

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

PÚBLICO



Declaración de Prácticas del servicio de Emisión de Certificados Digitales

ATEB - BPM

Dirección General

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

Identificador de objeto: 2.16.484.101.10.316.100.9.1.1.1.2

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 1 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

Contenido

1. Información inicial	6
1.1 Información del documento	6
1.2 Registro de cambios y calendario de revisión	6
1.3 Responsables de revisión y autorización	7
1.4 Clasificación de la información del documento	7
2. Introducción	8
2.1 Antecedentes	8
2.2 Objetivo	8
2.3 Alcance	8
2.4 Datos de Contacto	9
2.5 Responsables de la administración de la declaración de prácticas de certificación	9
2.6 Publicación de la Declaración de Prácticas de Certificación	9
2.6.1 Identificador de objeto	10
2.7. Términos y Condiciones del servicio de Emisión de Certificados Digitales	10
2.8 Referencias normativas	10
2.9 Definiciones	10
3. Partes interesadas y Participantes de la PKI	13
3.1 Autoridad Certificadora	13
3.2 Agente Certificador	13
3.3 Autoridad Registradora	13
3.4 Suscriptor	14
3.5 Solicitante	14
3.6 Parte que confía	14
3.7 Secretaría de Economía	14
4. Obligaciones y responsabilidades del servicio de Emisión de Certificados Digitales (ECD)	14
4.1 Obligaciones de la AC	14
4.2 Obligaciones de la AR – Agentes Certificadores	16
4.3 Responsabilidades de la AC	17

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 2 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

4.4 Responsabilidades de la AR.....	17
4.5 Obligaciones de los solicitantes y suscriptores - usuarios	19
4.6 Responsabilidades de los solicitantes y suscriptores - usuarios.....	20
4.7 Obligaciones de la parte que confía	21
4.8 Responsabilidades de la parte que confía y del destinatario	22
5. Matriz RACI.....	22
6. Tipos de Certificados a emitir por la Autoridad Certificadora	23
6.1 Importancia y uso de los certificados digitales	23
6.2 Procesos de operación que integran el Servicio de Emisión de Certificados Digitales de la Autoridad Certificadora	24
6.3 Procesos Operativos del Ciclo de Vida del Certificado	24
6.4 Controles de gestión, operativos y físicos	25
6.4.1 Seguridad física	25
6.4.2 Seguridad del personal	26
6.4.3 Registros de auditoría	27
6.4.4 Compromiso y recuperación ante desastres	28
6.5 Controles técnicos de seguridad	28
6.5.1 Módulo criptográfico.....	28
6.5.2 Generación de par de claves de la AC	28
6.5.3 Generación de par de claves de los certificados digitales emitidos por la AC	29
6.6 Perfiles de Certificados, CRL y OCSP	29
6.6.1 Estructura de Certificados.....	29
6.6.2 Estructura de la CRL.....	29
6.6.3 Estructura del OCSP.....	30
6.7 Alcance y usos de los certificados emitidos	30
6.8 Aceptación de los certificados	31
7. Procesos de auditoría y respaldo	31
7.1 Proceso de Auditoría	31
7.1.1 Tipos de eventos registrados	32
7.1.2 Registro de frecuencia	32

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 3 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

7.1.3	Período de conservación del registro de auditoría	33
7.1.4	Protección del registro de auditoría	33
7.1.5	Procedimientos de copia de seguridad respaldo de los registros de auditoría	33
7.1.6	Sistema de recopilación de auditorías	33
7.1.7	Evaluaciones de vulnerabilidad Análisis y Evaluación de Riesgos y Amenazas	34
7.2	Procedimientos de Respaldos y Archivo de registros	34
7.2.1	Tipos de registros archivados	34
7.2.2	Periodo de conservación del archivo	35
7.2.3	Frecuencia de respaldo de archivos Protección del archivo	35
8.	Privacidad de datos	35
8.1	Protección de la confidencialidad de la información	35
8.1.1	Alcance de la Información Confidencial.....	35
8.1.2	Información que no se considera Confidencial.....	35
8.1.3	Responsabilidad de proteger la Información Confidencial	36
8.2	Protección de datos personales	36
8.2.1	Estándares	37
8.3	Procedimientos de protección de confidencialidad de la información de los solicitantes	38
9.	Otros asuntos comerciales y legales	43
9.1	Tarifas	43
9.2	Reembolsos	43
9.3	Seguros de responsabilidad	43
9.3.1	Propiedad Intelectual	44
9.4	Procedimientos de suspensión.....	44
9.4.1	Suspensión Temporal o Suspensión Definitiva	44
9.5	Procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de los Certificados Digitales y resguardarlas de manera confiable	46
9.5.1	Solicitud del servicio de Emisión de Certificados Digitales.....	46
9.5.2	Llenado de formato de Solicitud de servicio de ECD y documentación	47
9.5.3	Formato de Informe de Verificación de Identidad	47

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 4 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

9.5.4 Registro de operaciones del servicio que el Usuario puede realizar dentro del Portal de Certificados Digitales	47
9.5.5 Registro de operaciones del servicio que el Agente Certificador puede realizar dentro del Portal de Certificados Digitales	47
9.5.6 Aceptación del Certificado Digital	48
10. Fases y procedimientos del servicio de Emisión de Certificados Digitales	48
10.1 Tipos de Certificados Digitales que se entregarán	48
10.2 Personas que pueden solicitar el Servicio de Emisión de Certificados Digitales. Solicitud del Servicio de Emisión de Certificados Digitales	49
10.3 Registro y gestión de solicitudes de Certificados Digitales	49
10.4 Verificación de identidad.....	50
10.4.1 Objetivos, alcances y limitaciones de uso de los Certificados Digitales	55
10.4.2 Obligaciones y responsabilidades de la Autoridad Registradora – Agentes Certificadores	56
10.4.3 Obligaciones y responsabilidades de la Autoridad Certificadora	58
10.4.4 Limitaciones de responsabilidad	60
10.5 Generación de Certificados Digitales y controles para la generación de datos de creación de firma electrónica del usuario	61
10.6 Publicación de Certificados Digitales	62
10.7 Solicitud de sello de tiempo	62
10.8 Revocación de Certificados Digitales	62
10.9 Renovación de certificados digitales	64
11. Interoperabilidad.....	64

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

1. Información inicial

1.1 INFORMACIÓN DEL DOCUMENTO

Información del documento
Denominación formal del Documento: Plan Estratégico de Negocios en ATEB 2026-2030
Descripción: Declaración de Prácticas 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

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	Elaboración de documento inicial	Definición inicial del documento

*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	Abril
Año	
2027	Actualización
	Abril
2028	Actualización

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 6 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

	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

1.4 CLASIFICACIÓN DE LA INFORMACIÓN DEL DOCUMENTO

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

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

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

Además, y de conformidad con la LFPDPPP, con excepción de la información confidencial prevista en la ley, los sujetos obligados deben poner a disposición del público los términos del reglamento y los lineamientos, así como las actualizaciones que expida el instituto o la instancia equivalente a

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 7 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

que se refiere el Artículo 61 de la citada ley y toda la información que no esté clasificada como confidencial y que contravenga la protección de datos personales.

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

2. Introducción

2.1 ANTECEDENTES

En el presente documento se estipula la Declaración de Prácticas necesarias para la prestación del servicio de Emisión de Certificados Digitales, con base en las Reglas Generales No. 1 a 77 a las que deben sujetarse los Prestadores de Servicio de Certificación (PSC), con fundamento en lo dispuesto 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 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 con el RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, incluyendo los apartados que los integran, el Código de Comercio, Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación de la Secretaría de Economía y demás leyes aplicables.

De igual manera, este documento establece los procedimientos, prácticas, medidas de seguridad, las responsabilidades y obligaciones de las partes interesadas en el servicio de Emisión de Certificados Digitales, así como, la definición de los términos, condiciones y características que se deben cumplir para la prestación de este servicio.

2.2 OBJETIVO

Establecer y divulgar las normas, lineamientos, condiciones, procedimientos, prácticas, medidas de seguridad y demás elementos que mínimamente se requieren para el cumplimiento de las políticas aplicables a la prestación del servicio de Emisión de Certificados Digitales, que ATEB ha desarrollado e implementado, asegurando los elementos humanos, económicos, materiales y tecnológicos requeridos para brindar un servicio de calidad como Autoridad de Certificación y cuyo conocimiento sirva de guía para los suscriptores y demás partes interesadas.

2.3 ALCANCE

Esta Declaración de Prácticas aplica para todos aquellos suscriptores, solicitantes, (Personas Físicas o Morales) que soliciten el servicio de Emisión de Certificados Digitales, así como a las demás partes interesadas, incluyendo las normas, políticas y reglas que deba seguir ATEB como Autoridad Certificadora, siempre y cuando estén acorde a las leyes y normativas aplicables vigentes y, que se encuentren establecidos en el presente documento.

Así mismo, para todas las personas de las áreas involucradas en el desarrollo, implementación y soporte del servicio de Emisión de Certificados Digitales, estas son PSC-EDI, Seguridad, Jurídico, Desarrollo y Sistemas, para la correcta preservación de la confidencialidad, integridad y

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 8 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

disponibilidad de la información manejada en cada uno de los procesos que ATEB provee como Autoridad de Certificación.

2.4 DATOS DE CONTACTO

Para cualquier duda, aclaración o solicitud relacionada con el “Servicio”, el “Usuario” podrá comunicarse a:

ATEB Servicios, S.A. de C.V.

- Correo electrónico: contacto.psc@ateb.mx
- Teléfono: 55 5118 0300 opción. 9
- De forma presencial directamente en la Oficina Administrativa de ATEB ubicadas en: Av. Insurgentes Norte No. 554, Piso 2, Col. Atlampa, Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06450.
 - Horario de atención: de 09:00 a 18:00 horas.
- Sitio web: <https://www.ateb.mx/psc.html>

2.5 RESPONSABLES DE LA ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

El Profesional Informático, el Auxiliar de Apoyo Informático de Seguridad y el Profesional Jurídico, son los responsables de mantener actualizados los documentos que contienen la presente Declaración de Prácticas de Certificación, así como la Política de Certificación, con el fin de asegurar la correcta ejecución de todas las directrices relacionadas con el servicio de Emisión de Certificados Digitales emitidos por la Autoridad de Certificación de ATEB.

El Auxiliar de Apoyo Informático de Seguridad se encarga de ejecutar el Sistema de Gestión de Seguridad de la Información, planes, políticas, procedimientos y prácticas de Seguridad necesarias para garantizar la autenticidad, confidencialidad, integridad y disponibilidad en la Emisión de Certificados Digitales.

Una vez que se ha realizado algún cambio, actualización o modificación en la Declaración de Prácticas de Certificación y/o en la Política de Certificación, los responsables ponen a disposición de la Dirección General la información propuesta, quien una vez realizado el análisis y en caso de ser procedente, la autoriza y devuelve el documento a los responsables para su posterior publicación a través del sitio <https://www.ateb.mx/psc.html>

2.6 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 9 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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>

2.6.1 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.

2.7. 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>

2.8 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) Profiles on
- 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 por parte 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.

2.9 DEFINICIONES

Concepto	Definición
AC	Autoridad Certificadora (CertificationAuthority)

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 10 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

AR	Autoridad Registradora (Registration Authority)
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 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 11 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 12 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

	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. Partes interesadas y Participantes de la PKI

3.1 AUTORIDAD CERTIFICADORA

Autoridad Certificadora (AC): Dependencias y entidades de la Administración Pública Federal y los Prestadores de Servicios de Certificación que, conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos.

3.2 AGENTE CERTIFICADOR

Agente Certificador: Es una persona física o moral encargado de llevar a cabo la verificación de la identidad de los usuarios y su vinculación con los medios de identificación electrónica para la emisión de Certificados Digitales.

3.3 AUTORIDAD REGISTRADORA

Autoridad Registradora (AR): Aquella que lleva el registro de los elementos de identificación de los firmantes y de la información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y de emitir certificados digitales.

ATEB es responsable de su propia Autoridad Registradora, que se conforma con lo siguiente:

- Agente Certificador** quien realiza la verificación de la identidad de los usuarios solicitantes del servicio de Emisión de Certificados Digitales.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 13 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- b. **Portal de Certificados Digitales de Autoridad Registradora**, proporcionado por la Autoridad Certificadora, donde se gestionan los procedimientos correspondientes a la primera Autoridad.

3.4 SUScriptor

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

3.5 SOLICITANTE

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.

3.6 PARTE QUE CONFÍA

Parte que confía: La Persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

3.7 SECRETARÍA DE ECONOMÍA

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

4. Obligaciones y responsabilidades del servicio de Emisión de Certificados Digitales (ECD)

4.1 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 Declaración de Prácticas de Certificación se cumpla y esté acorde con la Política de Seguridad de la Información, con la Política de Certificados y los Procedimientos y Modelos Operacionales de la Autoridad Certificadora y Registradora.
- 2) Asegurar el cumplimiento de los Términos y Condiciones, así como, con lo establecido en la Política de Certificados, en la presente 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 14 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.
- 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 15 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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 presente Declaración de Prácticas de Certificación y la Política de Certificados en los medios establecidos.
- 28) Cumplir con el resguardo de información conforme a lo establecido por las leyes y normas aplicables.

4.2 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 Política de Certificados, en la presente 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 16 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.

4.3 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.

4.4 RESPONSABILIDADES DE LA AR

- 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 17 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.

4.4.1 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 presente Declaración de Prácticas de Certificación y la 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.
- 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 18 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.

4.5 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 Política de Certificados y la presente 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.
- 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 19 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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 presente Declaración de Prácticas de Certificación y la 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 presente Declaración de Prácticas de Certificación y en la Política de Certificados publicadas por la Autoridad Certificadora.

4.6 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 presente Declaración de Prácticas de Certificación y en la 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.
- 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 20 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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 este 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.

4.7 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 Política de Certificados y en la presente 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 Política de Certificados y en la presente Declaración de Prácticas de Certificación.
- 7) Validar y verificar la integridad de los documentos firmados con los Certificados Digitales en los que confía.
- 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 21 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

establecidas en la Política de Certificados y en la presente Declaración de Prácticas de Certificación.

4.8 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 Certificado, y o revocación del Certificado.
 - b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

5. Matriz RACI

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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 22 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

9.	Auxiliar de Apoyo Informático de Administrador de Bases de Datos	—	—	*	*
10.	Agente certificador	—	*	—	—

Nota: (*) Participa; (—) No participa

6. 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 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>.

6.1 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).

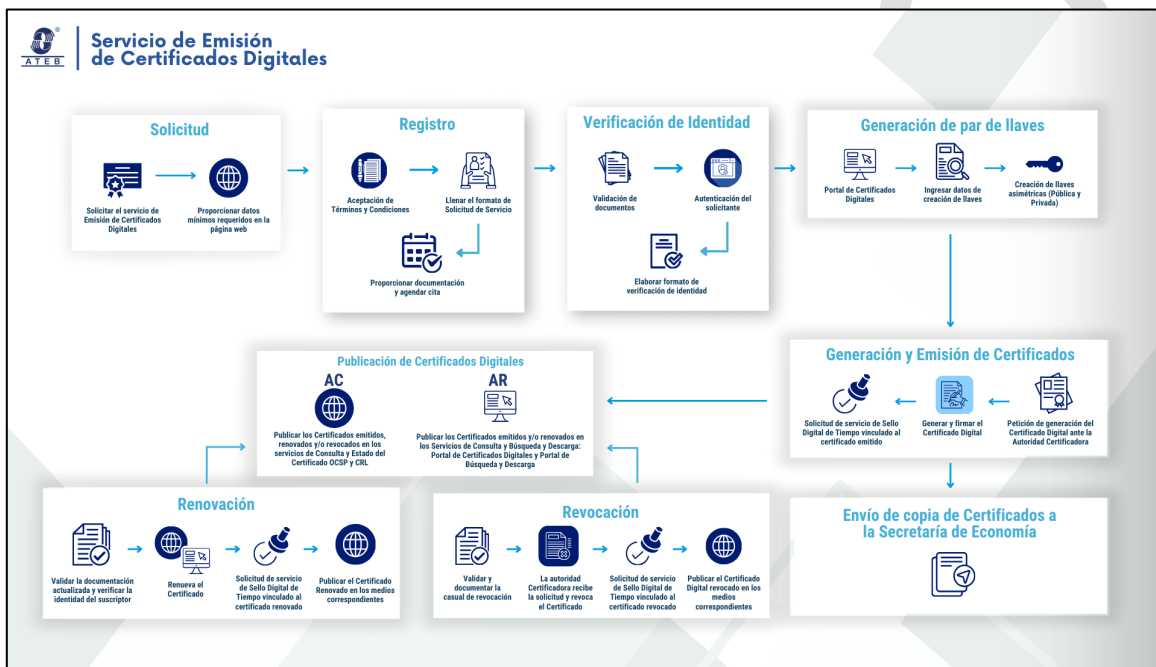
Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 23 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- **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.

6.2 PROCESOS DE OPERACIÓN QUE INTEGRAN EL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES DE LA AUTORIDAD CERTIFICADORA



6.3 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 Política de Certificados y el apartado 10.2 de la presente Declaración de Prácticas.
- **Gestión de Solicitudes.** La gestión y registro de solicitudes es llevada a cabo conforme lo señalado en el apartado 7.3 de la Política de Certificados y el apartado 10.3 de la presente Declaración de Prácticas.
- **Emisión de Certificados.** Inicia una vez 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 Política de

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 24 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

Certificados, mismo que tiene asociado su sello digital de tiempo y el apartado 10.5 de la presente Declaración de Prácticas.

- **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 Política de Certificados así como sus limitaciones de uso, las cuales se señalan en el mismo apartado y el apartado 10.4.1 de la presente Declaración de Prácticas.
- **Renovación del Certificado.** Se debe realizar conforme al apartado 7.9 de la Política de Certificados y el apartado 10.9 de la presente Declaración de Prácticas. 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 Política de Certificados y el apartado 10.8 de la presente Declaración de Prácticas.
- **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.

6.4 CONTROLES DE GESTIÓN, OPERATIVOS Y FÍSICOS

6.4.1 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 25 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.

6.4.2 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 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 26 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

6.4.3 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.

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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 27 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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

6.5 CONTROLES TÉCNICOS DE SEGURIDAD

6.5.1 Módulo criptográfico

Las medidas de seguridad adoptadas para proteger los Datos de Creación de Firma Electrónica del Certificado de la Autoridad Certificadora del Prestador de Servicios de Certificación:

La generación de las Claves Criptográficas utilizadas por la Autoridad Certificadora para el servicio de Emisión de Certificados Digitales se realiza en el Módulo de Seguridad de Hardware (HSM), de la marca Futurex, modelo Vectera Plus 100, el cual, cuenta con la Certificación FIPS140-2 nivel 3, y se encuentra resguardado en el Centro de Datos Principal, adicionalmente se cuenta con redundancia de este dispositivo en el Centro de Datos Alterno.

El Módulo de Seguridad de Hardware (HSM) modelo de HSM Vectera Plus 100 permite el manejo de particiones (slots) para el resguardo de las Claves Pública y Privada, para cada uno de los servicios acreditados.

La administración del acceso a los dispositivos HSM se divide por diferentes responsables que resguardarán las llaves y tarjetas del Módulo de Seguridad de Hardware (HSM) en diferentes niveles y cuyas responsabilidades se delimitan a cada uno de ellos.

La información es resguardada bajo 3 niveles:

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

La información que se almacena dentro del HSM es la llave privada y el certificado que se utiliza para el servicio de Emisión de Certificados Digitales.

6.5.2 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,

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 28 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

de la marca Futurex, modelo Vectera Plus 100, los cuales, cuentan con la Certificación FIPS140-2 nivel I 3.

6.5.3 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 dos años.

6.6 PERFILES DE CERTIFICADOS, CRL Y OCSP

6.6.1 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 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.

6.6.2 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 29 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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>

6.6.3 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 Infrastructure Online Certificate Status Protocol - OCSP, alineándose a este estándar.

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

6.7 ALCANCE Y USOS DE LOS CERTIFICADOS EMITIDOS

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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 30 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.

Cuando haya sido revocado el certificado por cualquier causal establecida en esta Declaración de Prácticas de Certificación y la Política de Certificados o haya finalizado su periodo de vigencia, la llave privada no puede volver a ser usada por el suscriptor.

Para consulta permanente, la información correspondiente a los usos del certificado se encuentra en la Política de Certificados y la presente Declaración de Prácticas, las cuales se encuentran publicadas en el sitio web de ATEB <https://www.ateb.mx/psc.html>.

6.8 ACEPTACIÓN DE LOS CERTIFICADOS

En la solicitud de información de los servicios de Emisión de Certificados Digitales, el Agente Certificador da a conocer los Términos y Condiciones a los solicitantes, los cuales, deben leer y aceptar y, desde ese momento, se comprometen a revisar el contenido y datos del certificado que se les emita, una vez que hayan aprobado los requisitos establecidos para su emisión.

El suscriptor – usuario una vez que ha descargado su Certificado Digital debe verificar como parte de sus responsabilidades y obligaciones que, los datos sean correctos, notificando su aceptación del Certificado Digital por correo electrónico a cofidismart@ateb.mx, en caso de que exista un error se deberá notificar al Agente Certificador a través del correo contacto.psc@ateb.mx.

7. Procesos de auditoría y respaldo

7.1 PROCESO DE AUDITORÍA

La Secretaría de Economía a fin de verificar el cumplimiento de las obligaciones como Prestador de Servicios de Certificación podrá practicar auditorías y requerir, la información y documentación necesaria para llevar a cabo sus funciones de visitas de verificación respecto al cumplimiento de las obligaciones establecidas para el servicio de Emisión de Certificados Digitales tanto en la Oficina Administrativa como en los Centros de Datos, siempre y cuando se reciba notificación y se desarrollen conforme a lo dispuesto en la Ley Federal de Procedimiento Administrativo.

Debido a que los Centros de Datos principal y alternativo son arrendados, ATEB asegurará que la Secretaría de Economía, cuente con los accesos, información y documentos necesarios para realizar las visitas de verificación, concernientes a las auditorías a que se refiere el párrafo anterior.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 31 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

7.1.1 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.

ATEB habilita todas las capacidades esenciales de auditoría de eventos en sus aplicaciones de Prestador de Servicios de Certificación registrando los eventos enumerados a continuación. Si las aplicaciones del servicio de Emisión de Certificados Digitales no pueden registrar automáticamente un evento, ATEB implementa procedimientos manuales para satisfacer los requisitos.

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.

Todos los registros de eventos están disponibles para los auditores como prueba de las prácticas de ATEB.

EVENTO AUDITABLE
AUDITORÍA DE SEGURIDAD:
AUTENTICACIÓN A LOS SISTEMAS
ENTRADA DE DATOS LOCALES
ENTRADA DE DATOS REMOTA
CARGA Y ALMACENAMIENTO DE CLAVES PRIVADAS
SELLO DE TIEMPO
SOLICITUDES DE REGISTRO
INFORMES DE VERIFICACIÓN DE IDENTIDAD
REQUERIMIENTO DE CERTIFICADO
CERTIFICADOS
VIGENCIA DE LOS CERTIFICADOS
DIVERSOS:
CAMBIOS DE CONFIGURACIÓN
ACCESO FÍSICO/SEGURIDAD DEL SITIO
ANOMALÍAS

7.1.2 Registro de frecuencia

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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 32 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.

7.1.3 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.

7.1.4 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.

El rol de confianza de Auxiliar de Apoyo Informático de Seguridad es el encargado de depositar la información en el repositorio.

7.1.5 Procedimientos de copia de seguridad respaldo de los registros de auditoría

ATEB realiza respaldos completos de manera semanal, los cuales se trasladan del centro de datos principal al centro de datos alterno.

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

Los registros de acceso físico a los centros de datos se realizan mediante registro en bitácoras y estas son resguardadas por el personal responsable.

7.1.6 Sistema de 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 e informarlos a Dirección General junto con las partes interesadas.

Estos documentos aplican para:

- Todas las auditorías internas que se requieran hacer en la organización a fin de encontrar mejoras en los procesos y actividades actuales e implementarlas para una mejor eficacia en la operación del negocio.
- Las normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022.
- El seguimiento de la remediación de observaciones (Necesidad de Mejora y No Conformidades) realizadas en otras auditorías.

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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 33 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

7.1.7 Evaluaciones de vulnerabilidad Análisis y Evaluación de Riesgos y Amenazas

El Procedimiento de Análisis de Vulnerabilidades que se tiene implementado en ATEB, tiene como objetivo comprobar y medir la eficiencia de los mecanismos de seguridad implementados e identificar vulnerabilidades, debilidades y amenazas para reducir los riesgos y proteger la confidencialidad, integridad y disponibilidad de la información.

Para lo anterior, se identifican y se clasifican los activos tecnológicos estimando los tiempos de respuesta e impactos en caso de la presencia de alguna contingencia. También el personal de seguridad se mantiene informado de los nuevos ataques y vulnerabilidades que puedan afectar la seguridad.

De igual manera se utilizan herramientas de software para el análisis de vulnerabilidades que ayudan a determinar las acciones que se deben realizar para remediarlas.

ATEB, adicionalmente, realiza de manera anual el ejercicio de Análisis y Evaluación de Riesgos y Amenazas que incluye las operaciones relacionadas con el servicio de Emisión de Certificados Digitales a través del cual, se identifican y evalúan amenazas internas y externas razonablemente previsibles que podrían dar lugar a posibles vulnerabilidades, tales como: acceso no autorizado, divulgación, uso indebido, alteración o destrucción de cualquier información digital, para controlar y minimizar el impacto de eventos inciertos, detectando y mitigando los riesgos identificados estableciendo la forma en que deben ser tratados para reducirlos hasta alcanzar un nivel aceptable.

ATEB también evalúa periódicamente la eficacia de las políticas, procedimientos, sistemas de información, tecnología y otros lineamientos que ATEB ha establecido para controlar tales riesgos.

El Análisis y Evaluación de Riesgos y Amenazas se realiza utilizando el estándar del National Institute of Standards and Technology Special Publication 800-30 Revision 1. September 2012.

7.2 PROCEDIMIENTOS DE RESPALDOS Y ARCHIVO DE REGISTROS

Para garantizar la confidencialidad, integridad y disponibilidad de la información del servicio de Emisión de Certificados Digitales en los medios de almacenamiento e implementar y dar cumplimiento a la Política de Respaldos, en ATEB se cuenta con el Procedimiento de Respaldos de Bases de Datos que se describe en el Procedimiento de Respaldos (PRO-SIS-RBD-006), gestionando la estrategia para su correcto manejo y protección permanente y oportuno.

En dicho procedimiento, se describen las responsabilidades y actividades que el personal de administración de bases de datos tiene asignadas para llevar a cabo los procesos de respaldo. Así como, los métodos de seguridad utilizados para garantizar y salvaguardar la protección de la información en todo momento.

7.2.1 Tipos de registros archivados

ATEB conserva la siguiente información de los archivos en la operación del servicio de Emisión de Certificados Digitales como Prestador de Servicios de Certificación.

- Solicitudes de registro
- Informes de verificación de identidad
- Requerimiento de certificado
- Certificados
- Vigencia de certificados
- Sellos de Tiempo

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 34 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- Acuses de recibo de envío de copia de certificados a la SE

7.2.2 Periodo de conservación del archivo

El tiempo de resguardo de la información, se establece con base en lo que determina la normatividad y autoridades que regulan el servicio de Emisión de Certificados Digitales.

El periodo de resguardo definido para los archivos es un plazo de diez (10) años.

7.2.3 Frecuencia de respaldo de archivos Protección del archivo

ATEB realiza respaldos incrementales de manera diaria y respaldos completos de manera semanal, los cuales, se trasladan del centro de datos principal al centro de datos alterno, de esta manera, se mantienen libres de modificaciones, sustituciones o destrucción no autorizadas y evitando su publicación.

8. Privacidad de datos

8.1 PROTECCIÓN DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

8.1.1 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.

8.1.2 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:

- Que haya sido de dominio público, o que sea publicada sin que medie ninguna acción y/o intervención de la parte que la recibe.
- Que la parte que la comparte la haga del dominio público.
- Que antes de ser revelada estuviera en posesión legítima de la parte que la recibe.
- 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.
- 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 35 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.

8.1.3 Responsabilidad de proteger la Información Confidencial

Con el fin de garantizar la protección de la información confidencial requerida que ATEB Autoridad Registradora intercambiará con los suscriptores – usuario y/o solicitantes para la prestación del servicio de Emisión de Certificados Digitales, 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.

8.2 PROTECCIÓN DE DATOS PERSONALES

ATEB como Autoridad Registradora que participa 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 del procedimiento 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 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 36 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

8.2.1 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.
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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 37 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

8.3 PROCEDIMIENTOS DE PROTECCIÓN DE CONFIDENCIALIDAD DE LA INFORMACIÓN DE LOS SOLICITANTES

ATEB en cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento, el GDPR (General Data Protection Regulation), el Convenio 108 y el 108 Plus, y demás relativas, pero sobre todo consciente de la importancia de la privacidad de las personas con los que mantiene relación, pone a disposición el presente procedimiento para solicitar el ejercicio de cualquiera de los derechos de Acceso, Rectificación, Cancelación, Oposición o Portabilidad, reconocidos por la normativa vigente, y a los cuales de manera conjunta se les denominará como Derechos ARCO.

Los derechos que toda persona pueda ejercer, en relación con el tratamiento de sus datos personales son:

- ❖ **Derecho de Acceso:** Tiene derecho a obtener de ATEB sus datos personales que obren en sus archivos, así como información relativa a las condiciones y generalidades del tratamiento.
- ❖ **Derecho de Rectificación:** El titular podrá solicitar en todo momento al responsable que rectifique sus datos personales que resulten ser inexactos, incompletos o no se encuentren actualizados.
- ❖ **Derecho de Cancelación:** El titular tiene derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en posesión del responsable. Lo anterior implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de estos y su posterior supresión.
- ❖ **Derecho de Oposición:** Oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, puede el titular delimitar las finalidades en el tratamiento de sus datos.
- ❖ **Derecho de Portabilidad:** Cuando a solicitud del titular se entrega una copia de sus datos personales al titular o a cualquier otro designado por este.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

Procedimiento de ATEB para la Atención de Solicitudes de Titulares relativas al Ejercicio de Derechos (ARCO)

Para realizar cualquier ejercicio relacionado con sus derechos personales, deberá seguir el siguiente procedimiento:

1. El Titular de los Datos Personales o su Representante Legal son los únicos facultados para solicitar el ejercicio de sus derechos ARCO.
2. La solicitud para ejercer derechos ARCO podrá presentarse a través de:
 - a. Escrito libre o formato de solicitud entregado directamente en nuestras oficinas ubicadas en: Avenida Insurgentes Norte, Número 554, Piso 2, Col. Atlampa, Alcaldía

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 38 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

Cuauhtémoc, Ciudad de México, C.P. 06450. El horario de Atención de Lunes a Viernes de 09:00 a 18:00 horas.

- b. Correo electrónico dirigido a: protecciondedatos@ateb.mx
3. Dicha solicitud será dirigida y canalizada a los responsables de la Protección de Datos Personales, quienes verificarán que la misma contenga lo siguiente:
 - a. El nombre del Titular de los datos, teléfono, así como domicilio completo, correo electrónico u otro medio para comunicarle la respuesta a su solicitud.
 - b. Documento vigente que acredite la identidad del Titular, o en su caso documento que acredite la representación legal del titular.
 - c. La descripción clara y precisa de los datos personales y/o las razones respecto de los que se busca ejercer alguno de los derechos ARCO.
 - d. Cualquier otro elemento o documento que facilite la localización de los datos personales.
 - e. La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado.
 - f. La solicitud de portabilidad deberá indicar el medio por el cual se solicita la entrega de los datos personales, la cual deberá ser evaluada por ATEB e informar al Titular si puede entregarse por ese medio, o se debe evaluar otro. En todo caso, el Titular deberá entregar el medio por el cual se realizará la entrega, en caso de no ponerlo a disposición de ATEB, se tomará como improcedente la solicitud, derivado de la falta de elementos para la entrega.
 4. En caso de que la solicitud no cumpla con alguno de estos requisitos de forma, se hará una prevención a la solicitud y se informará al solicitante por el medio que haya señalado dentro del periodo de 5 días hábiles posteriores a la presentación de la solicitud.
 5. En caso de que la solicitud reúna todos los requisitos de forma, se continuará el trámite de acuerdo con el siguiente procedimiento.

Procedimiento de ATEB para la Atención de Solicitudes de Titulares relativas al ejercicio de Derechos ARCO:

1. El Oficial de la Protección de Datos Personales comunicará la respuesta de la solicitud al Titular o a su Representante Legal, en un plazo máximo de 20 (veinte) días hábiles, contados a partir de la fecha de recepción de la solicitud de ejercicio de derechos ARCO, mediante el medio indicado por este en su solicitud.
2. Si resulta procedente la solicitud, se hará efectiva la misma dentro de los 15 (quince) días hábiles siguientes a la fecha en que se comunique la respuesta.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 39 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

Nota: Para cualquier tipo de solicitud, se deberá acreditar previamente la identidad del solicitante o representante legal, según corresponda, lo cual tendrá que hacer de manera presencial y personal el Titular o su representante legal.

3. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.
4. En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y esta resulte no serlo, bastará con que así se le indique al titular por cualquiera de los medios establecidos en la solicitud, para tener por cumplida la solicitud.
5. Se podrá negar el acceso, rectificación, cancelación, oposición o portabilidad al tratamiento de los datos personales al Titular de estos en los siguientes supuestos:
 - a. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello.
 - b. Cuando en su base de datos, no se encuentren los datos personales del solicitante.
 - c. Cuando ATEB no sea el Responsable de los datos personales indicados por el Titular.
 - d. Cuando se lesionen los derechos de un tercero.
 - e. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de estos.
 - f. Cuando la rectificación, cancelación u oposición ya haya sido previamente realizada.
 - g. Cuando no se ponga a disposición de ATEB el medio para la entrega de los datos personales, cuando se trate de una solicitud de Portabilidad.

El responsable deberá informar el motivo de su decisión y comunicarla al Titular, o en su caso, al representante legal, en un plazo de 20 (veinte) días hábiles, por el mismo medio establecido en la solicitud.

En caso de dudas sobre el procedimiento, usted se podrá comunicar vía telefónica al número 55 5118 0300 al Área de Atención al Cliente o al Área de Jurídico en la ext. 1286.

** Esta versión será publicada en la página electrónica de ATEB: www.ateb.mx, y será actualizada cada vez que este procedimiento sea actualizado.

Procedimiento de Solicitudes de RESPONSABLES relativas al Ejercicio de Derechos (ARCO)

ATEB en cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de Particulares, su Reglamento, el GDPR (General Data Protection Regulation), el Convenio 108 y el 108 Plus, y demás disposiciones relativas, pero sobre todo consciente de la importancia de su privacidad, pone a disposición el presente procedimiento para solicitar el ejercicio de cualquiera de los derechos de Acceso, Rectificación, Cancelación, Oposición o Portabilidad, reconocidos por la normativa vigente, y a los cuales de manera conjunta se le denominará como Derechos ARCO.

Los derechos que toda persona pueda ejercer, en relación con el tratamiento de sus datos personales son:

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 40 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- ❖ **Derecho de Acceso:** Tiene derecho a obtener de ATEB sus datos personales que obren en sus archivos, así como información relativa a las condiciones y generalidades del tratamiento.
- ❖ **Derecho de Rectificación:** El titular podrá solicitar en todo momento al responsable que rectifique sus datos personales que resulten ser inexactos ,incompletos o no se encuentren actualizados.
- ❖ **Derecho de Cancelación:** El titular tiene derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en posesión del responsable. Lo anterior implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión.
- ❖ **Derecho de Oposición:** oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, puede el titular delimitar las finalidades en el tratamiento de sus datos.
- ❖ **Derecho de Portabilidad:** Cuando a solicitud del titular se entrega una copia de sus datos personales al titular o a cualquier otro designado por este.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

NOTA: Para el ejercicio de estos derechos la solicitud deberá ser realizada por el Responsable que haya transmitido los Datos Personales a ATEB para su tratamiento.

Procedimiento de ATEB para la Recepción de Solicitudes de RESPONSABLES relativas al Ejercicio de Derechos (ARCO)

Para realizar cualquier ejercicio relacionado con los derechos personales de sus titulares, deberá seguir el siguiente procedimiento:

1. El Responsable de los Datos Personales, a través de su Oficial de Protección de Datos o su Representante legal, es el único facultado para solicitar la ejecución de derechos ARCO.
2. La Solicitud para ejercer derechos ARCO podrá presentarse a través de:
 - a) Escrito libre o formato de solicitud entregado directamente en nuestras oficinas ubicadas en: Avenida Insurgentes Norte, Número 554, Piso 2, Col. Atlampa, Alcaldía. Cuauhtémoc, Ciudad de México, C.P. 06450. El horario de Atención es de lunes a viernes de 09:00 a 18:00 horas.
 - b) Correo electrónico dirigido: protecciondedatos@ateb.mx

Cuando ATEB es ENCARGADO, el RESPONSABLE de los Datos Personales podrá solicitar cualquier derecho ARCO de cualquiera de sus Titulares.

Deberá realizarlo a través de una solicitud, que a su vez deberá ser realizada por el Oficial de Protección de Datos, o en su defecto por el Representante legal, dicha solicitud será por escrito y firmada.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 41 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

1. Dicha solicitud será dirigida y canalizada al Oficial de la Protección de Datos Personales, quien verificará que la misma contenga lo siguiente:
 - a. El nombre del Oficial de Protección de Datos o Representante Legal, correo electrónico u otro medio para comunicarle la ejecución de su solicitud.
 - b. Documento vigente que acredite la identidad del Titular, o en su caso documento que acredite la representación legal del titular.
 - c. La descripción clara y precisa de los datos personales y/o las razones respecto de los que se debe ejercer alguno de los derechos ARCO.
 - d. Cualquier otro elemento o documento que facilite la localización de los datos personales.
 - e. La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado.
 - f. La solicitud de portabilidad deberá indicar el medio por el cual se solicita la entrega de los datos personales, la cual deberá ser evaluada por ATEB e informar al Titular de si puede entregarse por ese medio, o se debe evaluar otro. En todo caso, el Titular deberá entregar el medio por el cual se realizará la entrega, en caso de no ponerlo a disposición de ATEB, se tomará como improcedente la solicitud derivado de la falta de elementos para la entrega.
2. En caso de que la solicitud no cumpla con alguno de estos requisitos de forma, se rechazará la solicitud y se informará al responsable por el medio que haya señalado.
3. En caso de que la solicitud reúna todos los requisitos de forma, se continuará el trámite de acuerdo con el siguiente procedimiento.

Procedimiento de ATEB para la Atención de Solicitudes de RESPONSABLES relativas al Ejercicio de Derechos (ARCO)

1. El Oficial de la Protección de Datos Personales comunicará la respuesta de la solicitud Responsable, en un plazo máximo de 20 (veinte) días hábiles, contados a partir de la fecha de recepción de la solicitud de ejecución de derechos ARCO, mediante el medio indicado por este en su solicitud.
2. Si resulta procedente la solicitud, se hará efectiva la misma dentro de los 15 (quince) días hábiles siguientes a la fecha en que se comunique la respuesta.
 Nota: Para cualquier tipo de Solicitud, se deberá acreditar previamente la identidad del solicitante o representante legal, según corresponda, lo cual se tendrá que hacer de manera presencial y personal el Titular o su representante legal.
3. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.
4. En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y esta resulta no serlo, bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior, para tener por cumplida la solicitud.
5. Se podrá negar el ejercicio de los derechos ARCO cuando:

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 42 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- El solicitante no sea el Oficial de los datos personales por parte del Responsable, o el representante legal no esté debidamente acreditado para ello;
- Cuando en su base de datos, no se encuentren los datos personales del solicitante;
- Cuando se lesionen los derechos de un tercero;
- Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
- Cuando la rectificación, cancelación u oposición ya haya sido previamente realizada.

ATEB informará el motivo de su decisión al Oficial de Datos Personales, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio indicado en la solicitud.

En caso de dudas sobre el procedimiento, usted se podrá comunicar vía telefónica al número 55 5118 0300 al área de Atención al Cliente o al área Jurídica Ext. 1286.

** Esta versión será publicada en la página electrónica de ATEB: www.ateb.mx, y será actualizada cada vez que este procedimiento sea actualizado.

9. Otros asuntos comerciales y legales

9.1 TARIFAS

Los solicitantes del servicio de Emisión de Certificados Digitales serán informados oportunamente de las tarifas establecidas para este servicio.

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

9.2 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 presente 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 estos, 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.

9.3 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

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 43 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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 estos 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.

9.3.1 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.

9.4 PROCEDIMIENTOS DE SUSPENSIÓN

9.4.1 Suspensión Temporal o Suspensión Definitiva

Si ATEB Servicios, S.A. de C.V. como Autoridad Certificadora y Autoridad Registradora incumple con las obligaciones que se le imponen en el Código de Comercio, 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, podrá ser sancionada por la Secretaría de Economía con **suspensión temporal o definitiva** de sus funciones, conforme a lo dispuesto en los artículos 110 del Código de Comercio y 24, 25, 26 y 27 del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.

Procedimiento en caso de Suspensión Temporal o Suspensión Definitiva

En caso de **suspensión temporal**, se deberá seguir el siguiente procedimiento:

- Notificar a los suscriptores, usuarios y demás partes interesadas la suspensión temporal del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable, y el tiempo de la suspensión temporal.
- Suspender de forma temporal cualquier recepción de solicitudes y la Emisión de Certificados Digitales de Firma Electrónica Avanzada.
- Publicar en la página web <https://www.ateb.mx/psc.html> el motivo y el periodo de suspensión temporal.
- Asegurar en todo momento la disponibilidad de los servicios de consulta y estado de los certificados CRL y OCSP.
- Solventar las observaciones realizadas por la Secretaría de Economía, entregando documentos con las evidencias correspondientes de su solvencia.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 44 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- Recibir notificación de las observaciones atendidas y solventadas.
- Reanudar las actividades regulares.

En caso de **suspensión definitiva**, se deberá seguir el siguiente procedimiento:

- Notificar a los suscriptores, usuarios y demás partes interesadas la suspensión definitiva del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable.
- Recibir la notificación de parte de la Secretaría de Economía de a qué Prestador de Servicios de Certificación deberá ser transferida la información relacionada con los archivos y registros del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable que se dejará de proporcionar.
- Notificar y poner a disposición de los suscriptores, usuarios y demás partes interesadas toda la información relacionada con la suspensión definitiva del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable por correo electrónico y publicarlo en la página web <https://www.ateb.mx/psc.html>, incluyendo quién será el Prestador de Servicios de Certificación que seguirá otorgando el servicio, así como las acciones que deben considerar para minimizar los impactos que pudieran surgir de este cese.
- Notificar al personal interno la suspensión definitiva y eliminar los accesos a los que por cuestión de sus funciones tuvieran.
- Suspender cualquier recepción de solicitudes y Emisión de Certificados Digitales de Firma Electrónica Avanzada.
- Asegurar la disponibilidad de los servicios de consulta y estado de los Certificados Digitales CRL y OCSP hasta que el nuevo Prestador de Servicios de Certificación se haga cargo de esta actividad.
- Resguardar la información generada con motivo de la prestación del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable por los plazos que señale la normativa aplicable para los fines que correspondan.
- Eliminar los datos de Creación de Firma del Certificado Digital de la Autoridad Certificadora.

Cese de Funciones

En el caso de cesar en su actividad, ATEB Servicios, S.A. de C.V. como Autoridad Certificadora y Autoridad Registradora, deberá comunicarlo a la Secretaría de Economía a fin de determinar el destino que se dará a sus registros y archivos, conforme al artículo 104 fracción VI del Código de Comercio y al numeral 18 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

En caso de **cese de funciones**, se deberá seguir el siguiente procedimiento:

- Notificar mediante escrito a la Secretaría de Economía con cuarenta y cinco (45) días de anticipación en caso de que ya no se desee continuar prestando el servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable, adjuntando el comprobante del pago de derechos.
- Cerciorarse de recibir acuse de recibo por parte de la Secretaría de Economía a la notificación realizada del deseo de cese de funciones.
- Recibir la notificación de parte de la Secretaría de a qué Prestador de Servicios de Certificación deberá ser transferida la información relacionada con los archivos y registros

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 45 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada que se dejará de proporcionar.

- Notificar y poner a disposición de los suscriptores, usuarios y demás partes interesadas toda la información relacionada con el cese de funciones del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable por correo electrónico y publicarlo en la página web <https://www.ateb.mx/psc.html>, incluyendo quién será el Prestador de Servicios de Certificación que seguirá otorgando el servicio, así como las acciones que deben considerar para minimizar los impactos que pudieran surgir de este cese.
- Notificar al personal interno el cese de funciones y eliminar los accesos a los que por cuestión de sus funciones tuvieran.
- Suspender cualquier recepción de solicitudes y emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable.
- Asegurar la disponibilidad de los servicios de consulta y estado de los Certificados Digitales CRL y OCSP hasta que el nuevo Prestador de Servicios de Certificación se haga cargo de esta actividad.
- Resguardar la información generada con motivo de la prestación del servicio de Emisión de Certificados Digitales de Firma Electrónica Avanzada o Fiable por los plazos que señale la normativa aplicable para los fines que correspondan.
- Eliminar los datos de Creación de Firma del Certificado Digital de la Autoridad Certificadora.

Durante el proceso de cese de funciones, ATEB Servicios S.A. de C.V. como Autoridad Certificadora y Autoridad Registradora, realizará todo lo necesario para asegurar que se minimicen al máximo los impactos posibles a los suscriptores, usuarios y demás partes interesadas. De igual manera, en caso de que la Secretaría de Economía, dentro de la Resolución emitida, notificara alguna acción adicional por realizar, ésta se llevará a cabo y se informará en su caso, a los suscriptores, usuarios y demás partes interesadas.

9.5 PROCEDIMIENTO PARA REGISTRAR LA FECHA Y HORA DE TODAS LAS OPERACIONES RELACIONADAS CON LA EMISIÓN DE LOS CERTIFICADOS DIGITALES Y RESGUARDARLAS DE MANERA CONFIABLE

9.5.1 Solicitud del servicio de Emisión de Certificados Digitales

Cuando se presenta el primer contacto del solicitante del servicio de Emisión de Certificados Digitales hacia ATEB, este proporciona sus datos básicos, para ser contactado, si el contacto es mediante el sitio web <https://www.ateb.mx/Contacto.aspx> y, cuando se otorga el consentimiento del Tratamiento de Datos Personales a través del Aviso de Privacidad, así como, cuando se aceptan los Términos y Condiciones se genera un correo electrónico automático, el cual, se resguarda en la nube de Microsoft OneDrive por default, y la información contenida en el correo se captura en un archivo Excel, denominado "Registro solicitantes del servicio de ECD", que se resguarda en un sistema de versiones centralizado (SVN).

En caso de que el solicitante establezca contacto por otros de los medios establecidos: WhatsApp, Teléfono, Correo Electrónico o directo en la Oficina Administrativa, podrá otorgar, de igual manera, el consentimiento del Tratamiento de Datos Personales a través del Aviso de Privacidad, así como, la aceptación de los Términos y Condiciones mediante el sistema COFIDI Smart, generándose un

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 46 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

correo electrónico para este trámite y resguardándose en la base de datos correspondiente de dicho sistema.

9.5.2 Llenado de formato de Solicitud de servicio de ECD y documentación

El solicitante recibe el formato de Solicitud de servicio de Emisión de Certificados Digitales a través de correo electrónico, el cual, deberá llenar y firmar a través del sistema COFIDI Smart, así mismo, adjuntar la documentación de requisitos en forma electrónica, lo cual, resguarda en una base de datos de dicho sistema.

9.5.3 Formato de Informe de Verificación de Identidad

Cuando se realiza la Verificación de Identidad, tanto la información revisada y validada, como el resulta de este proceso, se captura en el formato de Informe de Verificación de Identidad, mismo que se resguarda de forma física en el mobiliario específico con mecanismos de seguridad.

9.5.4 Registro de operaciones del servicio que el Usuario puede realizar dentro del Portal de Certificados Digitales

Cuando la verificación de Identidad es exitosa, se crea el usuario dentro del Portal de Certificados Digitales, resguardándose esta información en la base de datos correspondiente AR_Log.

Una vez ingresando el usuario por primera vez, debe cambiar su contraseña y se resguarda en la base de datos antes mencionada.

Cuando el usuario ya cuenta con sus propias llaves de acceso, puede realizar las siguientes acciones:

1. Creación de certificados digitales
2. Descarga de archivo .cer. Múltiples veces
3. Descarga de archivo .key. Solo una vez, al finalizar la generación.
4. Revocación de certificado digital
5. Solicitud de renovación de certificado digital
6. Renovación de certificado digital autorizado por el Agente Certificador. Revoca el actual y genera uno nuevo.
7. Habilitación de autenticación por doble factor
8. Deshabilitación de autenticación por doble factor

Todas estas acciones son registradas a nivel base de datos llamada "AR_Log" indicando el usuario ejecutor, la acción, la fecha y hora en la que se realizó.

9.5.5 Registro de operaciones del servicio que el Agente Certificador puede realizar dentro del Portal de Certificados Digitales

El Agente Certificador cuenta con un perfil de tipo Admin y las acciones que puede ejecutar dentro del sistema son las siguientes:

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 47 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

1. Dar de alta clientes
2. Dar de baja clientes
3. Dar de alta usuarios
4. Cambiar la contraseña de los usuarios
5. Desbloquear los usuarios que han sido bloqueados por fallar los intentos de inicio de sesión
6. Dar de baja usuarios
7. Relacionar un usuario con un cliente
8. Quitar la relación entre usuario y cliente
9. Revocar certificados
10. Autorizar la renovación de certificados
11. Habilitación de autenticación por doble factor
12. Deshabilitación de autenticación por doble factor

Todas estas acciones son registradas a nivel base de datos llamada "AR_Log" indicando el usuario ejecutor, la acción, la fecha y hora en la que se realizó.

9.5.6 Aceptación del Certificado Digital

El usuario cuando ha recibido su Certificado Digital de Firma Electrónica Avanzada recibe correo electrónico con el formato de Carta de Aceptación de Certificado Digital, la cual, firma mediante el sistema COFIDI Smart, misma que se resguarda en la base de datos correspondiente de dicho sistema.

10. Fases y procedimientos del servicio de Emisión de Certificados Digitales

El servicio de Emisión de Certificados Digitales incluye las siguientes fases y procedimientos con alcance aplicable a los tipos de certificados que se entregarán:

10.1 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 48 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.

10.2 PERSONAS QUE PUEDEN SOLICITAR EL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES. SOLICITUD DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES

- 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.
- 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.

10.3 REGISTRO Y GESTIÓN DE SOLICITUDES DE CERTIFICADOS DIGITALES

- 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 estas solicitudes es como el responsable las atenderá.
- 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.

- El Agente Certificador proporciona el Formato de Solicitud del servicio de Emisión de Certificados Digitales al solicitante para su llenado.
- Solicita la documentación de identificación al solicitante, siendo esta la siguiente:
 - Comprobante de domicilio en formato electrónico
 - Clave Única del Registro de Población (CURP) en formato electrónico
 - 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 49 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.

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.

10.4 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:

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 50 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

No.	Actividad	Descripción	Responsable	Entrada	Salida
1	Revisar la información y documentación proporcionada	<p>Revisa la información y documentación proporcionada por el solicitante, suscriptor - usuario</p> <p>1. ¿Cuál es el motivo de revisión de la información proporcionada?</p> <p>PRIMERA SOLICITUD: Continúa en la pregunta 2</p> <p>RENOVACIÓN: Pasa a la actividad 2</p> <p>2. ¿La información está completa y correcta?</p> <p>NO: Pasa a la actividad 3</p> <p>SI: Pasa a la actividad 4</p>	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor - usuario	Información y documentación proporcionada por el solicitante, suscriptor - usuario debidamente revisada
2	Solicitar la documentación actualizada al suscriptor - usuario	<p>Solicita la documentación actualizada con respecto a la que proporcionó cuando se le emitió el certificado digital</p> <p>Regresa a la pregunta 2 de la actividad 1</p>	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	<p>Notifica sobre la información faltante al solicitante, suscriptor - usuario y solicita que le sea enviada para su revisión</p> <p>Regresa a la pregunta 2 de la actividad 1</p>	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	<p>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:</p>	Agente Certificador	Información y documentación proporcionada por el solicitante, suscriptor - usuario debidamente revisada	Validación de veracidad de la información y documentos proporcionados

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 51 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

		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			
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)	Agente Certificador	Recepción del Formato de solicitud del servicio de Emisión de Certificados Digitales firmado	Documentos originales recibidos

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 52 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

		<p>3.- Documento de identificación oficial con fotografía vigente expedido por autoridad competente (credencial para votar)</p> <p>4.- Cédula de Identificación Fiscal actualizada</p> <p>5.- Acta de nacimiento o Carta de Naturalización en caso de ser extranjero.</p> <p>6.- Documento de migración que acredite la Residencia Temporal o Permanente en México, en formato electrónico en caso de ser extranjero</p> <p>Cuando la solicitud del certificado es para una persona moral, también se deberá solicitar:</p> <p>7.- Cédula de Identificación Fiscal actualizada de la Persona Moral</p> <p>8.- Carta de solicitud de emisión del certificado digital, en hoja membretada firmada por el representante legal de la persona moral</p> <p>9.- Documento que acredite la Representación Legal del firmante solicitante</p> <p>NOTA: En caso de renovación solo deberá entregar la información actualizada</p>			
9	Cotejar los documentos originales del solicitante, suscriptor - usuario con los recibidos en formato electrónico	<p>Coteja los documentos originales del solicitante, suscriptor - usuario con los recibidos en formato electrónico</p> <p>¿Coincide la información con los documentos originales?</p> <p>SI: Pasa la actividad 10</p> <p>NO: Pasa a la actividad 12</p> <p>NOTA. Cuando no coincida la información se debe de registrar el hecho</p>	Agente Certificador	Documentos originales recibidos	Documentos originales y documentos en formato electrónico cotejados

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

10	Realizar la autenticación y prueba de vida con la presencia del solicitante, suscriptor - usuario	<p>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.</p> <p>¿La verificación de identidad fue exitosa?</p> <p>NO: Pasa a la actividad 12</p> <p>SI: Pasa a la actividad 13</p>	Agente Certificador	Documentos originales y documentos en formato electrónico cotejados	Autenticación y prueba de vida realizada
11	Solicitar el video y/o realizar una videollamada	<p>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.</p> <p>En caso de extranjeros, se solicita documento oficial que acredite su estancia en el territorio nacional.</p> <p>¿La verificación de identidad fue exitosa?</p> <p>NO: Pasa a la actividad 12</p> <p>SI: Pasa a la actividad 13</p> <p>NOTA: La renovación remota no se puede realizar por más de una ocasión</p>	Agente Certificador	Solicitud de renovación remota	Autenticación y prueba de vida realizadas
12	Registrar el hecho y rechazar la solicitud	<p>Registra el hecho en el "Formato de Informe de Verificación de Identidad" (FOR-EDI-VDI-057) y rechaza la solicitud</p> <p>NOTA.- En caso de no aprobarse la solicitud se debe informar al solicitante los motivos del rechazo.</p> <p>FIN DEL PROCEDIMIENTO</p>	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

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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					

10.4.1 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 55 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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 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.
- 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.

10.4.2 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 56 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 57 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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.

10.4.3 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 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 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 58 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.
- 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 Política de Certificados en los medios establecidos.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 59 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.
- 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.

10.4.4 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 de 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 60 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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 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.
- 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.

10.5 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 **6.1 Importancia y uso de los certificados digitales** mismo que será

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 61 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

publicado y se podrá descargar de los medios de consulta y descarga señalados en el apartado **10.6 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.

10.6 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>
- 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>

10.7 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.

10.8 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;

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 62 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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.
- El suscriptor del certificado digital, de acuerdo con las causales señaladas anteriormente y consideradas en la 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como "Público"	Página: 63 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

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 **10.6 Publicación de Certificados Digitales**.

10.9 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.

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 **10.6 Publicación de Certificados Digitales**.

11. Interoperabilidad

ATEB Autoridad Certificadora, dentro de su 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.

Elaboró: EAP	Elaboración inicial: 20/Abr./2026	Actualización: 02/Abr./2026
Versión: 1.0	Documento clasificado como “Público”	Página: 64 de 65

	Plan Estratégico de Negocios en ATEB 2026-2030	MIA-SEG-DPC-109
	Declaración de Prácticas del servicio de Emisión de Certificados Digitales	
	Modelado de Procesos de Negocio en ATEB	

- 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”*.