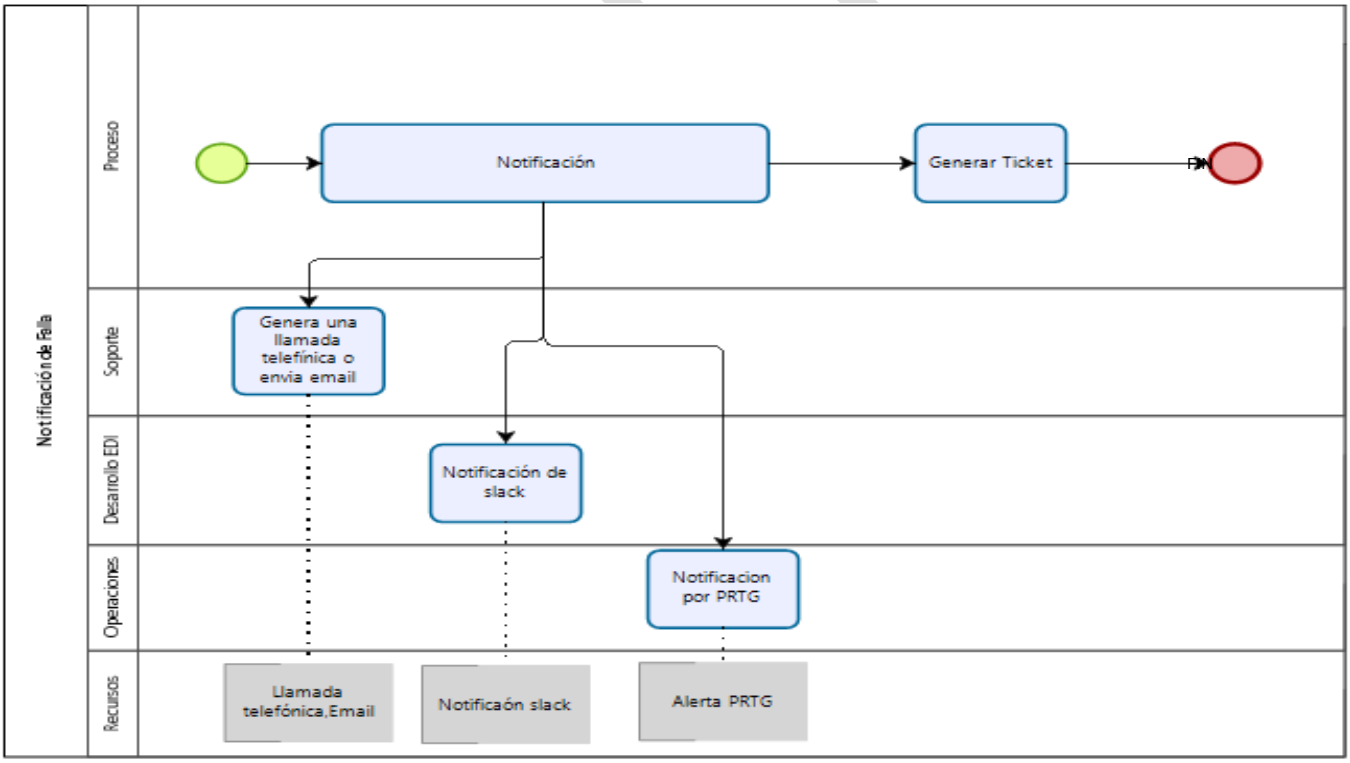
| No. | Actividad | Descripción | Responsable | Entrada | Salida |
|---|---|---|---|---|---|
| **1** | Enviar información para registro a través de correo electrónico | Envía información al cliente por correo electrónico para que este se registre en el portal de Registro | Ejecutivo de ventas | Solicitud de servicio de Emisión de Sellos Digitales de Tiempo | Envío de información para registro |
| **2** | Firmar el contrato de servicio de Emisión de Sellos Digitales de Tiempo de manera digital | Firma el contrato de solicitud del servicio de Emisión de Sellos Digitales de Tiempo a través del sitio web de ATEB | Cliente | Envío de información para registro | Contrato firmado |
| **3** | Generar credenciales para uso del servicio de Emisión de Sellos Digitales de Tiempo | Genera credenciales de cliente para uso del servicio de Emisión de Sellos Digitales de Tiempo | ATEB | Contrato firmado | Credenciales generadas |
| **4** | Recibir correo de confirmación de credenciales | Recibe correo electrónico donde se confirma la generación de credenciales para acceso al servicio de Emisión de Sellos Digitales de Tiempo | Cliente | Credenciales generadas | Correo de confirmación recibido |
| **5** | Confirmar credenciales | Confirma sus credenciales para el uso del servicio de Emisión de Sellos Digitales de Tiempo | Cliente | Correo de confirmación recibido | Credenciales confirmadas |
| **FIN DEL PROCEDIMIENTO** | | | | | |

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

### - Diagrama general del procedimiento



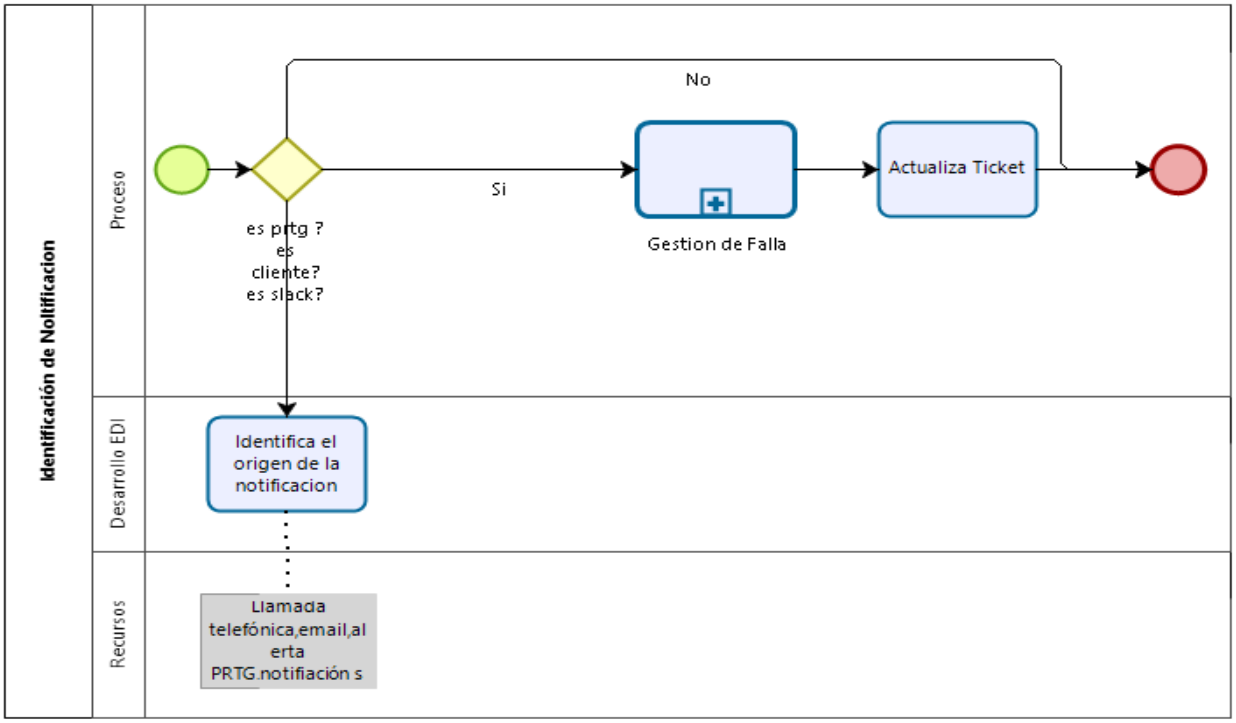

### - Subprocedimiento 1: Notificación de Falla



## - 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,**<br>**Si es Slack pasar a la actividad 4,**<br>**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

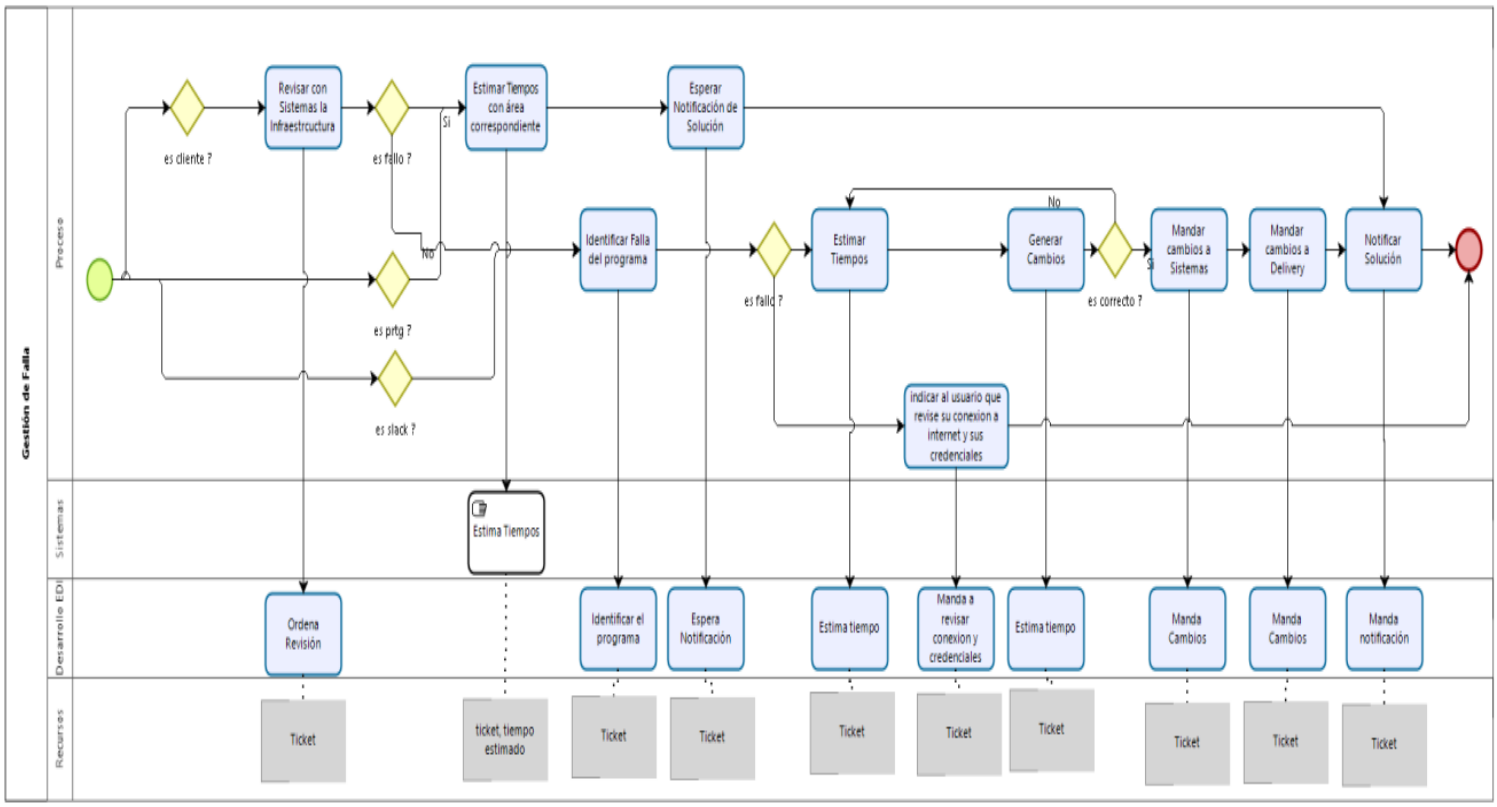



## - Descripción del procedimiento

| 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** | | | | | |
| **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

## - Diagrama del procedimiento



## - Descripción del procedimiento

| No. | Actividad | Descripción | Responsable | Entrada | Salida |
|---|---|---|---|---|---|
| **Si es Notificación del Cliente pasar a la actividad 1,**<br>**Si es Notificación de PRTG pasar a la actividad 2,**<br>**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 | Se mandan los cambios del | Desarrollo EDI | Ticket | Ticket |

| | | | | | |
|---|---|---|---|---|---|
| | Sistemas | programa a sistemas. | | | 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** | | | | | |

## 8. Consulta del documento

La información correspondiente al presente Manual de Declaración de Prácticas estará publicada en la página: **https://www.ateb.mx/psc.html** para su consulta.