PÚBLICO

ATEB

Política de Certificados del servicio de Emisión de Certificados Digitales

ATEB - BPM

Dirección General

Fecha de inicio de operaciones: 27/Oct./2026

Identificador de objeto: 2.16.484.101.10.316.100.9.1.1.1.1

Contenido

1. Información inicial 5

1.1 Información del documento 5

1.2 Registro de cambios y calendario de revisión, actualización y evaluación continua 5

1.3 Responsables de revisión y autorización 6

1.4 Clasificación de la información del documento 6

2. Introducción 7

2.1 Objetivo 8

2.2 Alcance 8

2.3 Referencias normativas 8

2.4 Definiciones 9

3. Tipos de Certificados a emitir por la Autoridad Certificadora 11

3.1 Importancia y uso de los certificados digitales 12

3.2 Procesos Operativos del Ciclo de Vida del Certificado 12

3.3 Controles de gestión, operativos y físicos 13

3.4 Controles técnicos de seguridad 16

3.5 Perfiles de Certificados, CRL y OCSP 16

4. Matriz RACI 18

5. Obligaciones y responsabilidades en el servicio de Emisión de Certificados Digitales (ECD) 18

5.1 Obligaciones de la AC 18

5.2 Obligaciones de la AR – Agentes Certificadores 20

5.3 Responsabilidades de la AC 21

5.4 Responsabilidades de la AR - Agentes Certificadores 21

5.5 Obligaciones de los solicitantes y suscriptores - usuarios 23

5.6 Responsabilidades de los solicitantes y suscriptores - usuarios 24

5.7 Obligaciones de la parte que confía 25

5.8 Responsabilidades de la parte que confía y del destinatario 26

6. Privacidad de datos 26

PÚBLICO

6.1 Protección de la Confidencialidad de la Información 26

6.1.1 Alcance de la Información Confidencial 26

6.1.2 Información que no se considera Confidencial 26

6.1.3 Responsabilidad de proteger la Información Confidencial 27

6.2 Protección de Datos Personales 27

6.2.1 Estándares 28

7. Procesos de operación que integran el Servicio de Emisión de Certificados Digitales de la Autoridad Certificadora 29

7.1 Tipos de Certificados Digitales que se entregarán 29

7.2 Personas que pueden solicitar el Servicio de Emisión de Certificados Digitales. Solicitud del Servicio de Emisión de Certificados Digitales 30

7.3 Registro y gestión de solicitudes de Certificados Digitales 30

7.4 Verificación de identidad 31

7.4.1 Objetivos, alcances y limitaciones de uso de los Certificados Digitales 36

7.4.2 Obligaciones y responsabilidades de la Autoridad Registradora – Agentes Certificadores 37

7.4.3 Obligaciones y responsabilidades de la Autoridad Certificadora 39

7.4.4 Limitaciones de responsabilidad 41

7.5 Generación de Certificados Digitales y controles para la generación de datos de creación de firma electrónica del usuario 42

7.6 Publicación de Certificados Digitales 42

7.7 Solicitud de sello de tiempo 43

7.8 Revocación de Certificados Digitales 43

7.9 Renovación de certificados digitales 44

8. Interoperabilidad 45

9. Publicación de la Política de Certificados 45

9.1 Identificador de objeto 46

10. Auditoría de cumplimiento 46

11. Otros asuntos comerciales y legales 46

11.1 Tarifas 46

11.2 Reembolsos 46

PÚBLICO

11.3 Seguros de Responsabilidad 47

11.4 Propiedad Intelectual 47

11.5 Suspensión o cese de funciones de la AC 47

11.6 Términos y Condiciones del servicio de Emisión de Certificados Digitales 47

PÚBLICO

1. Información inicial

1.1 Información del documento

Información del documento
Denominación formal del Documento: Plan Estratégico de Negocios en ATEB 2026-2030
Descripción: Política de Certificados del servicio de Emisión de Certificados Digitales
Organización: ATEB Servicios, S.A de C. V.
Fecha de elaboración del documento: 02/Abr./2026
Fecha de actualización del documento: 02/Abr./2026
Administrador: Auxiliar de Apoyo Informático de Seguridad
Patrocinador: Director General
Destinatario / usuario: **Interno**: Personal involucrado con el servicio de Emisión de Certificados Digitales. **Externo**: Secretaría de Economía, demás autoridades relevantes y competentes.

1.2 Registro de cambios y calendario de revisión, actualización y evaluación continua

La revisión de este documento se efectuará de manera periódica cada 12 (doce) meses a partir de su fecha de creación o de la fecha de su última actualización, o antes si las necesidades del negocio así lo requieren y se registrarán estas revisiones en la siguiente tabla de control de cambios.

Fecha	Autor	Versión	Referencia del cambio	Estatus del documento
02/Abr./2026	EAP	1.0	Definición inicial del documento	Aprobado

*Se anexa el calendario para los próximos años señalados, sin embargo, las fechas de actualización podrían ser modificadas con base en las necesidades del negocio.

Calendario de revisión del documento	
Mes / ***Año***	Abril
2027	Actualización

PÚBLICO

	Abril
2028	Actualización
	Abril
2029	Actualización
	Abril
2030	Actualización

1.3 RESPONSABLES DE REVISIÓN Y AUTORIZACIÓN

AUTORIZADO

_____

Profesional Jurídico

AUTORIZADO

_____

Profesional Informático

AUTORIZADO

_____

Auxiliar de Apoyo Informático de Seguridad

AUTORIZADO

_____

Director General

PÚBLICO

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 de **Uso interno.**

Bajo el esquema de clasificación de información el presente documento se clasifica como información:

• **Uso interno.** La información que solo será para compartirse con los socios de la empresa, los empleados y socios de negocio.

Se entenderá como “confidencialidad de la información” aquella información que está protegida en todo momento de su revelación sobre la divulgación no autorizada ya sea a personal interno o externo de la organización.

Confidencial. Se considera aquella información que cumpla con cualquiera de los siguientes apartados:

- Información que, si es divulgada a individuos no autorizados, podría repercutir en un impacto negativo y significativo para la organización, en sus obligaciones legales, regulatorias o en sus estados financieros.

- Información acerca de clientes, de empleados y de negocios de las organizaciones, a los que esté obligado a proteger.
- Información que las áreas de negocio determinen que tiene el potencial de perder ventajas competitivas o repercutir en impactos negativos y significativos para el negocio, si se divulga a individuos no autorizados.

- Que cumpla con cualquiera de las especificaciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, de la información considerada como “Confidencial”.

Por las características de los datos sensitivos del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable que brindamos a nuestros clientes como Prestador de Servicios de Certificación, todos los datos o la información que los pueda llegar a identificar de manera específica y que puedan poner en riesgo el negocio del cliente, su situación financiera, de imagen o salud de los individuos que trabajen o representen a los intereses de la empresa, será clasificada bajo el esquema CONFIDENCIAL siempre y cuando así lo estipule formalmente el Cliente.

Toda la información que el cliente haya establecido como CONFIDENCIAL deberá estar protegida tanto en su almacenamiento, tránsito y medios que la contengan.

Esta información se genera dentro de los procesos operativos y administrativos de la organización, si se divulga o revela tendría un efecto negativo al personal y/o a la organización.

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

2. Introducción

Esta política cumple con los requerimientos que se establecen en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación de acuerdo con la estructura y contenido que deben considerarse como parte del proceso de registro y emisión de certificados digitales por la autoridad correspondiente y atendiendo a la definición y alcance que se establece dentro del Código de Comercio. Así mismo, dentro de esta se establecen los lineamientos a través de los cuales se da cumplimiento a los requerimientos para la Emisión de Certificados Digitales de firma electrónica avanzada definidos en el estándar ETSI EN 319 411-1 V1.5.1. (2025-04) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service

PÚBLICO

Providers issuing certificates, el cual sustituye al estándar ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates y el RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, con los cuales es compatible.

2.1 Objetivo

Establecer los lineamientos, procedimientos y controles necesarios para la emisión, administración, renovación y revocación de certificados digitales, garantizando su confidencialidad, integridad, disponibilidad y autenticidad, en cumplimiento con la normativa aplicable y las mejores prácticas internacionales. Esta política busca asegurar que los servicios de certificación proporcionados por el PSC sean confiables, seguros y transparentes, protegiendo la información de los usuarios y manteniendo la continuidad operativa del servicio.

2.2 Alcance

Esta política aplica a todos los Certificados Digitales emitidos, renovados y/o revocados por ATEB Autoridad Certificadora para los suscriptores, usuarios y demás partes interesadas, asegurando que cumplan con los estándares legales y técnicos, estableciendo la confianza del usuario en el servicio de Emisión de Certificados Digitales.

2.3 Referencias normativas

- ETSI EN 319 411-1 V1.5.1. (2025-04) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates, el cual sustituye al estándar ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profileson
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación de la Secretaría de Economía.
- LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Código de Comercio.
- Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

PÚBLICO

2.4 DEFINICIONES

Concepto	Definición
AC	Autoridad Certificadora (CertificationAuthority)
AR	Autoridad Registradora (RegistrationAuthority)
ARCO	Acceso, Rectificación, Corrección y Oposición.
Auditoría	Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.
Centro de Datos	Es una instalación física que alberga la infraestructura de Tecnologías de la Información para crear, ejecutar y entregar aplicaciones y servicios.
Certificado	Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
CRL	Certificate Revocation List (Lista de Certificados Revocados).
DPC	Declaración de Prácticas de Certificación
ETSI TS	European Telecommunications Standards Institute Technical Specification
FIPS	Federal Information Processing Standards (Normativa Federal de Procesamiento de Información)
Firma Electrónica Avanzada o Fiable	Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97 del Código de Comercio.
Firmante – Suscriptor – Usuario	Persona que posee los datos de la creación de la firma y actúa en nombre propio o de la persona a la que representa.
HSM	Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y aporta funcionalidad criptográfica de clave pública (PKI) de alto rendimiento efectuada dentro del mismo
Infraestructura de Clave Pública (PKI)	Es un sistema de tecnologías, políticas y procedimientos que permite garantizar la seguridad de las comunicaciones digitales, principalmente mediante el uso de claves

PÚBLICO

	criptográficas y certificados digitales que emitidos dentro de una PKI permiten confirmar la identidad de las partes que participan en una comunicación, asegurando la confianza y seguridad en las transacciones digitales.
ISO	Information Security Officer (Oficial de Seguridad de la Información)
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission (Organización Internacional de Normalización/Comisión Electrotécnica Internacional)
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de Particulares
Llave privada o Clave Privada	Se mantiene en secreto y se utiliza para descifrar los datos que han sido cifrados con la llave o clave pública. Solo el propietario de la llave privada puede acceder a la información.
Llave pública o Clave Pública	Se comparte abiertamente y se utiliza para cifrar datos. Cualquier persona puede usarla para enviar mensajes seguros a quien posee la llave privada.
Mensaje de Datos	Información generada, enviada, recibida o archivada por medios electrónicos, ópticos u otros.
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología de Estados Unidos de América)
OCSP	Online Certificate Status Protocol (Protocolo de Estado de Certificado en Línea)
OID	Object Identifier Digital (Identificador Digital de Objetos)
Página Web	Sitio en Internet de la Autoridad Certificadora que contiene información, aplicaciones y, en su caso, vínculos a otras páginas.
PC	Política de Certificados.
Parte que confía	La Persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.
Prestador de Servicios de Certificación (PSC)	De acuerdo con el Art. 89 del Código de Comercio, es la persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios

PÚBLICO

	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.
Reglas	Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación
RFC	Request for Comments (Solicitud de Comentarios)
Sello Digital de Tiempo	El registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello.
SGSI	Sistema de Gestión de Seguridad de la Información.
Solicitante	Cualquier Persona Física que solicite los servicios de Emisión de Certificados Digitales en cualquiera de sus procesos para sí misma o en representación de una Persona Moral.
URL	(Uniform Resource Locator) es la dirección única que identifica la ubicación de un recurso específico en Internet, como una página web, una imagen o un archivo

3. Tipos de Certificados a emitir por la Autoridad Certificadora

La Autoridad Registradora ATEB, a través de su sistema entregará lo siguientes tipos de Certificados Digitales generados por la Autoridad Certificadora, que cumplen con los requerimientos dispuestos en las fracciones I a IV del artículo 97 del Código de Comercio:

Certificados Digitales de Firma Electrónica Avanzada o Fiable

Identidad Personal: Este tipo de Certificados Digitales son expedidos a personas físicas para garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

Representación: Este tipo de Certificados Digitales son expedidos a personas físicas con facultades legales para representar a una persona moral con el objeto de garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

Los Certificados Digitales de Firma Electrónica Avanzada o Fiable que emite la Autoridad Certificadora ATEB, tienen un tamaño de llave de 2048 bits y son creados con criptografía RSA (algoritmo de cifrado asimétrico Rivest-Shamir-Adleman) y el algoritmo de firmado usado es SHA256.

El alcance y las limitaciones de los Certificados Digitales, así como las obligaciones y responsabilidades que contrae el suscriptor al utilizar los Certificados Digitales, se encuentran en la

PÚBLICO

Política de Certificados y la Declaración de Prácticas de Certificación, las cuales se pueden consultar en su Página Web https://www.ateb.mx/psc.html y en el Portal de búsqueda y descarga https://psc.ateb.com.mx:7011.

3.1 IMPORTANCIA Y USO DE LOS CERTIFICADOS DIGITALES

El Certificado Digital de Firma Electrónica Avanzada o Fiable se puede utilizar para los siguientes fines:

- **Firma Digital:** Firmar documentos electrónicos reemplazando la firma autógrafa, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

- **Sin repudio:** Garantiza que el firmante no puede negar haber realizado una acción o enviado un mensaje, debido a que, el certificado digital, vincula inequívocamente el mensaje al mismo, quien utiliza una clave privada única.

- **Cifrado de datos:** Convertir información legible (texto plano) en un código ilegible (texto cifrado).

- **Acuerdo de clave:** Protocolo criptográfico donde dos o más partes establecen de forma segura una clave secreta compartida, utilizada para cifrar y descifrar comunicaciones.

Con lo anterior, se da certeza jurídica y se aporta mayor nivel de seguridad y blindaje normativo a los documentos firmados.

3.2 PROCESOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

El ciclo de vida del certificado digital comprende las actividades necesarias para su gestión integral, el cual, está integrado por las siguientes fases que garantizan la correcta administración y confiabilidad de los certificados digitales por parte de ATEB Autoridad Certificadora.

- **Solicitud del Certificado.** Se realiza conforme a lo establecido en el apartado 7.2 de la presente Política de Certificados.
- **Gestión de Solicitudes.** La gestión y registro de solicitudes se llevada a cabo conforme lo señala en el apartado 7.3 de la presente Política de Certificados.
- **Emisión de Certificados.** Comienza concluido el proceso de verificación de identidad, para lo cual, es necesario que el suscriptor – usuario genere su par de llaves requeridas para la Emisión del Certificado Digital, como se describe en el apartado 7.5 de la presente Política de Certificados, mismo que tiene asociado su sello digital de tiempo.
- **Aceptación del Certificado.** El suscriptor – usuario una vez que ha descargado su Certificado Digital debe de verificar como parte de sus responsabilidades y obligaciones que, los datos sean correctos, notificando su aceptación del Certificado Digital por correo electrónico.
- **Usos del Certificado.** El suscriptor – usuario sólo deberá utilizar el certificado digital para los fines que ha sido emitido, conforme a lo establecido en el apartado 7.4.1.de la presente Política de Certificados así como sus limitaciones de uso, las cuales se señalan en el mismo apartado.

PÚBLICO

- **Renovación del Certificado.** Se debe realizar conforme al apartado 7.9 de la presente Política de Certificados**.** No se podrá realizar una renovación de forma remota por más de una ocasión.

- **Revocación del Certificado.** Se puede llevar a cabo conforme a lo señalado en el apartado 7.8 de la presente Política de Certificados**.**

- **Servicios de Consulta y Estado del Certificado. Se encuentran publicados en las siguientes URL´s:**

  - Portal de búsqueda y descarga https://psc.ateb.com.mx:7011
  - CRL Lista: https://psc.ateb.com.mx:7012/psc/crl/list
  - CRL Delta: https://psc.ateb.com.mx:7012/psc/crl/delta
  - OCSP https://psc.ateb.com.mx:7013/psc/ocsp/response

- **Finalización del servicio.** El suscriptor que desee finalizar el servicio deberá notificarlo a ATEB Autoridad Certificadora, quien conservará los registros de sus datos conforme a la normativa aplicable y para los fines que establezcan las autoridades regulatorias.

3.3 CONTROLES DE GESTIÓN, OPERATIVOS Y FÍSICOS

Seguridad física

La Seguridad Física que se tiene establecida para la prestación del servicio de Emisión de Certificados Digitales es compatible con el estándar ETSI EN 319 411-1 V1.5.1 (2025-04) Sección 6.4.2 “Physical security controls” considerando los apartados, conceptos y recomendaciones que ahí se señalan, el cual, sustituye al ETSI TS 102 042 V2.4.1, Sección 7.4.4 “Physical and Environmental Security”, siendo compatibles con el estándar actual.

Las instalaciones y áreas asignadas para la prestación del servicio de Emisión de Certificados Digitales, en los centros de datos donde residen y se ejecutan las aplicaciones críticas, no críticas y sensibles, se encuentran en lugares seguros, libres de amenazas de alto impacto y con controles de protección perimetrales, controles de señalización de seguridad y con la infraestructura de seguridad, instalación eléctrica y monitoreo que minimiza cualquier riesgo y la posibilidad de detener las operaciones.

De igual manera en la Política de Seguridad Física, se consideran los requerimientos de seguridad para el personal, así como en los Procedimientos de control de acceso a las instalaciones de los centros de datos y de la oficina administrativa.

Seguridad del personal

Roles de confianza

Para asegurar que los elementos humanos contratados por ATEB que participan en la Emisión de Certificados Digitales cumplan con los requisitos, conocimientos, experiencia y calificaciones requeridos, se cuenta con el Procedimiento de Reclutamiento, Selección, Evaluación y Contratación de Personal para el Servicio de Emisión de Certificados Digitales, el cual, sirve como herramienta para validar que quienes ocupen los roles de confianza sean evaluados y seleccionados

PÚBLICO

correctamente, contribuyendo al logro de los objetivos establecidos en materia de Seguridad de la Información.

ATEB cuenta con los elementos humanos necesarios y requeridos por la autoridad regulatoria para la prestación del servicio de Emisión de Certificados Digitales.

Número de personas necesarias por tarea

ATEB requiere que cada tarea sea realizada por 2 personas que posean un rol de confianza.

Separación de funciones

Requisitos de conocimiento, calificaciones y experiencia

ATEB se asegura de que todas las personas asignadas a los roles de confianza tengan la experiencia, las calificaciones y la confiabilidad requeridas para desempeñar sus funciones asignadas.

Verificación de antecedentes y evaluación de confianza

ATEB, durante su proceso de reclutamiento, selección, evaluación y contratación de personal para el servicio de Emisión de Certificados Digitales, realiza la verificación de los antecedentes penales y pruebas de confiabilidad del personal que forma parte de los roles de confianza.

Requisitos de formación

ATEB proporciona capacitación de habilidades relevantes a todos los elementos humanos involucrados en las operaciones de Prestador de Servicios de Certificación para el servicio de Emisión de Certificados Digitales.

La formación se imparte mediante un programa de capacitación constante en el que participan las áreas involucradas, con base a las funciones laborales de la persona y abarca, entre otros los siguientes temas: Conocimientos básicos de criptografía asimétrica; Versiones de software utilizadas por ATEB; Seguridad de la Información; Procedimientos de recuperación en casos de desastre y continuidad del negocio y Protección de Datos Personales.

Sanciones por acciones no autorizadas

Cualquier colaborador que se encuentre que ha violado la normatividad de ATEB, incluyendo de manera enunciativa más no limitativa, las leyes, códigos, reglamentos, procedimientos, políticas, etc., estará sujeto a acciones disciplinarias correctivas considerando el grado de incumplimiento.

Registros de auditoría

Recopilación de auditorías

ATEB cuenta con un Procedimiento de Auditoría, el cual, tiene como objetivo determinar los lineamientos y bases para establecer la forma correcta de realizar auditorías y emitir los resultados correspondientes.

Todas las auditorías que se requieran hacer en la organización se realizan con el fin de encontrar mejoras en los procesos y actividades actuales e implementarlas para una mejor eficacia en las operaciones.

PÚBLICO

Tipos de eventos registrados

Los sistemas de ATEB requieren identificación y autenticación en el inicio de sesión del sistema con un nombre de usuario y contraseña únicos. Se registran importantes acciones del sistema para establecer la responsabilidad de los operadores que inician tales acciones.

Para cada evento, ATEB registra (i) fecha y hora, (ii) tipo de evento, (iii) éxito o fallo, y (iv) usuario o sistema que causó el evento o inició la acción, asegurando el registro del tiempo preciso de cualquier evento significativo de los servicios de Prestador de Servicios de Certificación.

Frecuencia de procesamiento o archivo de registro de auditoría

ATEB realiza las auditorías correspondientes al servicio de Emisión de Certificados Digitales de forma anual con el objetivo de asegurar que, todas las áreas involucradas en la revisión de los eventos registrados para la generación de reportes cumplan con los procesos establecidos referentes a la documentación y con todos los requisitos necesarios para operar el servicio, así como también para mantener su compromiso de mejora continua.

Adicionalmente a las auditorías internas realizadas por ATEB, la Secretaría de Economía tiene la facultad de realizar visitas de verificación para validar el cumplimiento de los requisitos establecidos en la normativa aplica al servicio de Emisión de Certificados Digitales.

Período de conservación del registro de auditoría

El periodo de resguardo definido por ATEB para sus reportes de auditoría es un plazo de (10) diez años.

Protección del registro de auditoría

Los reportes de auditoría de ATEB son almacenados en un repositorio interno, con cumplimiento en las políticas de seguridad internas.

Copia de seguridad de respaldo de los registros de auditoría

ATEB realiza respaldos completos de manera semanal, los cuales se resguardan de manera segura en diferentes sitios.

Los registros de auditoría de seguridad se guardan en base de datos y se aplica el procedimiento de respaldo.

Compromiso y recuperación ante desastres

Plan de Continuidad de Negocio (BCP)

En ATEB es primordial contar con un procedimiento que sirva de guía y que permita la gestión de la continuidad del negocio, que considere controles administrativos, operativos y tecnológicos necesarios para continuar con las operaciones del servicio de Emisión de Certificados Digitales, por ello, ha desarrollado el Plan de Continuidad de Negocio.

Plan de Recuperación ante Desastres (DRP)

Con el fin de asegurar una respuesta y recuperación ante desastres de cualquiera de los elementos necesarios para la prestación del servicio de Emisión de Certificados Digitales, se cuenta con el

PÚBLICO

Plan de Recuperación ante Desastres que contempla diversas fases que contribuyen a lograr una recuperación pronta y efectiva.

3.4 CONTROLES TÉCNICOS DE SEGURIDAD

Generación de par de claves de la AC

La generación de las claves utilizadas para el servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada se realiza a 4096 bits y un algoritmo de firma SHA256RSA en equipos HSM, de la marca Futurex, modelo Vectera Plus 100, los cuales, cuentan con la Certificación FIPS140-2 nivel l 3.

Generación de par de claves de los certificados digitales emitidos por la AC

Los Certificados Digitales de Firma Electrónica Avanzada o Fiable que emite la Autoridad Certificadora ATEB, tienen un tamaño de llave de 2048 bits y son creados con criptografía RSA (algoritmo de cifrado asimétrico Rivest-Shamir-Adleman) y el algoritmo de firmado usado es SHA256.

La vigencia de estos certificados es de 2 (dos) años.

3.5 PERFILES DE CERTIFICADOS, CRL Y OCSP

Estructura de Certificados

Bajo el estándar ISO/IEC 9594-8 Information technology--Open Systems Interconnection--The Directory--Part 8: Public-key and attribute certificate frameworks, y el RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profileson, la Autoridad Certificadora ATEB, ofrece el servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable, a través de un sistema que permite la generación y emisión de los siguientes tipos de Certificados Digitales, que cumplen con los requerimientos dispuestos en las fracciones I a IV del artículo 97 del Código de Comercio:

Certificados Digitales de Firma Electrónica Avanzada o Fiable

Identidad Personal: Este tipo de Certificados Digitales son expedidos a personas físicas para garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

Representación: Este tipo de Certificados Digitales son expedidos a personas físicas con facultades legales para representar a una persona moral con el objeto de garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

Los nombres de los certificados estarán compuestos por número de serie y Registro Federal de Contribuyentes. En el caso de extranjeros con su número de identificador asignado por Migración y por número de serie.

En la nominación de los certificados digitales emitidos por ATEB Autoridad Certificadora, no se admite el uso por ningún motivo de anónimos ni pseudónimos para identificar los nombres de las

PÚBLICO

personas físicas o morales titulares.

La estructura de los Certificados Digitales contiene lo datos requeridos en el artículo 108 del Código de Comercio, con lo cual, se garantiza su validez.

Estructura de la CRL

ATEB Autoridad Certificadora publica su Lista de Certificados Revocados (CRL) para asegurar la interoperabilidad en los servicios de Emisión de Certificados Digitales, permitiendo verificar de manera permanente si un certificado ha sido revocado o no.

La CRL está alineada y es compatible con la última versión del estándar ISO/IEC 9594-8:2020 Information Technology — Open Systems Interconnection Part 8: The Directory: Public Key and attribute certificate frameworks y al RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile versión 2, en la cual se resaltan los siguientes datos:

- Algoritmo de firma de la AC utilizado
- Nombre del emisor de la CRL
- Fecha y hora de emisión de la CRL.
- Fecha en que se emitirá la próxima CRL
- Número de serie de los certificados revocados.
- Fecha y hora de revocación.
- Número de versión

La CRL deberá ser firmada por ATEB, con sus datos de Creación de Firma Electrónica.

La lista se actualizará en periodos no mayores a veinticuatro (24) horas, apegándose a las Reglas Generales emitidas por la Secretaría de Economía, para los Prestadores de Servicios de Certificación (PSC) y el RFC 5280

El servicio de consulta de CRL crea dos tipos: List y Delta:

- CRL Lista, la cual, recupera todos los certificados revocados hasta antes del día actual en el que se realiza la consulta. Esta lista se puede consultar en la siguiente URL https://psc.ateb.com.mx:7012/psc/crl/list
- CRL Delta, la cual, recupera los certificados revocados el día actual en el que se realiza la consulta. Esta lista se puede consultar en la siguiente URL https://psc.ateb.com.mx:7012/psc/crl/delta

Estructura del OCSP

El Protocolo en Línea del Estado de los Certificados (OCSP), es otro de los servicios que ATEB Autoridad Certificadora pone a disposición de los suscriptores y demás partes interesadas, para conocer el estado actual de los certificados digitales emitidos, con el fin de validar si se encuentran vigentes, es decir, válidos o, si han sido revocados.

El servicio de consulta a través del OCSP, se realiza conforme a lo establecido en el RFC 6960 - X.509 Internet Public Key InfrastructureOnline Certificate Status Protocol - OCSP, alineándose a este estándar.

PÚBLICO

La URL para consultar el estado de los certificados mediante el OCSP es: https://psc.ateb.com.mx:7013/psc/ocsp/response

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.	Information Security Officer (ISO)	*	*	*	—
6.	Auxiliar de Apoyo Informático de Administrador de Redes	—	—	*	*
7.	Auxiliar de Apoyo Informático de Operador de Sistemas	—	—	*	*
8.	Auxiliar de Apoyo Informático de Administrador de Sistemas	—	—	*	*
9.	Auxiliar de Apoyo Informático de Administrador de Bases de Datos	—	—	*	*
10.	Agente certificador	—	*	—	—

Nota: (*) Participa; (—) No participa

5. Obligaciones y responsabilidades en el servicio de Emisión de Certificados Digitales (ECD)

5.1 Obligaciones de la AC

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

1) Asegurar que la presente Política de Certificados se cumpla y esté acorde con la Política de Seguridad de la Información, con la Declaración de Prácticas de Certificación y los Procedimientos Operacionales de las Autoridades Certificadora y Registradora.

PÚBLICO

2) Asegurar el cumplimiento de los Términos y Condiciones, así como, con lo establecido en la presente Política de Certificados, en la Declaración de Prácticas de Certificación y en los procesos operativos y administrativos relacionados con el servicio de emisión de Certificados Digitales.

3) Aplicar los controles de acceso a las instalaciones donde se ejecutan los procesos del servicio de emisión de Certificados Digitales.

4) Garantizar en todo momento la Seguridad de la Información proporcionada por las partes interesadas, preservando su Confidencialidad, Integridad y Disponibilidad y dando cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

5) Informar al suscriptor - usuario los requisitos que debe cumplir relacionados con la prestación del servicio de emisión de Certificados Digitales.

6) Informar al suscriptor - usuario los términos y condiciones en que se prestarán los Servicios de Emisión de Certificados Digitales.

7) Contar con un control de accesos que apoye a validar la identidad de los usuarios que utilizan los servicios y los sistemas, con la finalidad de salvaguardar la integridad de la información suministrada.

8) Contar con los elementos humanos, tecnológicos, materiales y económicos necesarios para brindar el servicio de emisión de Certificados Digitales.

9) Brindar Soporte Técnico para entregar solución a los inconvenientes presentados durante la prestación del servicio de emisión de Certificados Digitales.

10) Realizar y permitir auditorías para verificación del cumplimiento correcto y completo del servicio acreditado.

11) Realizar respaldos incrementales de manera diaria y completos de manera semanal.

12) Contar con un plan para la respuesta y recuperación de la operación ante desastres y de continuidad de negocio que garantice que las operaciones no se interrumpan.

13) Utilizar elementos y dispositivos de seguridad para garantizar un entorno seguro para la información del suscriptor - usuario y demás partes interesadas.

14) Garantizar la autenticidad e integridad de los certificados emitidos en el transcurso del tiempo.

15) Salvaguardar la llave privada del Certificado que utilizará la AC para la emisión de Certificados Digitales.

16) No copiar ni almacenar las llaves privadas de los certificados emitidos a los suscriptores – usuarios.

17) Emitir los certificados de las solicitudes autorizadas por la Autoridad Registradora con base en la legislación aplicable y de acuerdo con lo contratado por los suscriptores - usuarios.

PÚBLICO

18) Garantizar que todos los certificados emitidos y/o revocados cuenten con un Sello Digital de Tiempo.

19) Almacenar de forma segura los certificados y administrar de forma efectiva los directorios, actualizando oportunamente el estado de los certificados.

20) Publicar y poner a disposición de las partes interesadas, servicios de consulta, descarga y estado de los certificados CRL y OCSP con alta disponibilidad.

21) Asegurar el almacenamiento y actualización de las CRL y estados de los certificados OCSP.

22) Enviar en línea una copia de cada certificado digital emitido a la Secretaría de Economía.

23) Informar de inmediato a los suscriptores cuando sus certificados hayan sido revocados por alguna causal de revocación.

24) Informar a la Secretaría de Economía sobre cualquier incidente que pueda comprometer la prestación de los servicios de emisión de Certificados Digitales.

25) Poner a disposición de las partes interesadas en los medios establecidos, los procedimientos para la renovación o revocación de un certificado digital, así como los requisitos necesarios.

26) Entregar de forma segura los archivos correspondientes de los Certificados Digitales emitidos.

27) Poner a disposición de los suscriptores - usuarios la Declaración de Prácticas de Certificación y la presente Política de Certificados en los medios establecidos.

28) Cumplir con el resguardo de información conforme a lo establecido por las leyes y normas aplicables.

5.2 Obligaciones de la AR – Agentes Certificadores

1) Recopilar el consentimiento de la recolección y tratamiento de datos personales de los suscriptores – usuarios y solicitantes.

2) Cumplir con el resguardo de información conforme a lo establecido por las leyes y normas aplicables.

3) Aplicar controles de acceso a las instalaciones donde se realiza el proceso de verificación de identidad.

4) Recabar firmas de aceptación de los Términos y Condiciones de prestación del servicio de emisión de Certificados Digitales y del consentimiento para el tratamiento de datos personales de los solicitantes y suscriptores – usuarios.

5) Recolectar la documentación que será sometida al proceso de verificación de identidad de los suscriptores y solicitantes del servicio de emisión de Certificados Digitales.

6) Asegurar el cumplimiento de lo establecido en la presente Política de Certificados, en la Declaración de Prácticas de Certificación y en los procesos operativos y administrativos relacionados con el servicio de emisión de Certificados Digitales.

PÚBLICO

7) Diseñar y aplicar las medidas necesarias para evitar falsificación de información, suplantación de identidad y cualquier situación que se pueda presentar durante la prestación del servicio de emisión de Certificados Digitales

8) Publicar y poner a disposición de las partes interesadas, servicios de consulta y descarga de los certificados digitales que sean emitidos por la Autoridad Certificadora.

9) Garantizar en todo momento la Seguridad de la Información proporcionada por los solicitantes y suscriptores – usuarios, preservando su Confidencialidad, Integridad y Disponibilidad y dando cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

10) Informar por medio de correo electrónico a los suscriptores de los vencimientos próximos de sus certificados con al menos 30 días de anticipación.

11) Informar a los suscriptores - usuarios y demás partes interesadas, los medios para notificar cualquier evento que ponga en riesgo o comprometa los datos de creación de firma de los Certificados Digitales.

12) Informar a los suscriptores – usuarios los procedimientos para la renovación o revocación de un certificado digital, así como los medios y requisitos necesarios.

13) Aprobar o rechazar las solicitudes de emisión de certificados digitales, con base en los resultados de la verificación de identidad y demás aplicaciones de procesos correspondientes.

5.3 Responsabilidades de la AC

1) Responder por las irregularidades que puedan suscitarse durante la prestación del servicio de emisión de Certificados Digitales cuando sean imputables a la AC.

2) Atender de manera correcta y oportuna las solicitudes de revocación de certificados realizadas por los suscriptores – usuarios y autoridades competentes a través de la Autoridad Registradora.

3) Mantener actualizada la documentación dirigida a los suscriptores – usuarios que se encuentre publicada en los medios establecidos.

4) Dar solución a los incidentes reportados por los suscriptores – usuarios por cualquier falla en el servicio.

5) Detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.

6) Mantener la disponibilidad del servicio.

7) Responder por daños y perjuicios imputables a la AC por eventos debidamente comprobados.

5.4 Responsabilidades de la AR - Agentes Certificadores

1) Responder por las irregularidades que puedan suscitarse durante la prestación del servicio de Emisión de Certificados Digitales cuando sean imputables a la AR.

PÚBLICO

2) Para el manejo de datos personales, implementar y mantener procedimientos que privilegien la seguridad de la información teniendo como enfoque principal la confidencialidad de la información.

3) Verificar de manera inequívoca la identidad de los solicitantes y suscriptores – usuarios del servicio de emisión de Certificados Digitales.

4) Solicitar a la Autoridad Certificadora la revocación del Certificado Digital cuando se haya identificado que la información proporcionada por el suscriptor – usuario es falsa o apócrifa.

5.4.1 Limitaciones de responsabilidad

1) Incidentes relacionados con la falta de cumplimiento de las obligaciones de los solicitantes, suscriptores – usuarios y las partes que confían.

2) El mal uso del servicio de emisión de Certificados Digitales.

3) Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión de las prácticas de certificación a las que lleguen los solicitantes, suscriptores – usuarios y demás partes interesadas, del servicio de emisión de Certificados Digitales.

4) La entrega de datos y/o documentación errónea, falsa o apócrifa, así como la suplantación de identidad de terceros para la emisión Certificados Digitales.

5) Por la falta de disponibilidad de los servicios proporcionados causados por eventos de fuerza mayor, caso fortuito, desastres naturales o hechos de un tercero.

6) Por las fallas ocasionadas y presentadas en los equipos de procesamiento, acceso, telecomunicaciones y/o por falta de conocimiento, del solicitante, suscriptor - usuario, y demás partes interesadas.

7) Por la negligencia en el uso, manejo y confidencialidad del certificado digital por parte del suscriptor – usuario y demás partes interesadas.

8) Por ataques realizados al suscriptor - usuario, solicitante y demás partes interesadas, tipificados como delitos informáticos en el uso de los servicios de Emisión de Certificados Digitales.

9) Por falta de adopción de medidas de seguridad, políticas y demás mecanismos por parte del suscriptor - usuario para preservar la confidencialidad y el buen uso y manejo de los certificados digitales que le sean emitidos,

10) Por el uso distinto que se les dé a los certificados digitales conforme a lo establecido en la Declaración de Prácticas de Certificación y la presente Política de Certificados.

11) Por la falta de validación y verificación del estado de los certificados digitales durante su uso.

12) Por cualquier incumplimiento de las obligaciones que le correspondan al suscriptor - usuario, solicitante y demás partes interesadas en el uso del servicio y en la normativa aplicable.

PÚBLICO

13) Por el contenido de los mensajes o documentos firmados con los certificados digitales que le correspondan al suscriptor - usuario.

14) Por los daños y/o perjuicios de cualquier naturaleza como pueden ser:

- Pérdida de información de cualquier índole
- Suspensión de labores
- Pérdida de utilidades

*Solo en el caso que estos daños sean propiciados por el mal uso del servicio por parte de los suscriptores – usuarios.

15) Por cualquier evento que comprometa la llave privada o el certificado digital y que no sea notificado correcta y oportunamente a las autoridades Certificadora y Registradora de ATEB.

16) En caso de que los servicios de emisión de Certificados Digitales sean requeridos por un “representante”, este deberá demostrar la confiabilidad del o los suscriptores, mediante la legitimidad de la documentación que será sometida al proceso de verificación y autenticación.

17) Por no ejecutar correctamente el proceso de solicitud de revocación de certificados cuando así se requiera.

18) Por la no recuperación de documentos cifrados con la llave pública del suscriptor – usuario.

Con la aceptación de los Términos y Condiciones de uso del servicio de emisión de Certificados Digitales emitidos por ATEB, el suscriptor - usuario se obliga a indemnizar a ATEB como Autoridad Certificadora por cualquier acto u omisión que ocasione daños y perjuicios, causados por:

a) Incumplimiento de Términos y Condiciones, responsabilidades y obligaciones establecidos a las que se hace acreedor;

b) Falsedad en los datos y documentación proporcionados;

c) Omisión de hechos que afecten la naturaleza del certificado digital;

d) Incumplimiento en la protección, custodia y resguardo de las llaves privadas.

5.5 OBLIGACIONES DE LOS SOLICITANTES Y SUSCRIPTORES - USUARIOS

1) Cumplir con todos los requisitos y procedimientos requeridos para la prestación del servicio de emisión de Certificados Digitales acordes con la presente Política de Certificados y la Declaración de Prácticas.

2) Revisar el Certificado emitido y asegurarse de que toda la información contenida en este sea completa y correcta y corresponde a sus datos proporcionados.

3) Asegurar que, la información proporcionada al Agente Certificador durante el proceso de solicitud del Certificado Digital es verdadera y exacta.

PÚBLICO

4) Asegurar que, durante la solicitud del certificado digital, los datos de creación de firma del suscriptor – usuario, estaban bajo su exclusivo control.

5) Conocer y aceptar los Términos y Condiciones del servicio de emisión de Certificados Digitales.

6) Firmar la carta de aceptación de certificado digital

7) Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.

8) Utilizar el certificado digital conforme a los usos señalados en la Declaración de Prácticas y la presente Política de Certificados.

9) Contar con los medios y mecanismos seguros para realizar los trámites necesarios relacionados con el servicio de emisión de Certificados Digitales.

10) Respetar las disposiciones y las limitaciones de uso del certificado establecidos en la Declaración de Prácticas de Certificación y en la presente Política de Certificados publicadas por la Autoridad Certificadora.

5.6 RESPONSABILIDADES DE LOS SOLICITANTES Y SUSCRIPTORES - USUARIOS

1) Notificar a la Autoridad Certificadora o al Agente Certificador en caso de que el Certificado contenga alguna irregularidad.

2) El titular del certificado resguardará bajo su exclusivo control y responsabilidad los datos de creación de firma del certificado digital (llave privada y contraseña), los cuales son de su exclusivo conocimiento.

3) Crear, conservar y utilizar de forma correcta su par de claves o llaves de acuerdo con la normatividad vigente.

4) Implementar las medidas necesarias para evitar la pérdida, revelación, alteración o uso no autorizado, así como, proteger y almacenar su clave privada y su certificado digital.

5) Solicitar de manera oportuna al Agente Certificador la inmediata revocación de su Certificado Digital en caso de que se actualice alguna de las causales de revocación establecidas en los Términos y Condiciones, así como, en la Declaración de Prácticas de Certificación y en la presente Política de Certificados.

6) Administrar el almacenamiento de sus Certificados Digitales por medios propios o mediante la contratación de un tercero.

7) El titular del certificado deberá conocer las tarifas de la Autoridad Certificadora como Prestador de Servicios de Certificación y aceptar que le sean emitidos los cargos correspondientes a la prestación del servicio contratado.

PÚBLICO

8) Resguardar el nombre de usuario y la contraseña establecida por el usuario para su acceso a la plataforma de Emisión de Certificados Digitales.

9) Cumplir con lo dispuesto en los Términos y Condiciones y/o contrato y documentos adicionales del servicio de Emisión de Certificados Digitales.

10) Utilizar únicamente los medios establecidos por ATEB para la solicitud y gestión de los certificados digitales.

11) No usar la llave privada y el certificado digital una vez que se haya solicitado la revocación por cualquier causa justificada, así como no usar el certificado cuando éste no sea válido.

12) Informar a las partes que confían las medidas, precauciones y obligaciones que le son otorgados para confirmar la validez de los certificados digitales que emite la Autoridad Certificadora.

13) No usar el servicio de emisión de Certificados Digitales de manera que sea contrario a la Ley y las buenas prácticas o cualquier otra causa que afecte la buena reputación de ATEB.

14) Respetar los derechos de terceras personas y responsabilizarse frente a las mismas por los perjuicios que la utilización del Certificado Digital pueda causar, así como sacar en paz y a salvo a ATEB de cualquier acción legal relacionada con la utilización del certificado digital.

5.7 OBLIGACIONES DE LA PARTE QUE CONFÍA

1) Verificar el origen y la validez del Certificado Digital antes de realizar cualquier acción que lo involucre.

2) Asegurarse que el certificado digital proporcionado por el suscriptor – usuario sea idóneo para los fines que se pretende utilizar.

3) Validar que ATEB se encuentre acreditado como Autoridad Certificadora dentro del directorio vigente de la Secretaría de Economía en el siguiente sitio: https://psc.economia.gob.mx/directorio.html

4) Conocer y validar el alcance de los certificados digitales establecidos en la presente Política de Certificados y en la Declaración de Prácticas de Certificación, así como en la normatividad aplicable al contenido del Certificado Digital.

5) Reconocer y aceptar que los mensajes o documentos firmados con la llave privada del Certificado Digital del suscriptor – usuario tiene el mismo efecto y validez legal como si hubieran sido firmados de forma autógrafa.

6) Conocer, respetar y sujetarse a las garantías, disposiciones y los límites de responsabilidad establecidos en la presente Política de Certificados y en la Declaración de Prácticas de Certificación.

7) Validar y verificar la integridad de los documentos firmados con los Certificados Digitales en los que confía.

PÚBLICO

8) Implementar los mecanismos necesarios para acceder a los servicios de consulta y del estado de los Certificados Digitales que ATEB pone a su disposición, tales como CRL y OCSP.

9) Verificar y validar en todo momento el estado y vigencia de los Certificados Digitales en los que confía en los servicios de consulta y estado CRL y OCSP, así como el servicio de consulta y descarga, puestos a disposición por ATEB.

10) Notificar de manera inmediata cualquier evento, hecho o situación anómala relativa al Certificado Digital que pueda ser considerada como una causal de revocación de las establecidas en la presente Política de Certificados y en la Declaración de Prácticas de Certificación.

5.8 Responsabilidades de la parte que confía y del destinatario

1) Verificar la fiabilidad de la Firma Electrónica, o

2) Cuando la Firma Electrónica esté sustentada por un Certificado:

   a) Verificar, incluso en forma inmediata, la validez, suspensión del Certificado, y o revocación del Certificado.

   b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

6. Privacidad de datos

6.1 Protección de la Confidencialidad de la Información

6.1.1 Alcance de la Información Confidencial

La Información Confidencial se refiere a toda la información escrita, oral, sea tangible o intangible, gráfica o contenida en medios escritos, electrónicos o electromagnéticos, cintas, grabaciones, diskettes o, cualquier otra, que se encuentre identificada claramente por la parte que la proporciona como confidencial y/o que sea entregada a la otra parte con medidas de protección físicas o electrónicas que evidencien indubitablemente su carácter confidencial.

Por confidencialidad, se entiende, la garantía de que la información estará accesible únicamente al personal autorizado en función de sus actividades, cuidando su revelación no autorizada, debiendo mantener estricta confidencialidad en el manejo de la información identificada y proporcionada por la otra parte como Información Confidencial.

6.1.2 Información que no se considera Confidencial

La información que no se considera confidencialidad es aquella que se conozca derivada de cualquiera de los siguientes eventos:

i. Que haya sido de dominio público, o que sea publicada sin que medie ninguna acción y/o intervención de la parte que la recibe.

PÚBLICO

ii. Que la parte que la comparte la haga del dominio público.
iii. Que antes de ser revelada estuviera en posesión legítima de la parte que la recibe.
iv. Que posteriormente a la revelación de esta, sea legalmente recibida de un tercero que tenga derechos para distribuir la información sin notificación de ninguna restricción de su derecho a revelarla posteriormente.
v. Que sea desarrollada independientemente o adquirida por la parte que la recibe, a través de personas que no han tenido directa ni indirectamente acceso o conocimiento de tal Información Confidencial.
vi. Que se revele con la aprobación previa y escrita de la parte que la proporciona.
vii. Que la revelación y/o divulgación de la información se realice en desarrollo o por mandato de una Ley, Decreto o Sentencia u Orden Judicial, Orden Ministerial u Orden de cualquier autoridad competente en ejercicio de sus funciones legales.
viii. Que la parte que la recibe determine que la información recibida está presuntamente relacionada o vinculada a un acto o acción criminal, por lo que, dará conocimiento a las autoridades competentes.
ix. Que el período de confidencialidad de la información haya fenecido.

6.1.3 Responsabilidad de proteger la Información Confidencial

Con el fin de garantizar la protección de la información confidencial requerida que ATEB, a través de sus Autoridades Registradora y Certificadora intercambiará con los suscriptores y/o solicitantes para la prestación del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada, dentro de los Términos y Condiciones se señala una cláusula de confidencialidad y, en su caso, se elabora un Convenio de Confidencialidad, que tienen como finalidad, establecer el uso y la protección de la información que se entreguen mutuamente.

6.2 Protección de Datos Personales

ATEB mediante sus Autoridades Registradora y Certificadora que participan en el servicio de Emisión de Certificados Digitales debe garantizar a los solicitantes, suscriptores, usuarios y demás partes interesadas que antes, durante y después del proceso de Emisión de Certificados Digitales, se mantiene la confidencialidad de sus datos conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), en los artículos 102 y 104 del Código de Comercio y el artículo 5 del Reglamento del Código de Comercio, y se asegura, además, que los elementos humanos que intervienen en cualquier fase de los procedimientos se comprometan a resguardar la confidencialidad e integridad de la información manejada.

ATEB se compromete a poner a disposición de los solicitantes, suscriptores y demás partes interesadas, en su portal de internet, el Aviso de Privacidad y la Política de Protección de Datos Personales que cumple con los principios establecidos en la LFPDPPP, así como el procedimiento y las condiciones para poder ejercer sus derechos ARCO.

Con lo anterior, ATEB se asegura de tomar las medidas necesarias para proteger los datos personales de modificaciones no autorizadas, su destrucción o divulgación ya sea accidental o intencional y de la alta disponibilidad continua de los sistemas y datos de, y para, las partes interesadas, esto con base en la LFPDPPP.

En el caso de que alguna autoridad legal, administrativa o jurídica, solicitara a ATEB información que no le pertenece, ATEB notificará al titular correspondiente para que actúe a su consideración

PÚBLICO

tomando las acciones pertinentes y, ATEB como sujeto obligado, deberá proporcionar a las autoridades correspondientes únicamente la información solicitada.

ATEB, se compromete a garantizar en todo momento el cumplimiento de la Política de Seguridad de la Información, preservando así, bajo el Sistema de Gestión de Seguridad de la Información, la integridad, confidencialidad y disponibilidad de la información y hacer cumplir a todos los elementos humanos que intervengan en el proceso de Emisión de Certificados Digitales.

6.2.1 Estándares

1. ATEB se compromete como responsable del tratamiento de los datos personales a poner en práctica los principios que la Ley establece a estos, y el Profesional Jurídico será el responsable de dar seguimiento y respuesta a las solicitudes del ejercicio de derechos ARCO y corroborar el debido cumplimiento de los principios de: a) Licitud, b) Consentimiento, c) Información, d) Calidad, e) Finalidad, f) Lealtad, g) Proporcionalidad y h) Responsabilidad

2. Cuando los datos personales recabados dejen de ser necesarios para el cumplimiento de las finalidades previstas, se deben cancelar y posteriormente eliminar.

3. ATEB revisará periódicamente y actualizará los diferentes Avisos de Privacidad que mantenga con las diferentes partes interesadas, esto con motivo de cumplir con las actualizaciones legales competentes y fomentar la Protección de Datos Personales en todo momento.

4. En el momento en que ATEB se percate de que los Datos Personales de los que es responsable han sido vulnerados procederá a notificar a las partes afectadas el suceso, el riesgo y las acciones a tomar, para que decida qué medidas llevará a cabo.

5. ATEB como Autoridad Certificadora, que proporciona el servicio de Emisión de Certificados Digitales, así como su Autoridad Registradora y sus Agentes Certificadores, tienen implementados controles y mecanismos requeridos para proteger y hacer buen uso de la información y datos personales a los que tuvieran acceso, así como asegurar el apego a la LFPDPPP y otras legislaciones aplicables.

6. El acceso a los Datos Personales se delimita únicamente a los elementos humanos autorizados y capacitados de la Autoridad Certificadora, Autoridad Registradora y Agentes Certificadores, para resguardar y proteger en todo momento del proceso de Emisión de Certificados Digitales, los Datos Personales, siempre, basados en los principios de mínimo privilegio (least privilege) y en la necesidad de conocer (need to know).

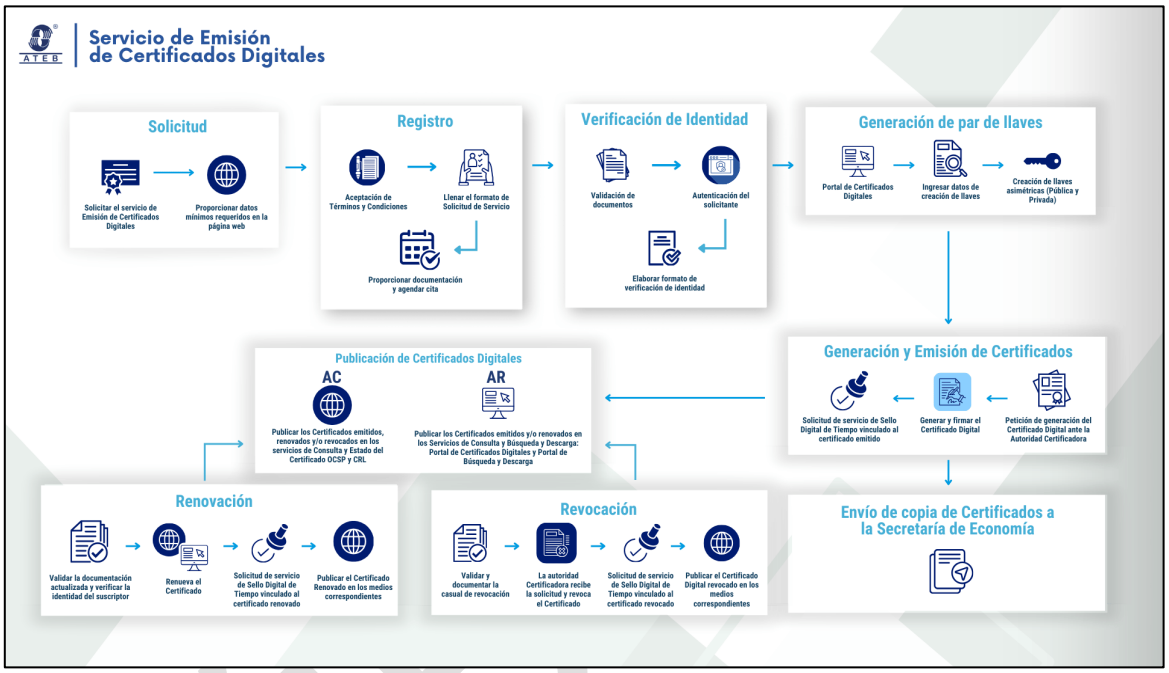
7. Los controles de acceso deben ser tanto físicos como lógicos y, deben establecer un acceso controlado, es decir, prohíben el acceso o intento de acceso a la información o a los elementos que no han sido autorizados para disponer de esa información.

8. Aquellos elementos humanos que incumplan con alguna de las Políticas de Seguridad de la Información o del presente documento serán responsables de los daños y perjuicios que pudieran ocasionar a cualquiera de las partes interesadas en el proceso de Emisión de Certificados Digitales, haciéndose también acreedores de las sanciones correspondientes derivadas de la gravedad de su incumplimiento.

PÚBLICO

9. Una vez otorgada la acreditación por parte de la Secretaría de Economía, el Prestador de Servicio de Certificación podrá iniciar las operaciones como Autoridad Certificadora y Autoridad Registradora en el servicio de Emisión de Certificados Digitales.

7. Procesos de operación que integran el Servicio de Emisión de Certificados Digitales de la Autoridad Certificadora



7.1 Tipos de Certificados Digitales que se entregarán

La Autoridad Certificadora ATEB, a través de su sistema emitirá y entregará los siguientes tipos de Certificados Digitales, que cumplen con los requerimientos dispuestos en las fracciones I a IV del artículo 97 del Código de Comercio:

Certificados Digitales de Firma Electrónica Avanzada o Fiable

Identidad Personal: Este tipo de Certificados Digitales son expedidos a personas físicas para garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

Representación: Este tipo de Certificados Digitales son expedidos a personas físicas con facultades legales para representar a una persona moral con el objeto de garantizar a terceros la autenticidad e integridad de sus mensajes de datos y dar validez jurídica a los actos que se realicen con ellos.

La vigencia de estos certificados es de dos años.

7.2 Personas que pueden solicitar el Servicio de Emisión de Certificados Digitales. Solicitud del Servicio de Emisión de Certificados Digitales

a) La solicitud de Emisión de Certificados Digitales puede ser realizada por cualquier Persona Física que actúe en nombre propio o en representación de un tercero que puede ser una Persona Moral, con la capacidad y facultad suficientes para obligarse por sí misma u obligar a terceros, bajo los Términos y Condiciones del servicio de Emisión de Certificados Digitales, así como, las obligaciones y responsabilidades que conlleva tanto, el poseer como, utilizar un certificado digital emitido por ATEB Autoridad Certificadora.

b) La solicitud se realiza a la Autoridad Registradora, puede hacerse tanto de forma directa en la Página Web https://www.ateb.mx/psc.html donde deberá proporcionar datos básicos y posteriormente llenar el formato correspondiente con la información que ahí solicita, como de forma presencial en la oficina administrativa de ATEB ubicada en Av. Insurgentes Norte No. 554, Piso 2, Col. Atlampa, Alcaldía Cuauhtémoc, C.P. 06450, Ciudad de México.

7.3 Registro y gestión de solicitudes de Certificados Digitales

1) En esta fase, la Autoridad Registradora o el Agente Certificador reciben las solicitudes del servicio de Emisión de Certificados Digitales realizadas por los solicitantes, dependiendo el medio por el cual se realicen estás solicitudes es como el responsable las atenderá.

2) En caso de realizar su solicitud a través de la oficina administrativa, llamada telefónica o WhatsApp, el Agente Certificador contactará al solicitante para darle a conocer los términos y condiciones del servicio de Emisión de Certificados Digitales, el Aviso de Privacidad y la Política de Datos Personales para su aceptación.

   En caso de hacer su solicitud a través de la página web, podrá aceptar los términos y condiciones a través de ese mismo medio.

3) El Agente Certificador proporciona el Formato de Solicitud del servicio de Emisión de Certificados Digitales al solicitante para su llenado.

4) Solicita la documentación de identificación al solicitante, siendo esta la siguiente:

   a) Comprobante de domicilio en formato electrónico
   b) Clave Única del Registro de Población (CURP) en formato electrónico
   c) El documento de identificación oficial con fotografía vigente expedido por autoridad competente en formato electrónico (PDF) (Credencial para votar); En caso de ser extranjeros algún documento que le identifique.
   d) Cédula de Identificación Fiscal actualizada en formato electrónico
   e) Acta de nacimiento o Carta de Naturalización en caso de ser extranjero en formato electrónico.
   f) Documento de migración que acredite la Residencia Temporal o Permanente en México, en formato electrónico en caso de ser extranjero.

PÚBLICO

Si la solicitud de Certificado Digital es para una Persona Moral, además el solicitante deberá presentar lo siguiente:

a) Cédula de Identificación Fiscal actualizada en formato electrónico de la Persona Moral
b) Carta de solicitud de emisión del Certificado Digital, en hoja membretada firmada por el Representante Legal de la persona moral.
c) Documento que acredite la Representación Legal del solicitante

Si la solicitud de Emisión del Certificado Digital es generada por un tercero autorizado a nombre y representación de una Persona Moral, además, se deberá proporcionar la siguiente información:

a) Registro Federal de Contribuyentes de la Persona Moral (Cédula de Identificación Fiscal actualizada no mayor a quince días en formato electrónico), para la cual solicita la Emisión del Certificado Digital.

b) Carta de solicitud de emisión del certificado digital, en hoja membretada firmada por el Representante Legal de la Persona Moral.

c) Documento que acredite la Representación Legal.

5) El Solicitante agenda una cita para la entrega de su documentación original a través de los medios establecidos.
6) El Agente Certificador otorga la cita al solicitante y este acude en la fecha y hora establecidos.

NOTA: Los datos recabados serán tratados con la finalidad señalada en el Aviso de Privacidad y la Política de Protección de Datos Personales aplicando los procedimientos correspondientes.

7.4 VERIFICACIÓN DE IDENTIDAD

Con base en la información proporcionada por el Solicitante, Suscriptor – Usuario, se lleva a cabo la verificación de identidad con el fin de determinar si se autoriza la emisión y/o renovación de Certificados Digitales o en su caso, se rechaza si no se puede autenticar de forma exitosa al solicitante.

Para el caso de renovación remota, se debe verificar de forma fehaciente la identidad del Suscriptor – Usuario, conforme al siguiente proceso:

No.	Actividad	Descripción	Responsable	Entrada	Salida
1	Revisar la información y documentación proporcionada	Revisa la información y documentación proporcionada por el solicitante, suscriptor - usuario 1. ¿Cuál es el motivo de revisión de la información proporcionada?	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor - usuario	Información y documentación proporcionada por el solicitante, suscriptor – usuario

PÚBLICO

		PRIMERA SOLICITUD: Continúa en la pregunta 2 RENOVACIÓN: Pasa a la actividad 2 2. ¿La información está completa y correcta? NO: Pasa a la actividad 3 SI: Pasa a la actividad 4			debidamente revisada
2	Solicitar la documentación actualizada al suscriptor - usuario	Solicita la documentación actualizada con respecto a la que proporcionó cuando se le emitió el certificado digital Regresa a la pregunta 2 de la actividad 1	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor – usuario debidamente revisada	Documentación actualizada solicitada
3	Notificar sobre la información faltante al solicitante, suscriptor – usuario y solicitar que le sea enviada	Notifica sobre la información faltante al solicitante, suscriptor - usuario y solicita que le sea enviada para su revisión Regresa a la pregunta 2 de la actividad 1	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor - usuario debidamente revisada	Notificación y solicitud de la información faltante
4	Validar la veracidad de la información y los documentos proporcionados	Valida la veracidad de la información y los documentos proporcionados por el solicitante, suscriptor - usuario en los servicios de consulta que las autoridades y entidades gubernamentales relevantes y competentes, ponen a disposición del público en general, de acuerdo con lo siguiente: 1.- Credencial para votar con fotografía en la Página Web: https://listanominal.ine.mx/scpln/ 2.- CURP en la Página Web: https://www.gob.mx/curp/ 3.- Registro Federal de Contribuyentes en la Página Web: https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor – usuario debidamente revisada	Validación de veracidad de la información y documentos proporcionados

PÚBLICO

5	Registrar los resultados de la validación realizada a la información y documentos proporcionados	Registra los resultados en el "Formato de Informe de Verificación de Identidad" (FOR-EDI-VDI-057) de la validación realizada a la información y documentos proporcionados. ¿La verificación de identidad es para ***renovación remota***? NO: Pasa a la actividad 6 SI: Pasa a la actividad 11	Agente Certificador	Validación de veracidad de la información y documentos proporcionados	Resultados de la validación realizada registrados
6	Recibir y atender al solicitante, suscriptor - usuario el día de su cita	Recibe y atiende al solicitante, suscriptor - usuario el día de su cita	Agente Certificador	Resultados de la validación realizada registrados	Recepción y atención al solicitante, suscriptor - usuario
7	Solicitar el Formato de solicitud del servicio de Emisión de Certificados Digitales firmado	Solicita el "Formato de Solicitud del Servicio de Emisión de Certificados Digitales" (FOR-EDI-SEC-058) firmado por el solicitante NOTA. En caso de ***renovación*** no se requiere el formato antes señalado debido a que lo proporcionó cuando se le emitió el certificado digital por primera vez	Agente Certificador	Recepción y atención al solicitante	Recepción del Formato de solicitud del servicio de Emisión de Certificados Digitales firmado
8	Solicitar los documentos originales al solicitante, suscriptor - usuario	Solicita los siguientes documentos originales al solicitante, suscriptor - usuario: 1.- Comprobante de domicilio 2.- Clave Única del Registro de Población (CURP) 3.- Documento de identificación oficial con fotografía vigente expedido por autoridad competente (credencial para votar) 4.- Cédula de Identificación Fiscal actualizada 5.- Acta de nacimiento o Carta de Naturalización en caso de ser extranjero. 6.- Documento de migración que acredite la Residencia Temporal o	Agente Certificador	Recepción del Formato de solicitud del servicio de Emisión de Certificados Digitales firmado	Documentos originales recibidos

PÚBLICO

		Permanente en México, en formato electrónico en caso de ser extranjero Cuando la solicitud del certificado es para una persona moral, también se deberá solicitar: 7.- Cédula de Identificación Fiscal actualizada de la Persona Moral 8.- Carta de solicitud de emisión del certificado digital, en hoja membretada firmada por el representante legal de la persona moral 9.- Documento que acredite la Representación Legal del firmante solicitante NOTA: En caso de **renovación** solo deberá entregar la información actualizada			
9	Cotejar los documentos originales del solicitante, suscriptor - usuario con los recibidos en formato electrónico	Coteja los documentos originales del solicitante, suscriptor - usuario con los recibidos en formato electrónico ¿Coincide la información con los documentos originales? SI: Pasa la actividad 10 NO: Pasa a la actividad 12 NOTA. Cuando no coincida la información se debe de registrar el hecho	Agente Certificador	Documentos originales recibidos	Documentos originales y documentos en formato electrónico cotejados
10	Realizar la autenticación y prueba de vida con la presencia del solicitante, suscriptor - usuario	Realiza la autenticación y prueba de vida con la presencia del solicitante, suscriptor - usuario en la Oficina Administrativa o en las instalaciones del cliente, validando que la persona sea la misma que la de la identificación oficial vigente proporcionada y sea quien dice ser. ¿La verificación de identidad fue exitosa? NO: Pasa a la actividad 12 SI: Pasa a la actividad 13	Agente Certificador	Documentos originales y documentos en formato electrónico cotejados	Autenticación y prueba de vida realizada

PÚBLICO

11	Solicitar el video y/o realizar una videollamada	Adicional a la revisión y validación de la información y documentación actualizada, en caso de ***renovación remota*** solicita un video al suscriptor mostrando su identificación oficial con fotografía vigente (credencial para votar) y/o realiza una videollamada para confirmar la autenticación y prueba de vida. En caso de extranjeros, se solicita documento oficial que acredite su estancia en el territorio nacional. ¿La verificación de identidad fue exitosa? NO: Pasa a la actividad 12 SI: Pasa a la actividad 13 NOTA: La **renovación remota** no se puede realizar por más de una ocasión	Agente Certificador	Solicitud de renovación remota	Autenticación y prueba de vida realizadas
12	Registrar el hecho y rechazar la solicitud	Registra el hecho en el "Formato de Informe de Verificación de Identidad" (FOR-EDI-VDI-057) y rechaza la solicitud NOTA.- En caso de no aprobarse la solicitud se debe informar al solicitante los motivos del rechazo. FIN DEL PROCEDIMIENTO	Agente Certificador	Documentos originales y documentos en formato electrónico inválidos y/o prueba de vida no exitosa	Rechazo de la solicitud y registro de hechos
13	Registrar el hecho y autorizar la solicitud de Emisión o Renovación del Certificado Digital	Registra el hecho en el "Formato de Informe de Verificación de Identidad" (FOR-EDI-VDI-057) y autoriza la solicitud de Emisión o Renovación del Certificado Digital	Agente Certificador	Verificación de identidad exitosa	Solicitud de emisión o renovación de certificado digital autorizada
FIN DEL PROCEDIMIENTO					

PÚBLICO

7.4.1 Objetivos, alcances y limitaciones de uso de los Certificados Digitales

ATEB, en su calidad de Autoridad Certificadora, tiene la responsabilidad de informar a los suscriptores que, como parte del proceso de renovación de los Certificados Digitales, deberán conocer y aceptar los objetivos, alcances y limitaciones del uso de los Certificados Digitales emitidos, de acuerdo con la información siguiente:

Objetivos del Certificado Digital:

- **Acreditación de identidad.** Sirve para la identificación y demostración de una persona o un ente, confirmando que es quien dice ser, mediante la utilización del certificado digital como un medio de seguridad.

- **Cifrado de información.** Transforma datos legibles a un formato codificado e ilegible para aquellos a quienes no está dirigida la información.

- **Cifrado de llaves.** Protege la información utilizando dos llaves diferentes, una pública y una privada, donde una de ellas se usa para cifrar y la otra para descifrar, asegurando con ello la confidencialidad y autenticidad de los datos en comunicaciones seguras.

Los Certificados Digitales, emitidos por ATEB Autoridad Certificadora, tienen los siguientes alcances y se limitan a los siguientes usos:

- **Firma Digital:** Firmar documentos electrónicos reemplazando la firma autógrafa, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

- **Sin repudio:** Garantiza que el firmante no puede negar haber realizado una acción o enviado un mensaje, debido a que, el certificado digital, vincula inequívocamente el mensaje al mismo, quien utiliza una clave privada única.

- **Cifrado de datos:** Convertir información legible (texto plano) en un código ilegible (texto cifrado).

- **Acuerdo de clave:** Protocolo criptográfico donde dos o más partes establecen de forma segura una clave secreta compartida, utilizada para cifrar y descifrar comunicaciones.

Con lo anterior, se da certeza jurídica y se aporta mayor nivel de seguridad y blindaje normativo a los documentos firmados.

Para consulta permanente, la información correspondiente a los usos del certificado se encuentra en la presente Política de Certificados, la cual se encuentra publicada en el sitio web de ATEB https://www.ateb.mx/psc.html.

Limitaciones del uso de Certificado Digital:

- El certificado digital emitido por ATEB es de uso estrictamente personal e intransferible, no podrá ser compartido ni utilizarse para suplantar identidades, representar a terceros sin autorización legal ni generar firmas o autenticaciones en nombre de personas o entidades distintas del usuario.

- ATEB no será responsable por daños derivados del uso de Certificados vencidos, no renovados oportunamente o utilizados de manera indebida por el “Titular” o terceros.

PÚBLICO

- El uso del certificado emitido podrá estar limitado por la compatibilidad técnica de plataformas, sistemas o aplicaciones. ATEB Autoridad Certificadora no garantiza su funcionamiento fuera de los entornos tecnológicos que cumplan los estándares establecidos.

- El suscriptor no podrá modificar, alterar, duplicar o intentar intervenir en la estructura técnica del certificado ni en los dispositivos criptográficos asociados.

- El certificado digital deberá emplearse exclusivamente para los fines previstos en la Política de Certificados y Declaración de Prácticas de Certificación de ATEB Autoridad Certificadora.

- Cualquier uso distinto o no contemplado se considera no autorizado.

- El certificado digital emitido por ATEB no podrá utilizarse si existe sospecha de compromiso, robo, pérdida o acceso no autorizado a la clave privada asociada.

- El certificado solo será válido durante el período de vigencia establecido por ATEB. Cumplido dicho plazo, caducará automáticamente, quedando prohibido su uso posterior.

- El uso del certificado digital emitido por ATEB estará limitado por la adecuada custodia del certificado digital raíz almacenado en el dispositivo HSM; el certificado puede quedar comprometido si el dispositivo en el que está almacenado se pierde, es robado o es víctima de un ataque de malware.

7.4.2 Obligaciones y responsabilidades de la Autoridad Registradora – Agentes Certificadores

Obligaciones de la AR – Agentes Certificadores

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

1) Recopilar el consentimiento de la recolección y tratamiento de datos personales de los suscriptores – usuarios y solicitantes.

2) Cumplir con el resguardo de información conforme a lo establecido por las leyes y normas aplicables.

3) Aplicar controles de acceso a las instalaciones donde se realiza el proceso de verificación de identidad.

4) Recabar firmas de aceptación de los Términos y Condiciones de prestación del servicio de Emisión de Certificados Digitales y del consentimiento para el tratamiento de datos personales de los solicitantes y suscriptores – usuarios.

5) Recolectar la documentación que será sometida al proceso de verificación de identidad de los suscriptores y solicitantes del servicio de Emisión de Certificados Digitales.

PÚBLICO

6) Asegurar el cumplimiento de lo establecido en la Política de Certificados, en la Declaración de Prácticas de Certificación y en los procesos operativos y administrativos relacionados con el servicio de Emisión de Certificados Digitales.

7) Diseñar y aplicar las medidas necesarias para evitar falsificación de información, suplantación de identidad y cualquier situación que se pueda presentar durante la prestación del servicio de Emisión de Certificados Digitales

8) Publicar y poner a disposición de las partes interesadas, servicios de consulta y descarga de los certificados digitales que sean emitidos por la Autoridad Certificadora.

9) Garantizar en todo momento la Seguridad de la Información proporcionada por los solicitantes y suscriptores – usuarios, preservando su Confidencialidad, Integridad y Disponibilidad y dando cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

10) Informar por medio de correo electrónico a los suscriptores de los vencimientos próximos de sus certificados con al menos 30 días de anticipación.

11) Informar a los suscriptores - usuarios y demás partes interesadas, los medios para notificar cualquier evento que ponga en riesgo o comprometa los datos de creación de firma de los Certificados Digitales.

12) Informar a los suscriptores – usuarios los procedimientos para la renovación o revocación de un certificado digital, así como los medios y requisitos necesarios.

13) Informar de inmediato a los suscriptores cuando sus certificados hayan sido revocados por alguna causal de revocación.

14) Aprobar o rechazar las solicitudes de emisión de certificados digitales, con base en los resultados de la verificación de identidad y demás aplicaciones de procesos correspondientes.

Responsabilidades de la AR – Agentes Certificadores

1) Responder por las irregularidades que puedan suscitarse durante la prestación del servicio de Emisión de Certificados Digitales cuando sean imputables a la AR.

2) Para el manejo de datos personales, implementar y mantener procedimientos que privilegien la seguridad de la información teniendo como enfoque principal la confidencialidad de la información.

3) Verificar de manera inequívoca la identidad de los solicitantes y suscriptores – usuarios del servicio de Emisión de Certificados Digitales.

4) Solicitar a la Autoridad Certificadora la revocación del Certificado Digital cuando se haya identificado que la información proporcionada por el suscriptor – usuario es falsa o apócrifa.

PÚBLICO

7.4.3 Obligaciones y responsabilidades de la Autoridad Certificadora

Obligaciones de la AC

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

1) Asegurar que la Declaración de Prácticas de Certificación se cumpla y esté acorde a la Política de Seguridad de la Información, con la presente Política de Certificados y los Procedimientos Operacionales de las Autoridades Certificadora y Registradora.

2) Asegurar el cumplimiento de los Términos y Condiciones, así como, con lo establecido en la presente Política de Certificados, en la Declaración de Prácticas de Certificación y en los procesos operativos y administrativos relacionados con el servicio de Emisión de Certificados Digitales.

3) Aplicar los controles de acceso a las instalaciones donde se ejecutan los procesos del servicio de Emisión de Certificados Digitales.

4) Garantizar en todo momento la Seguridad de la Información proporcionada por las partes interesadas, preservando su Confidencialidad, Integridad y Disponibilidad y dando cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

5) Informar al suscriptor - usuario los requisitos que debe cumplir relacionados con la prestación del servicio de Emisión de Certificados Digitales.

6) Informar al suscriptor - usuario los términos y condiciones en que se prestarán los Servicios de Emisión de Certificados Digitales.

7) Contar con un control de accesos que apoye a validar la identidad de los usuarios que utilizan los servicios y los sistemas, con la finalidad de salvaguardar la integridad de la información suministrada.

8) Contar con los elementos humanos, tecnológicos, materiales y económicos necesarios para brindar el servicio de Emisión de Certificados Digitales.

9) Brindar Soporte Técnico para entregar solución a los inconvenientes presentados durante la prestación del servicio de Emisión de Certificados Digitales.

10) Realizar y permitir auditorías para verificación del cumplimiento correcto y completo del servicio acreditado.

11) Realizar respaldos incrementales de manera diaria y completos de manera semanal.

12) Contar con un plan para la respuesta y recuperación de la operación ante desastres y de continuidad de negocio que garantice que las operaciones no se interrumpan.

PÚBLICO

13) Utilizar elementos y dispositivos de seguridad para garantizar un entorno seguro para la información del suscriptor - usuario y demás partes interesadas.

14) Garantizar la autenticidad e integridad de los certificados emitidos en el transcurso del tiempo.

15) Salvaguardar la llave privada del Certificado que utilizará la AC para la Emisión de Certificados Digitales.

16) No copiar ni almacenar las llaves privadas de los certificados emitidos a los suscriptores – usuarios.

17) Emitir los certificados de las solicitudes autorizadas por la Autoridad Registradora con base en la legislación aplicable y de acuerdo con lo contratado por los suscriptores - usuarios.

18) Garantizar que todos los certificados emitidos y/o revocados cuenten con un Sello Digital de Tiempo.

19) Almacenar de forma segura los certificados y administrar de forma efectiva los directorios, actualizando oportunamente el estado de los certificados.

20) Publicar y poner a disposición de las partes interesadas, servicios de consulta, descarga y estado de los certificados CRL y OCSP con alta disponibilidad.

21) Asegurar el almacenamiento y actualización de las CRL y estados de los certificados OCSP.

22) Enviar en línea una copia de cada certificado digital emitido a la Secretaría de Economía.

23) Informar a la Secretaría de Economía sobre cualquier incidente que pueda comprometer la prestación de los servicios de Emisión de Certificados Digitales.

24) Poner a disposición de las partes interesadas en los medios establecidos, los procedimientos para la renovación o revocación de un certificado digital, así como los requisitos necesarios.

25) Entregar de forma segura los archivos correspondientes de los Certificados Digitales emitidos.

26) Poner a disposición de los suscriptores - usuarios la Declaración de Prácticas de Certificación y la presente Política de Certificados en los medios establecidos.

27) Cumplir con el resguardo de información conforme a lo establecido por las leyes y normas aplicables.

Responsabilidades de la AC

1) Responder por las irregularidades que puedan suscitarse durante la prestación del servicio de Emisión de Certificados Digitales cuando sean imputables a la AC.

2) Atender de manera correcta y oportuna las solicitudes de revocación de certificados realizadas por los suscriptores – usuarios y autoridades competentes a través de la Autoridad Registradora.

3) Mantener actualizada la documentación dirigida a los suscriptores – usuarios que se encuentre publicada en los medios establecidos.

PÚBLICO

4) Dar solución a los incidentes reportados por los suscriptores – usuarios por cualquier falla en el servicio.

5) Detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.

6) Mantener la disponibilidad del servicio.

7) Responder por daños y perjuicios imputables a la AC por eventos debidamente comprobados.

7.4.4 Limitaciones de responsabilidad

1) Incidentes relacionados con la falta de cumplimiento de las obligaciones de los solicitantes, suscriptores – usuarios y las partes que confían.

2) El mal uso del servicio de Emisión de Certificados Digitales.

3) Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión de las prácticas de certificación a las que lleguen los solicitantes, suscriptores – usuarios y demás partes interesadas, del servicio de Emisión de Certificados Digitales.

4) La entrega de datos y/o documentación errónea, falsa o apócrifa, así como la suplantación de identidad de terceros para la Emisión Certificados Digitales.

5) Por la falta de disponibilidad de los servicios proporcionados causados por eventos de fuerza mayor, caso fortuito, desastres naturales o hechos de un tercero.

6) Por las fallas ocasionadas y presentadas en los equipos de procesamiento, acceso, telecomunicaciones y/o por falta de conocimiento, del solicitante, suscriptor - usuario, y demás partes interesadas.

7) Por la negligencia en el uso, manejo y confidencialidad del certificado digital por parte del suscriptor – usuario y demás partes interesadas.

8) Por ataques realizados al suscriptor - usuario, solicitante y demás partes interesadas, tipificados como delitos informáticos en el uso de los servicios de Emisión de Certificados Digitales.

9) Por falta de adopción de medidas de seguridad, políticas y demás mecanismos por parte del suscriptor - usuario para preservar la confidencialidad y el buen uso y manejo de los certificados digitales que le sean emitidos.

10) Por el uso distinto que se les dé a los certificados digitales conforme a lo establecido en la Declaración de Prácticas de Certificación y la presente Política de Certificados.

11) Por la falta de validación y verificación del estado de los certificados digitales durante su uso.

12) Por cualquier incumplimiento de las obligaciones que le correspondan al suscriptor - usuario, solicitante y demás partes interesadas en el uso del servicio y en la normativa aplicable.

PÚBLICO

13) Por el contenido de los mensajes o documentos firmados con los certificados digitales que le correspondan al suscriptor - usuario.

14) Por los daños y/o perjuicios de cualquier naturaleza como pueden ser:

- Pérdida de información de cualquier índole
- Suspensión de labores
- Pérdida de utilidades

*Solo en el caso que estos daños sean propiciados por el mal uso del servicio por parte de los suscriptores – usuarios.

15) Por cualquier evento que comprometa la llave privada o el certificado digital y que no sea notificado correcta y oportunamente a las Autoridades Certificadora y Registradora de ATEB.

16) En caso de que los servicios de Emisión de Certificados Digitales sean requeridos por un "representante", este deberá demostrar la confiabilidad del o los suscriptores, mediante la legitimidad de la documentación que será sometida al proceso de verificación y autenticación.

17) Por no ejecutar correctamente el proceso de solicitud de revocación de certificados cuando así se requiera.

18) Por la no recuperación de documentos cifrados con la llave pública del suscriptor – usuario.

7.5 Generación de Certificados Digitales y controles para la generación de datos de creación de firma electrónica del usuario

Una vez verificada la identidad y autorizada la solicitud, se envía al Suscriptor la información de credenciales de acceso al portal de gestión donde proporciona la información solicitada y se procede a la generación y emisión del Certificado Digital solicitado, el cual podrá ser utilizado para los fines señalados en el apartado **4.1 Importancia y uso de los certificados digitales** mismo que será publicado y se podrá descargar de los medios de consulta y descarga señalados en el apartado **7.6 Publicación de Certificados Digitales.**

Nota: Es importante considerar que la clave privada sólo se puede descargar una sola vez y es responsabilidad exclusiva del Suscriptor - Usuario, debido a que, nunca es conocida ni resguardada por las Autoridades Certificadora y Registradora ni por el Agente Certificador.

Asimismo, el acceso al portal se encuentra protegido mediante un esquema de autenticación basado en usuario y contraseña, complementado con un mecanismo de doble factor de autenticación (2FA), lo que fortalece significativamente el control de acceso.

7.6 Publicación de Certificados Digitales

La publicación de Certificados Digitales emitido y/o renovados se realiza mediante la puesta a disposición en las siguiente URL's:

1.- Portal de Certificados Digitales https://psc.ateb.com.mx:7010

PÚBLICO

2.- Portal de búsqueda y descarga https://psc.ateb.com.mx:7011
3.- OCSP https://psc.ateb.com.mx:7013/psc/ocsp/response

Por otro lado, los certificados digitales que hayan sido revocados se publican en las siguientes URL's:

1.- CRL Lista: https://psc.ateb.com.mx:7012/psc/crl/list
2.- CRL Delta: https://psc.ateb.com.mx:7012/psc/crl/delta
3.- OCSP: https://psc.ateb.com.mx:7013/psc/ocsp/response

7.7 SOLICITUD DE SELLO DE TIEMPO

Todos los Certificados Digitales cuentan con un sello de tiempo para registrar la marca de fecha y hora del momento en que han sido emitidos y/o renovados o revocados.

7.8 REVOCACIÓN DE CERTIFICADOS DIGITALES

Los Certificados Digitales podrán ser revocados si se presenta alguna de las siguientes causales:

- Cuando el período de vigencia haya concluido;
- Cuando se compruebe con posterioridad que, los documentos que presentó el suscriptor del certificado digital para acreditar su identidad son falsos;
- Cuando así lo solicite el suscriptor del certificado digital a la Autoridad Certificadora que lo emitió a través de la Autoridad Registradora;
- Cuando el suscriptor, el Agente Certificador de la Autoridad Registradora o la Autoridad Certificadora han incumplido una obligación, declaración o responsabilidad establecida en los Términos y Condiciones del servicio.
- Por uso prohibido del certificado;
- Por fallecimiento o incapacidad inesperada del suscriptor;
- Cuando se extravíe o se inutilice por daños en el medio electrónico que contenga el certificado digital;
- Cuando se presenten cambios en la información o datos originales utilizados al momento de la emisión del certificado digital, en cuyo caso, tales cambios deben ser notificados por el suscriptor;
- Cuando el suscriptor sea una Persona Moral y sea sujeta de proceso de liquidación;
- Cuando el titular del certificado digital informe que la llave privada del certificado ha sido comprometida por cualquier causa o motivo;
- Cuando el certificado haya sido emitido sin cumplir con los requisitos y los procedimientos operacionales requeridos y señalados en la presente Política de Certificados y la Declaración de Prácticas de Certificación;
- Cuando el suscriptor confirme que alguna información del contenido en el certificado digital no es correcta;
- Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación de la firma del certificado digital, y
- Por resolución de autoridad judicial o administrativa que así lo determine.

Las personas que pueden solicitar la revocación de certificados digitales son:

- El Agente Certificador cuando tenga conocimiento de que existe una causal debidamente comprobada que de origen a la revocación.

PÚBLICO

- El suscriptor del certificado digital, de acuerdo con las causales señaladas anteriormente y consideradas en la presente Política de Certificados y la Declaración de Prácticas de Certificación.
- Autoridades Competentes en el momento en que tengan conocimiento y evidencia de que existe una causal de revocación.
- En el caso que refiere la causal por fallecimiento del suscriptor, la revocación se realizará previa solicitud de un tercero legalmente autorizado, quien deberá acompañar el acta de defunción del titular del certificado digital y el documento que acredita su autorización y facultad para solicitar dicha revocación.

Medios para solicitar la revocación de Certificados Digitales:

a) Los medios a través de los cuales se pueden solicitar revocaciones de certificados digitales emitidos por ATEB Autoridad Certificadora, son los siguientes:

- Portal de Certificados Digitales https://psc.ateb.com.mx:7010
- Correo electrónico certificados.psc@ateb.mx
- De forma presencial directamente en la Oficina Administrativa de ATEB ubicadas en: Av. Insurgentes Norte No. 554, Piso 2, Col. Atlampa, Alcaldía Cuauhtémoc, C.P. 06450, Ciudad de México.

Proceso de Revocación de Certificados Digitales

1) Realizar la solicitud de revocación del Certificado Digital por cualquiera de los medios señalados.
   Nota: En caso de no hacerlo a través del portal se realiza la autenticación del solicitante y la causal de revocación.

2) Se revoca el Certificado Digital.

3) Se publica en los medios establecidos en el apartado **9.6 Publicación de Certificados Digitales**.

7.9 RENOVACIÓN DE CERTIFICADOS DIGITALES

Consideraciones que debe tomar en cuenta el Suscriptor – Usuario para la solicitud de renovación de su Certificado Digital:

1.- Para solicitar la renovación de Certificado Digital, este debe estar vigente y para el caso de renovación remota, además podrá realizar la solicitud de su Certificado Digital con su certificado vigente y su contraseña.

2.- Tipos de renovación que se pueden solicitar: Presencial o remota.

3.- La renovación de manera remota no se puede realizar más de una vez.

4.- Se debe actualizar la información y documentación del Suscriptor – Usuario.

5.- En caso de realizarse la renovación remota, como parte de la verificación fehaciente de identidad del usuario, se realiza una prueba de vida.

PÚBLICO

Proceso de Renovación de Certificados Digitales

1) El Suscriptor – Usuario solicita la renovación de su Certificado Digital.
2) Se valida la vigencia del Certificado Digital.
3) Se verifica la identidad del Suscriptor – Usuario y en su caso se realiza la prueba de vida.
4) Se autoriza la renovación del Certificado Digital.
5) Se renueva el Certificado Digital.
6) Se publica en los medios establecidos en el apartado **9.6 Publicación de Certificados Digitales**.

8. Interoperabilidad

ATEB Autoridad Certificadora, dentro de la presente Política de Certificados asegura que se permita tener interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría de Economía con el fin de facilitar a todas las partes involucradas el cumplimiento regulatorio al que están sujetas, así como, no interferir en el desarrollo de las operaciones en la Emisión de Certificados Digitales.

En razón de lo anterior, la autoridad Certificadora de ATEB considera lo siguiente para permitir la interoperabilidad de los Certificados Digitales que emite:

- La estructura de los Certificados Digitales es compatible con el RFC 5280 *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* actualizado con el RFC 6818.
- La Lista de revocación de Certificados (CRL) es compatible con el RFC 5280 *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* actualizado con el RFC 6818.
- El Protocolo de Estado de Certificados en Línea (OCSP) donde se puede consultar en línea el estado del Certificado Digital, es compatible con el RFC 6960 *"X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"*.

9. Publicación de la Política de Certificados

ATEB Servicios, S.A. de C.V., como Autoridad Certificadora tiene un sitio de internet en el cual difunde la versión pública de la presente Política de Certificados del servicio de Emisión de Certificados Digitales, dicha información podrá ser periódicamente actualizada conforme a lo establecido en el calendario de revisión establecido en este documento.

Dicho sitio de internet será público y es el único espacio aprobado por ATEB Servicios, S.A. de C.V., como fuente de información confiable sobre la prestación del servicio de emisión de Certificados Digitales y cuyo acceso se realizará a través de las siguientes URL's: https://www.ateb.mx/psc.html y https://psc.ateb.com.mx:7011

PÚBLICO

9.1 IDENTIFICADOR DE OBJETO

Este identificador de objeto será proporcionado por la Secretaría de Economía una vez que se obtenga la acreditación para el servicio de Emisión de Certificados Digitales.

10. Auditoría de cumplimiento

ATEB contempla realizar las auditorías correspondientes al servicio de Emisión de Certificados Digitales de forma anual con el objetivo de asegurar que, todas las áreas involucradas en la revisión de los eventos registrados para la generación de reportes cumplan con los procesos establecidos referentes a la documentación y con todos los requisitos necesarios para operar el servicio, así como también para mantener su compromiso de mejora continua.

Es importante mencionar que, adicional a las auditorías internas realizadas por ATEB, la Secretaría de Economía tendrá la facultad de realizar visitas de verificación previamente notificadas conforme a lo dispuesto en la Ley Federal de Procedimiento Administrativo.

ATEB se compromete como responsable del tratamiento de los datos personales a poner en práctica los principios que la Ley establece a estos, y el Profesional Jurídico será el responsable de dar seguimiento y respuesta a las solicitudes del ejercicio de derechos ARCO y corroborar el debido cumplimiento de los principios de: a) Licitud, b) Consentimiento, c) Información, d) Calidad, e) Finalidad, f) Lealtad, g) Proporcionalidad y h) Responsabilidad.

11. Otros asuntos comerciales y legales

11.1 TARIFAS

Los solicitantes del servicio de Emisión de Certificados Digitales serán informados oportunamente de las tarifas establecidas para este servicio al momento de darles a conocer los Términos y Condiciones.

Adicionalmente al costo por la Emisión de Certificados Digitales, la Autoridad Certificadora podrá establecer algún costo por servicios extraordinarios a los señalados en esta Política de Certificados y la Declaración de Prácticas de Certificación.

11.2 REEMBOLSOS

Los reembolsos o devoluciones de alguna cantidad pagada por los servicios de Emisión de Certificados Digitales aplicarán solamente en los casos señalados en la Declaración de Prácticas de Certificación.

En caso de algún error cometido por parte del solicitante y/o suscriptor en la solicitud de los servicios de Emisión de Certificados Digitales y si se hubieran realizado actividades del proceso de emisión, así como o en casos de incumplimiento por parte éstos, no existirá ningún tipo de reembolso.

No existirá ningún reembolso o devolución cuando se haya emitido el certificado y sea aceptado por parte del suscriptor, tampoco existirán devoluciones parciales si el certificado ha sido utilizado y se quiera dejar de utilizarse antes de finalizar su vigencia.

PÚBLICO

11.3 Seguros de Responsabilidad

ATEB Autoridad Certificadora contará con un seguro de responsabilidad civil y fianzas requeridas en términos de lo señalado en el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación y las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación para cada año y durante el tiempo que permanezca acreditado como prestador de Servicios de Certificación, con el fin de pagar la indemnización que se deba a un tercero a consecuencia de un hecho que cause un daño.

Lo anterior, resultará aplicable cuando el hecho sea debidamente imputable y comprobado a la Autoridad Certificadora, por lo que, si éstos fueran consecuencia de casos fortuitos o de fuerza mayor, o por cualquier circunstancia que esté fuera del control de ATEB Autoridad Certificadora o por alguna limitación de responsabilidad, ésta no será responsable de algún daño o perjuicio.

11.4 Propiedad Intelectual

Toda la infraestructura tecnológica y la información que integran el servicio de Emisión de Certificados Digitales son propiedad exclusiva de ATEB Autoridad Certificadora, quien permitirá al suscriptor y demás partes interesadas hacer uso de los mismos, por lo que, bajo ninguna circunstancia, se puede considerar que, se otorga derecho alguno de exclusividad o licencia exclusiva a su favor, debido a que, pertenecen a ATEB quien dispone de los derechos de propiedad intelectual sobre éstos y los cuales, están protegidos por las leyes nacionales e internacionales en materia de derechos de propiedad intelectual.

Entendiéndose por “Propiedad Intelectual” todo lo que la normativa aplicable considere.

11.5 Suspensión o cese de funciones de la AC

ATEB Autoridad Certificadora cuenta con los procedimientos de actuación en casos de suspensión temporal o definitiva así como para el caso de cese de funciones, los cuales, contemplan las medidas necesarias para asegurar la disponibilidad de los servicios de consulta y estado de los certificados, así como aplicar lo establecido por la autoridad regulatoria con el fin de proteger en todo momento la seguridad de la información de los suscriptores – usuarios informándoles en todo momento las acciones correspondientes que realice y cumpliendo con sus obligaciones y responsabilidades.

Estos procedimientos de actuación se dan a conocer en la Declaración de Prácticas de Certificación la cual se puede consultar en las siguientes URL: https://www.ateb.mx/psc.html y https://psc.ateb.com.mx:7011

11.6 Términos y Condiciones del servicio de Emisión de Certificados Digitales

En el momento de solicitar información acerca del servicio de Emisión de Certificados Digitales a través de los medios establecidos, se dan a conocer al Solicitante los Términos y Condiciones que regulan el servicio de Emisión de Certificados Digitales de ATEB.

El documento de Términos y Condiciones, así como, el Aviso de Privacidad se pueden consultar en sitio web de la Autoridad Certificadora ATEB https://www.ateb.mx/psc.html.

PÚBLICO