
# POLÍTICA DE CERTIFICACIÓN

Aprobado con Resolución Administrativa
AGETIC/RA/0053/2026, de 29 de julio de 2026

## UNIDAD DE GESTIÓN Y ACTUALIZACIÓN TECNOLÓGICA (UGAT)

| | |
|---|---|
| AGETIC Digitalizando Bolivia | **FICHA DE CONTROL DE CAMBIOS** |

**Nombre del documento:** Política de Certificación.

**Código del Documento:**

| CONTROL DE CAMBIOS | | |
|---|---|---|
| **REF.** | **VERSIÓN ANTERIOR** | **VERSIÓN ACTUAL** |
| 1 | | |

**RESPONSABLES DE ELABORACIÓN, REVISIÓN Y DE CONFORMIDAD**

| **Elaborado por:** | **Revisado por:** | **Revisado por:** | **Conformidad:** |
|---|---|---|---|
| Juan de Dios Villafuerte Mollinedo<br>Cargo: Consultor en línea<br>Firma Digital | Julio Oswaldo Mujica Quispe<br>Cargo: Profesional de Diseño Conceptual I<br>Firma Digital<br><br>Jose Rodrigo Quiroz Barrios<br>Cargo: Jefe de la Unidad de Gestión y Asistencia Tecnológica<br>Firma Digital | Everth Rubin de Celis Gallardo<br>Cargo: Responsable de Planificación<br>Firma Digital<br><br>Gabriela Daniela Quino Melgarejo<br>Cargo: Técnico de Planificación<br>Firma Digital | Carlos Eduardo Rodrigo Prado<br>Cargo: Director General Ejecutivo a.i.<br>Firma Digital |

:

# CONTENIDO

## CAPÍTULO I
## DISPOSICIONES GENERALES

### 1. Objeto

Establecer los principios, criterios y lineamientos generales que rigen el servicio de emisión de certificados digitales por parte de la Agencia de Gobierno Electrónico y Tecnologias de Informacion y Comunicacion (AGETIC), en su calidad de Entidad Certificadora Pública (ECP), regulando las disposiciones aplicables a la solicitud, validación, emisión, renovación y gestión del ciclo de vida de los certificados digitales.

### 2. Marco Normativo

La presente documento se sustenta en las siguientes disposiciones legales y normativas, ordenadas de acuerdo a la jerarquía y cronología correspondiente:

- Constitución Política del Estado, de 07 de febrero de 2009.
- Ley Nº 1178, de 20 de julio de 1990, de Administración y Control Gubernamentales (SAFCO).
- Ley Nº 164, de 08 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- Decreto Supremo Nº 2514, de 09 de septiembre de 2015, de creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).
- Decreto Supremo Nº 3251, de 11 de julio de 2017, que aprueba el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos.
- Decreto Supremo N° 3527, de fecha 11 de abril de 2018, que modifica y actualiza el Decreto Supremo N° 1793.
- Decreto Supremo Nº 5519, de 13 de enero de 2026, que modifica las funciones de la AGETIC facultándola para prestar servicios de firma digital.
- Resolución Administrativa Regulatoria ATT-DJ-RAR-TL-LP-249-2026, emitida por la ATT, que otorga a la AGETIC la autorización para la prestación de servicios de certificación digital como Entidad Certificadora Pública (ECP).
- Contrato de Autorización ATT-DJ-CON SCD LP 1/2026, suscrito entre la ATT y la AGETIC para la prestación de servicios de certificación digital.
- Resolución Administrativa AGETIC/RA/0158/2023, de 21 de noviembre de 2023, Reglamento Específico del Sistema de Organización Administrativa de la AGETIC (RE-SOA).
- Directrices para la Elaboración de Reglamentos, Manuales, Políticas, Procesos, Procedimientos y Otros Documentos Sustantivos de la AGETIC, aprobadas mediante Resolución Administrativa AGETIC/RA/0047/2026.

### 3. Alcance y/o Ámbito de Aplicación

La presente Política es de aplicación obligatoria para la Unidad de Gestión y Asistencia Tecnológica (UGAT), la Unidad de Infraestructura Tecnológica (UIT), la Unidad de Producción

y Actualización Tecnológica (UPAT) y todas las áreas organizacionales de la AGETIC que intervienen en la prestación del servicio de certificación. Asimismo, es de cumplimiento obligatorio para los signatarios, usuarios corporativos y terceros que confían en los certificados emitidos por la ECP-AGETIC.

## 4. Previsión

En caso de presentarse dudas, omisiones, contradicciones y/o diferencias en la interpretación de la presente política, estas serán solucionadas en los alcances y previsiones establecidas en las disposiciones legales y normativas de mayor jerarquía, según corresponda.

## 5. Definiciones

Para efectos de la presente descripción, se establecen las siguientes definiciones ordenadas alfabéticamente:

- **Autenticación:** Proceso técnico de verificación por el cual se garantiza la identidad del signatario en un documento digital que contenga firma digital.
- **Certificado Digital:** Archivo firmado digitalmente por la ECP-AGETIC que incluye datos que permiten identificar al titular, a la entidad emisora, su vigencia y la información para verificar la firma digital**.**
- **Clave privada:** Conjunto de caracteres únicos que el signatario emplea para la generación de una firma digital y que debe mantenerse bajo su exclusivo control**.**
- **Clave pública:** Conjunto de caracteres de conocimiento público que permite verificar la firma digital del signatario contenida en el certificado.
- **Firma Digital:** Firma electrónica que identifica únicamente a su titular, creada por métodos bajo su absoluto control y vinculada a los datos de modo que cualquier modificación posterior sea detectable.
- **Identificador de Objeto (OID):** Valor numérico único registrado que identifica de manera inequívoca a la presente Política de Certificación dentro de la infraestructura jerárquica.
- **Política de Certificación (CP):** Documento de carácter estratégico y técnico que establece las reglas y lineamientos institucionales para la gestión de los certificados digitales en la AGETIC**.**
- **Repositorio:** Sitio web institucional donde se publican los documentos públicos del servicio, las listas de revocación y los certificados de la cadena de confianza.
- **Signatario:** Persona natural o jurídica titular de un certificado digital emitido por la AGETIC que le permite realizar firmas digitales.
- **Usuario Titular:** Persona física que posee los derechos de revocación, reemisión y renovación sobre el certificado digital**.**

## 6. Aprobación, Vigencia, Difusión e Implementación

La aprobación de la presente Política deberá ser realizada por el Director General Ejecutivo de la AGETIC, como Máxima Autoridad Ejecutiva, mediante la emisión de la Resolución Administrativa.

La puesta en vigencia del documento se considerará a partir de su aprobación o de la fecha expresamente establecida en la mencionada Resolución Administrativa.

La difusión será realizada por el Área de Planificación (AP) en coordinación con la Unidad de Gestión y Asistencia Tecnológica (UGAT), asegurando que sea de conocimiento general para el personal de la entidad.

La implementación de lo establecido en esta Política estará a cargo de la UGAT, en el ámbito de sus competencias y responsabilidades técnicas.

## 7. Revisión y Actualización

El presente documento deberá ser ajustado y/o actualizado cuando se produzcan cambios o ajustes en el marco normativo, o cuando por razones internas y/o del entorno se justifique realizar modificaciones.

El Área de Diseño Tecnológico (ADIT) dependiente de la Unidad de Gestión y Asistencia Tecnológica (UGAT) en coordinación con el Área de Planificación (AP), realizará el ajuste y actualización de este documento cuando se produzcan los cambios señalados.

Toda vez que la esta política sea actualizada, deberá darse cumplimiento al punto precedente de Aprobación, Vigencia, Difusión e Implementación.

# CAPÍTULO II
# POLÍTICAS DE CERTIFICACIÓN

## 8. Introducción

### 8.1. Descripción General

El presente documento presenta la Política de Certificación Digital para los Certificados Digitales emitidos por la Entidad Certificadora Pública AGETIC, y define los términos que rigen el servicio en el marco de la Ley N.º 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, Decretos Supremos Nº 1793 y Decreto Supremo Nº 3527 que aprueban el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación y modificaciones, respectivamente.

La Política de Certificación es un instrumento que establece las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, renovación y revocación de los certificados.

Las Políticas de certificación son desarrolladas y aprobadas por la Entidad Certificadora Pública AGETIC, y posteriormente presentadas a la ATT.

#### 8.1.1. Propósito

El certificado digital para firma digital cumple los siguientes propósitos:

a) Acredita la identidad del titular del Certificado Digital
b) Proporciona legitimidad del Certificado en base a los servicios de verificación de revocación de certificados.
c) Vincula un documento digital o mensaje electrónico de datos firmado digitalmente con el usuario titular.
d) Garantiza la integridad del documento digital o mensaje electrónico con firma digital.

#### 8.1.2. Descripción de la Entidad Certificadora.

El Decreto Supremo Nº 2514 y su modificación realizada por medio del Decreto Supremo N°5519 respecto a la firma digital, otorgan y consolidan las atribuciones a la AGETIC para la prestación de servicios de certificación digital como Entidad Certificadora Pública (ECP), dirigido el sector público y la población en general a nivel nacional, conforme a las disposiciones contenidas en la Ley N.° 164, velando por la autenticidad, integridad y el no repudio entre las partes.

En fecha 01 de abril de 2026 la AGETIC firma el contrato ATT-DJ-CON SCD 1/2026 con la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, por el cual se autoriza la prestación de servicios de certificación digital a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación en Bolivia.

Las funciones de la Entidad Certificadora Pública AGETIC están establecidas en el ARTÍCULO 39.- (FUNCIONES DE LA ENTIDAD CERTIFICADORA) del Decreto Supremo N.º 1793, que indica:

- Emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales;
- Facilitar servicios de generación de firmas digitales;
- Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario;
- Validar y comprobar cuando corresponda, la identidad y existencia real de la persona natural o jurídica;
- Reconocer y validar los certificados digitales emitidos en el exterior;
- Otras funciones relacionadas con la prestación de servicios de certificación digital.

Las oficinas administrativas de la Entidad Certificadora Pública AGETIC se encuentran ubicadas en Bolivia, departamento de La Paz, zona Sopocachi, calle Pedro Salazar n.º 631, esquina Andrés Muñoz, Edificio: Edificio del Fondo Nacional de Desarrollo Regional (FNDR), Pisos 3, 4 y 5, asimismo, las dependencias de su Centro de Procesamiento de Datos Principal se encuentran en Bolivia, departamento de La Paz, zona Central, Calle Ayacucho esquina Calle Potosí, Edificio de la Vicepresidencia del Estado, en la parte del subsuelo y su Centro de Procesamiento de Datos Alterno se encuentra ubicado en Bolivia, departamento de La Paz, zona San Miguel, calle Jaime Mendoza, No 981, Piso 1.

### 8.2. Identificación del documento.

#### 8.2.1. Nombre.

El presente documento lleva como título “Políticas de Certificación”.

#### 8.2.2. Versión.

La versión del presente documento se encuentra establecido en la cabecera del presente documento, vinculado a su respectiva Resolución Administrativa de aprobación.

#### 8.2.3. Fecha de elaboración.

La fecha de elaboración y la última actualización de la presente “Política de Certificación” se encuentran detalladas en la carátula del presente documento, vinculadas a su respectiva Resolución Administrativa de aprobación.

#### 8.2.4. Fecha de actualización.

Se considera como fecha de actualización a la fecha en la que el documento entre en vigencia a partir de su respectiva aprobación.

#### 8.2.5. Localización.

La presente política se la puede localizar en:
https://firmadigital.bo/politicas-de-certificacion-2026.pdf

#### 8.2.6. Identificador de Objeto.

Éste documento tiene el siguiente Identificador de Objeto (OID): 2.16.68.0.0.0.1.14.1.2.0.1.0.0

### 8.3. Infraestructura Nacional de Certificación Digital.

La Infraestructura Nacional de Certificación Digital, está establecida en el Decreto Supremo N.º 1793, el cual menciona los siguientes niveles:

- Primer nivel: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes: Entidad Certificadora Raíz.
- Segundo nivel: Entidades Certificadoras.
- Tercer nivel: Agencia de Registro.
- Cuarto nivel: Signatarios.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre cada nivel de la INCD.

### 8.4. Uso de los certificados.

#### 8.4.1. Usos apropiados de los certificados

Los certificados digitales emitidos por la AGETIC en calidad de Entidad Certificadora Pública podrán usarse en los términos establecidos en la normativa vigente relacionada a la Certificación Digital, con las condiciones adicionales establecidas en la Declaración de Prácticas de Certificación, la presente Política de Certificación y cualquier otra normativa vigente que así lo indique.

Los certificados digitales emitidos bajo esta Política de Certificación, pueden ser utilizados bajo los siguientes propósitos:

- Firma de documentos digitales.
- Protección de Correo Electrónico.
- Autenticación en sitio web.
- Firma de código informático.

Para la determinación de los propósitos específicos y el alcance aplicable a cada perfil de certificado, se remitirá a la sección “Usos apropiados del Certificado Digital”, contenida en los siguientes anexos:

- Anexo 1: Particularidades del Certificado Digital de tipo Persona Jurídica.
- Anexo 2: Particularidades del Certificado Digital de tipo Persona Natural."

### 8.4.2. Usos no autorizados de los certificados.

No se permite el uso de certificados digitales cuando este sea contrario a la legislación vigente, a las resoluciones establecidas por la ATT como ente regulador, a lo determinado en la “Declaración de Prácticas de Certificación”, la presente “Política de Certificación” y cualquier otra restricción establecida por el ordenamiento jurídico boliviano.

No se autoriza el uso de certificados digitales para la firma de Listas de Revocación de Certificados (CRLs) o respuestas bajo el protocolo de Estado de Certificado en Línea (OCSP).

Todo uso no autorizado o malintencionado que concluya en un proceso por daños y perjuicios, solamente surte efecto entre los usuarios intervinientes del acto o negocio jurídico. La Entidad Certificadora Pública AGETIC no opera como mediadora, ni entidad sancionadora en ningún caso; únicamente será la entidad encargada de facilitar información y ofrecer servicios que permitan validar la información de los certificados y la integridad de los documentos firmados digitalmente.

Las restricciones y limitaciones de uso adicionales para cada tipo de signatario se encuentran descritas en la sección «Usos no autorizados de los certificados», contenida en los siguientes anexos:

- Anexo 1: Particularidades del Certificado Digital de tipo Persona Jurídica.
- Anexo 2: Particularidades del Certificado Digital de tipo Persona Natural.

## 8.5. Administración de la Política de Certificación.

La responsabilidad de la administración de esta “Política de Certificación” corresponde a la AGETIC en su calidad de Entidad Certificadora Pública.

Cuando la Entidad Certificadora Pública AGETIC realice modificaciones a la presente "Política de Certificación", estas deberán ser remitidas al ente regulador (ATT) con la correspondiente justificación técnica y legal, para su posterior aprobación, socialización y publicación de la nueva versión en su repositorio oficial.

Para consultas y aclaraciones, la Entidad Certificadora Pública AGETIC designa el siguiente contacto:

- Dirección de correo: soporte@firmadigital.bo
- Teléfono: (591-2) 2184026

### 8.6. Definiciones y abreviaturas.

#### 8.6.1. Abreviaturas.

- **AGETIC:** Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación.
- **AR:** Agencia de Registro.
- **ATT:** Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- **CP:** (Certificate Policy) Política de Certificación.
- **CPD:** Centro de Procesamiento de Datos.
- **CPS:** (Certification Practice Statement) Declaración de Prácticas de Certificación.
- **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
- **CSR:** (Certificate Signing Request) Solicitud de Firma de Certificado.
- **DPC:** Declaración de Prácticas de Certificación.
- **EC:** Entidad Certificadora.
- **ECA:** Entidad Certificadora Autorizada.
- **ECR:** Entidad Certificadora Raíz.
- **ECP:** Entidad Certificadora Pública.
- **HSM:** (Hardware Security Module) Módulo de Hardware de Seguridad.
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **INCD:** Infraestructura Nacional de Certificación Digital.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.
- **NIT:** Número de Identificación Tributaria.
- **OCSP:** (Online Certificate Status Protocol) Protocolo de Estado de Certificados en Línea.
- **OID:** (Object Identifier) Identificador de Objeto.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RFC:** (Request For Comments) Requerimiento de comentarios.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **SEGIP:** Servicio General de Identificación Personal.
- **SERECI:** Servicio de Registro Cívico.
- **SHA:** (Secure Hash Algorithm) Algoritmo de Hash Seguro.
- **TIC:** Tecnologías de Información y Comunicación.

- **URI:** (Uniform Resource Identifier) Identificador Uniforme de Recursos.
- **UTF:** (Unicode Transformation Format) Formato de codificación de caracteres.

### 8.6.2. Definiciones

**Autenticación:** Proceso técnico de verificación por el cual se garantiza la identidad del signatario en un mensaje electrónico de datos o documento digital que contenga firma digital.
**Certificado Digital:** Documento digital firmado digitalmente por una Entidad Certificadora Autorizada que incluye datos que permiten identificar al titular del certificado, a la entidad certificadora que lo emitió, el periodo de vigencia e información necesaria para verificar la firma digital.
**Clave privada:** Conjunto de caracteres alfanuméricos generados mediante un sistema de cifrado que contiene datos únicos que el signatario emplea en la generación de una firma electrónica o digital sobre un mensaje electrónico de datos o documento digital.
**Clave pública:** Conjunto de caracteres de conocimiento público, generados mediante el mismo sistema de cifrado de la clave privada, que contiene datos únicos que permiten verificar la firma digital del signatario en el Certificado Digital.
**Caso Fortuito:** Obstáculo interno atribuible al hombre o a terceros vinculados, imprevisto o inevitable, relativo a las condiciones mismas en que la obligación debía ser cumplida (ataque informático, conmociones civiles, huelgas, bloqueos, revoluciones, entre otros).
**Firma digital:** Es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.
**Firma Digital Automática:** Firma Digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en este de acuerdo a las políticas establecidas.
**Fuerza Mayor:** Obstáculo externo, imprevisto o inevitable que origina una fuerza extraña al hombre que impide el cumplimiento de la obligación (incendios, inundaciones y otros desastres naturales).
**Infraestructura de clave pública:** Conjunto de todas las entidades certificadoras, usuarios de los certificados digitales y de las relaciones entre estos actores, organizada de manera jerárquica, encabezada por una entidad certificadora raíz con certificado auto-firmado, y por debajo entidades certificadoras que emiten certificados para los usuarios. En el caso del Estado Plurinacional de Bolivia, la Entidad Certificadora Raíz es la ATT, y la Entidad Certificadora Pública es la AGETIC.
**Lista de certificados revocados:** Archivo digital firmado por una autoridad competente de la PKI que contiene la relación de certificados cuya validez ha sido cancelada o suspendida antes de su fecha de expiración.
**Lista de confianza:** Instrumento técnico-jurídico que establece, mantiene y publica información relativa a las Entidades de Certificación Autorizadas, los certificados raíz de la INCD, así como los certificados emitidos a las Entidades de Certificación

Autorizadas, permitiendo garantizar el reconocimiento de validez de las firmas digitales.

**Módulo criptográfico basado en hardware:** Dispositivo de seguridad basado en hardware (por ejemplo: HSM, token o smartcard) que genera, almacena y protege claves criptográficas, debiendo estar homologado por la ATT de acuerdo a la normativa vigente.

**Nivel de seguridad:** Graduación de la protección del par de claves. Si este es generado por un dispositivo criptográfico basado en hardware, el certificado ostentará un nivel de seguridad alto; si es generado por software, poseerá un nivel de seguridad normal.

**Nota de Débito**: Documento operativo y comercial que detalla los montos de tasas o tarifas a pagar por el solicitante, identificando las cuentas bancarias de la entidad destinadas a la recaudación.

**Par de claves:** Conjunto complementario compuesto por la clave privada y la clave pública, generadas simultáneamente mediante el mismo mecanismo criptográfico.

**Repositorio:** Sitio o sistema de almacenamiento accesible vía web donde se publican las políticas, declaraciones y documentos relacionados al servicio de certificación digital, así como los servicios de consulta de estado de los certificados.

**Servicio OCSP:** Servicio que permite utilizar un protocolo estándar para realizar consultas en línea en tiempo real sobre el estado de validez de un Certificado Digital.

**Signatario:** Persona natural titular de un certificado digital emitido por una entidad certificadora autorizada, que le permite firmar digitalmente.

**Solicitud de firma de certificado (CSR):** Archivo digital que un solicitante transmite a una Entidad Certificadora para obtener la emisión de su certificado, conteniendo su identidad, su clave pública y estando auto-firmado para validar su autenticidad.

**Usuario titular:** Persona natural a nombre de quien se expide el certificado digital (sea para representación propia o de una persona jurídica), titular de los derechos de revocación, reemisión y renovación sobre el mismo.

**Usuario corporativo:** Clasificación administrativa aplicable a entidades públicas o privadas que suscriben contratos o convenios de provisión de servicios de certificación con la AGETIC, habilitándoseles roles para la gestión de solicitudes del personal bajo su dependencia.

## 9. Publicación de información y del repositorio.

### 9.1. Repositorio.

La Entidad Certificadora Pública AGETIC mantiene un repositorio de la documentación en el sitio web:

**https://firmadigital.bo/**

La Entidad Certificadora Pública AGETIC es responsable de mantener su repositorio actualizado y con todos los criterios de seguridad establecidos en las políticas de seguridad, así mismo, dicho repositorio es de acceso público y no contiene información confidencial o privada. El repositorio está disponible durante las 24 horas del día, los 7 días de la semana y en caso de presentarse algún incidente en el sitio web, la AGETIC, aplicará el plan de

contingencias, gestión de incidentes y continuidad del servicio para restablecer nuevamente el sitio web y se encuentre disponible.

Las listas de los certificados emitidos a los signatarios no se hacen públicas en ningún repositorio.

### 9.2. Repositorio CRL.

El Repositorio CRL se encuentra en:
**https://firmadigital.bo/firmadigital_bo3.crl**

### 9.3. Servicio OCSP.

El servicio de consulta OCSP se encuentra en:
**http://www.firmadigital.bo/ocsp3**

### 9.4. Términos y condiciones.

La prestación del servicio de Certificación Digital, se encuentra sujeta y sometida al cumplimiento de los Términos y condiciones ubicados en:
**https://firmadigital.bo/assets/terminos-y-condiciones-del-servicio-2026.pdf**

### 9.5. Políticas de Certificación.

La “Política de Certificación” vigente se encuentra en:
**https://firmadigital.bo/politicas-de-certificacion-2026.pdf**

### 9.6. Declaración de prácticas.

La Declaración de Prácticas de Certificación vigente se encuentran en:
**https://firmadigital.bo/assets/declaracion-de-practicas-de-certificacion-2026.pdf**

### 9.7. Publicación.

La Entidad Certificadora Pública AGETIC proporciona acceso público a la siguiente información:

- Los certificados digitales de la Entidad Certificadora Pública (AGETIC) y de la Entidad Certificadora Raíz (ATT) que constituyen la cadena de confianza de la INCD.
- La Lista de Certificados Revocados (CRL) y los servicios de validación de certificados en línea (OCSP).

- Los documentos públicos de la Entidad Certificadora Pública – AGETIC, que están compuestos por el presente documento y la Declaración de Prácticas de Certificación. La Entidad Certificadora Pública AGETIC mantiene un histórico de las versiones publicadas.
- Cualquier otra información relacionada con el servicio de Certificación Digital (Precios de cada tipo de certificado, manuales de usuario y otra información de interés).

### 9.8. Frecuencia de actualización.

La Entidad Certificadora Pública AGETIC realiza una constante actualización de los repositorios públicos. Al ser información crítica para la seguridad de la infraestructura, la vigencia, emisión y publicación periódica de las CRLs se rige bajo los límites máximos establecidos en la normativa regulatoria vigente, garantizando de forma complementaria la disponibilidad en línea y en tiempo real del servicio OCSP.

### 9.9. Controles de acceso al repositorio.

La Entidad Certificadora Pública AGETIC no restringe el acceso a las consultas del repositorio, sin embargo, para proteger la integridad y autenticidad de la información publicada se cuenta con controles que impiden a personas no autorizadas modificar la información (incluir, actualizar o eliminar datos).

## 10. Identificación y autenticación.

Conforme al estándar X.500, todos los Certificados Digitales requieren un nombre distinguido único. Por lo mismo, no serán admitidos o procesados por la Entidad Certificadora Pública AGETIC los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el usuario titular. En caso de que el titular pertenezca a una población indígena serán considerados los nombres que figuran en la cédula de identidad.

Se garantiza que los nombres de los Certificados Digitales son únicos para cada titular debido a que contienen el atributo del número de documento de identidad y, cuando corresponda, el código de complemento asignado por el SEGIP, elementos que permiten distinguir plenamente las identidades en caso de homonimia.

Para demostrar la identidad del usuario solicitante se solicitará lo siguiente:

- Documento de identidad original y vigente para contrastar los datos con el SEGIP.
- Confirmación física o virtual de la identidad del solicitante o signatario.
- Otros medios de verificación que garanticen la identidad del usuario solicitante y prueba de vida que estén disponibles.

En el documento “Declaración de Prácticas de Certificación” se detalla información sobre la identificación y autenticación de los titulares de los certificados.

### 10.1. Formato del Nombre distinguido.

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos por la AGETIC utilizan codificación UTF-8 para todos los atributos, según la RFC 5280 (“Internet X.509 Public Key Infraestructure and Certificate Revocation List (CRL) Profile”).

### 10.2. Validación de la identidad inicial.

La ECP-AGETIC establece que el proceso de registro y validación de la identidad inicial debe alcanzar un Nivel de Confianza Alto, en correspondencia con los estándares internacionales eIDAS (Nivel Alto) y NIST SP 800-63 (IAL3).

Para garantizar este nivel, las agencias de registro realizarán la validación de la identidad mediante servicios de interoperabilidad con fuentes oficiales (SEGIP u otras fuentes oficiales) y la aplicación de los siguientes métodos:

- **Modalidad Presencial:** Verificación física de la documentación de identidad original frente al titular.
- **Modalidad Virtual:** Verificación remota mediante mecanismos de interacción en tiempo real, tales como videollamadas asistidas por un Oficial de Registro.

En ambas modalidades, es requisito obligatorio la generación y resguardo de evidencia multimedia de la interacción (que podrá consistir en fotografías, videos u otros registros audiovisuales de respaldo) como prueba de fe de vida y constancia del proceso de validación realizado.

**Criterios de Rechazo de Solicitudes:** Se establecen como reglas de cumplimiento obligatorio el rechazo inmediato de una solicitud de certificado en los siguientes escenarios:

- **Inconsistencia de Datos:** Cuando exista falta de coincidencia entre la información declarada por el solicitante y los datos obtenidos de las fuentes oficiales del Estado (SEGIP).
- **Documentación Inválida:** Presentación de documentos de identidad caducados, con alteraciones físicas o que no permitan la identificación plena del titular.
- **Fallo de Identificación en Videollamada:** Se determinará cuando el oficial de registro que atiende la videollamada no pueda confirmar de manera fehaciente que el rostro del usuario coincide con su documento de identidad, o bien, cuando identifique de forma visual un intento de suplantación de identidad.

- **Incumplimiento de requisitos:** La falta de presentación de cualquier requisito adicional específico según el perfil de certificado solicitado (Persona Jurídica o Natural).

Ante cualquiera de estos impedimentos, el Oficial de Registro deberá interrumpir el proceso, registrando el evento y notificando al solicitante la causa técnica o legal del rechazo.

### 10.3. Identificación y autenticación para solicitudes de revocación.

La Entidad Certificadora Pública AGETIC establece que la revocación de un certificado digital es un acto de exclusiva responsabilidad del titular o de los administradores institucionales autorizados. Para garantizar la legitimidad de este proceso, se aplican las siguientes políticas de identificación y autenticación:

- **Exclusividad del Canal Digital:** Toda solicitud de revocación debe ser procesada de manera obligatoria y directa por el solicitante a través del sistema informático oficial de la AGETIC, utilizando mecanismos de autenticación fuerte, credenciales seguras de acceso.
- **Asistencia Presencial Orientativa:** En caso de que el titular se presente físicamente en una Agencia de Registro, el Oficial de Registro limitará sus funciones a guiar, explicar y orientar al usuario sobre el uso de la aplicación informática para que sea el propio titular quien ejecute la acción dentro del sistema. El Oficial de Registro está prohibido de realizar la revocación a nombre del usuario o de intervenir operativamente en su cuenta.
- **Solicitudes de Entidades (Roles Corporativos):** Los representantes o administradores autorizados de las entidades que cuenten con convenios o contratos vigentes con la AGETIC podrá revocar los certificados vinculados a su organización únicamente a través del módulo corporativo del sistema informático, debiendo el sistema registrar de forma automatizada la trazabilidad, identidad del solicitante y la respectiva justificación.

### 10.4. Identificación y autenticación de las solicitudes de renovación de certificado.

La renovación de un certificado digital es el proceso de emisión de un nuevo certificado que mantiene las características de identidad del titular. Las políticas de autenticación para este proceso determinan:

a) **Autenticación en el Sistema Informático:** El trámite de renovación se realizará únicamente por el titular mediante la plataforma o aplicación digital autorizada por la AGETIC. El usuario deberá autenticarse en el sistema utilizando las credenciales de seguridad asignadas o su firma digital vigente.
b) **Condición de Vigencia:** Las renovaciones por el canal digital automatizado son viables únicamente mientras el certificado precedente se encuentre **vigente**. Si el

certificado ha expirado o ha sido revocado, el usuario no podrá renovar y deberá iniciar un proceso completo de validación de identidad para una nueva emisión.

c) **Restricción de la Atención Presencial:** Si el titular acude de forma presencial a una Agencia de Registro para solicitar su renovación, el Oficial de Registro no procesará el trámite en su terminal de soporte; en su lugar, proporcionará la asistencia técnica, manuales e instrucciones necesarias para que el usuario aprenda a utilizar la aplicación y complete la renovación de forma autónoma desde su propio dispositivo o interfaz de usuario.

## 11. Requerimientos Operativos del Ciclo de Vida de los Certificados.

El Parágrafo I del Artículo 12 de la constitución política del estado Plurinacional de Bolivia, establece:

"...
Artículo 12.
I. El Estado se organiza y estructura su poder público a través de los órganos Legislativo, Ejecutivo, Judicial y Electoral. La organización del Estado está fundamentada en la independencia, separación, coordinación y cooperación de estos órganos."

En aplicación del principio de coordinación y cooperación previsto en el Parágrafo I del Artículo 12 de la Constitución Política del Estado, la Entidad Certificadora Pública AGETIC podrá suscribir convenios interinstitucionales con entidades públicas para la designación de servidores públicos como Oficiales de Registro Delegados.

Los Oficiales de Registro Delegados ejercerán las funciones delegadas y estarán sujetos a las mismas obligaciones y responsabilidades que los Oficiales de Registro de la Agencia de Registro de la AGETIC, debiendo cumplir la normativa y los procedimientos aplicables al servicio de Certificación Digital.

La Entidad Certificadora Pública AGETIC será responsable de su capacitación y certificación, conforme a los estándares de calidad y seguridad establecidos.

### 11.1. Requisitos para la obtención de certificado digital.

Los requisitos para la obtención de un Certificado Digital son:
De manera general:

- Documento de Identidad vigente (carnet de identidad o de Extranjero, según corresponda).
- Registro y solicitud de un certificado digital en el sistema de la Agencia de Registro.
- Confirmación física o virtual de la identidad del usuario solicitante.

De manera específica, según el perfil solicitado, existen requisitos adicionales que se encuentran descritos en la sección “Requisitos para la obtención de certificado digital” del Anexo 1 o Anexo 2, según corresponda.

### 11.2. Solicitud del certificado.

Para solicitar un certificado digital, el usuario solicitante debe ser mayor de 18 años. Los titulares pueden obtener más de un Certificado Digital al mismo tiempo.

La solicitud de un Certificado Digital, se inicia desde el sistema de Agencia de Registro, siguiendo los pasos indicados en el mismo. Para completar la solicitud, el usuario solicitante debe presentar los requisitos establecidos según el Perfil de Certificado solicitado; y finalmente se procederá a realizar la confirmación física o virtual de la identidad del usuario solicitante. En caso de ser necesario, el usuario solicitante podrá personarse en alguna Agencia de Registro para asesoramiento.

### 11.3. Generación del par de claves

Al momento de solicitar un Certificado Digital, se podrá definir el nivel de seguridad de acuerdo a la normativa vigente. Según el nivel de seguridad seleccionado, el solicitante podrá generar el par de claves de la siguiente forma:

**Certificados digitales emitidos por dispositivo criptográfico basado en hardware:** El solicitante deberá generar el par de claves (privada y pública) en un dispositivo que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente.

**Certificados digitales emitidos por dispositivo criptográfico basado en software:** El solicitante deberá generar el par de claves (público y privado) por software, en un dispositivo seguro que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente. La Entidad Certificadora Pública AGETIC pone a disposición de los solicitantes un software homologado por la ATT para la generación del par de claves, garantizando la confidencialidad de la información y proporcionando al usuario titular el contenedor PKCS#12.

Es política obligatoria que la generación del par de claves sea realizada bajo el control exclusivo del solicitante. De ser requerido, los Oficiales de Registro brindarán la asistencia técnica y orientación metodológica necesaria para la generación del par de claves, estando estrictamente prohibido que el personal de la Entidad Certificadora intervenga directamente en la manipulación o conocimiento de la clave privada, por tratarse de un acto privado e intransferible.

### 11.4. Procesamiento de la solicitud del Certificado.

La Agencia de Registro, debe realizar un proceso de validación de la identidad del solicitante, verificación de cumplimiento de requisitos y verificación del pago correspondiente. Una vez verificada la solicitud de emisión de certificado digital (CSR), debe ser firmada digitalmente y remitida a la Entidad Certificadora Pública AGETIC a través del Sistema de Agencia de Registro.

Cuando la Agencia de Registro, mediante algún Oficial de Registro, detecte que el usuario solicitante tiene algún impedimento para obtener su certificado digital, no deberá continuar con el proceso y deberá proceder a explicar al solicitante la causa del impedimento y las posibles soluciones.

Las solicitudes creadas se mantendrán en el sistema durante 15 días a la espera de pago o registro de los requisitos que se requieran antes de pasar al estado EXPIRADO. Este estado indica que la solicitud será desestimada y será necesario comunicarse con la Agencia de Registro para volver a habilitarla. La habilitación implica que se generará una nueva nota de débito con las formas de pago recomendadas.

### 11.5. Emisión de certificados.

La Entidad Certificadora Pública AGETIC dispone de procedimientos internos para la ceremonia de Firma Digital de los certificados que son estrictamente aplicados a las solicitudes CSR aprobadas y enviadas por cada Agencia de Registro.

La Entidad Certificadora Pública AGETIC, en cumplimiento de la normativa vigente, tendrá un plazo máximo de 72 horas para la emisión de los certificados digitales una vez recibida la solicitud CSR de la Agencia de Registro, salvo en caso fortuito, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante.

Una vez emitido un Certificado Digital, se lo remitirá al sistema de la respectiva Agencia de Registro donde se realizó el registro de la solicitud. El sistema de Agencia de Registro notificará al usuario titular poseedor de la clave privada que ya puede descargar su certificado correspondiente.

### 11.6. Aceptación del certificado.

Recibida la notificación de la emisión del Certificado Digital, es obligación del usuario titular realizar la importación del certificado digital a su respectivo medio de almacenamiento junto con su clave privada y proceder a firmar el contrato de adhesión; la no realización de estas acciones no afecta el cumplimiento del servicio.

El signatario debe firmar digitalmente el contrato de adhesión al servicio. Para ello tiene un plazo máximo de 120 horas, en caso de no firmar el contrato de adhesión en ese plazo el certificado digital será revocado de manera automática.

Si un Certificado Digital es revocado por no firma de Contrato de Adhesión, la Entidad Certificadora Pública AGETIC podrá emitir un nuevo certificado sin costo alguno y sin afectar el conteo de reemisiones del certificado; siempre y cuando se realice la solicitud por parte del usuario titular. El nuevo certificado reemitido tendrá la vigencia del certificado inicial revocado y no se aplicará ningún tipo de costo adicional.

### 11.7. Usos del certificado.

Los certificados digitales podrán ser utilizados según lo estipulado en la normativa vigente y/o en las Resoluciones Administrativas Regulatorias emitidas por la ATT, para cada tipo de certificado digital que corresponda.

Para determinar el uso del certificado es necesario comprobar el valor de la extensión ‘Key Usage’ del certificado en cuestión.

### 11.8. Solicitud de renovación de certificados.

La renovación de Certificados Digitales se podrá realizar hasta en tres (3) oportunidades consecutivas, siempre y cuando dicha solicitud se ejecute de forma exclusiva a través del sistema informático autorizado mientras el Certificado Digital a ser renovado se encuentre vigente. La solicitud de la cuarta (4ta) renovación del Certificado Digital deberá ser procesada obligatoriamente como una nueva solicitud de emisión.

La vigencia del Certificado Digital obtenido a partir de una renovación será de un (1) año calendario. Para certificados de firma digital automática, la vigencia a partir de una renovación no podrá exceder los dos (2) años calendario.

La renovación del Certificado Digital es de exclusiva responsabilidad y autoría del titular o usuario corporativo. En caso de que el titular acuda de forma presencial a una Agencia de Registro, el Oficial de Registro no operará ni procesará la renovación en su terminal de soporte; limitará sus funciones a proporcionar asistencia técnica, orientación y guías metodológicas para que el usuario complete el proceso de autogestión de forma autónoma desde su propio dispositivo. El sistema informático enviará notificaciones periódicas previas a la expiración del certificado para alertar al titular sobre el estado de su vigencia.

### 11.9. Solicitud de revocación de certificados.

El titular podrá realizar la solicitud de revocación de su certificado digital mediante el sistema informático autorizado de la Agencia de Registro de la AGETIC. Para usuarios vinculados a cuentas corporativas institucionales, la solicitud de revocación podrá ser gestionada a través de su respectivo módulo corporativo por los administradores autorizados.

Se podrá solicitar la revocación de un certificado únicamente mientras este se encuentre en estado vigente, bajo las condiciones y causales políticas establecidas en la Declaración de Prácticas de Certificación.

Como política institucional de la Entidad Certificadora Pública AGETIC, el único canal válido para procesar una revocación es el sistema informático oficial, requiriendo la autenticación fuerte del solicitante o el uso del módulo corporativo automatizado para registrar la trazabilidad inmediata del cambio de estado. En caso de asistencia presencial ante un Oficial de Registro, este actuará exclusivamente como un facilitador metodológico y técnico para orientar al usuario en el uso de la plataforma, quedando estrictamente prohibido que el Oficial de Registro intervenga operativamente en la cuenta o ejecute la acción de revocación a nombre del titular.

### 11.10. Solicitud de reemisión de certificados.

La reemisión de un certificado digital al mismo usuario titular es un procedimiento que no requiere su presencia física, y las condiciones para realizarla son:

- El certificado del titular se encuentre revocado.
- La solicitud se realice en el periodo de vigencia del certificado digital inicial.

Se puede solicitar la reemisión de un certificado en los siguientes casos:

- No supere la cuarta (4) solicitud de reemisión en el periodo de vigencia del certificado, ya sea realizada por el signatario o por el usuario corporativo asociada al Certificado Digital.
- En caso de que se requiera el cambio de alguno de los datos del certificado (Ej. Cambio de usuario titular o cambio de razón social de la entidad).
- En caso de requerir el cambio de modo de uso del Certificado Digital: de firma automática a firma simple, o viceversa.
- En caso de requerir el cambio de nivel de seguridad del Certificado Digital: de nivel normal a nivel alto, o viceversa.
- Cuando se comprueba que alguno de los datos del certificado es incorrecto.
- Cuando se quiera reutilizar un certificado digital revocado que aún se encuentre en un periodo de vigencia válido, y él mismo no se haya reemitido previamente.

El usuario solicitante podrá generar un nuevo par de claves con la nueva solicitud. El periodo de validez del nuevo Certificado será por el lapso restante del periodo de validez del certificado inicial.

El signatario puede solicitar la reemisión de su certificado desde el sistema de Agencia de Registro. Los usuarios corporativos podrán solicitar la reemisión de certificados mediante la cuenta corporativa.

Se podrá realizar una reemisión con cambio de titular; para ello, es necesario que el nuevo titular presente todos los requisitos necesarios y siga los procedimientos como si de una nueva solicitud se tratase, incluyendo la firma de un nuevo **contrato de adhesión**.

Las cuatro (4) reemisiones de Certificados Digitales no tienen ningún costo.

### 11.11. Servicio de estado de los certificados.

La Entidad Certificadora Pública AGETIC posee dos (2) servicios para comprobar el estado de los certificados digitales:

- Publicación de la lista de certificados digitales revocados (CRL), que tiene la finalidad de comprobar si un certificado ha sido revocado. Esta lista se actualiza periódicamente cada 15 minutos siempre y cuando exista una nueva revocación.
- Protocolo de comprobación del Estado de un Certificado (OCSP), disponible en línea 24 horas al día, los 7 días de la semana.

### 11.12. Finalización de la suscripción.

La suscripción del servicio de certificación digital está asociada a la vigencia del certificado digital y finaliza cuando el certificado expira o se solicita su revocación sin posterior reemisión.

### 11.13. Recuperación de la clave.

En casos excepcionales, el personal técnico de la Agencia de Registro brindará asistencia técnica exclusiva al usuario titular para el desbloqueo operativo del dispositivo criptográfico basado en hardware (Token), sin que esto implique en ningún caso el conocimiento, manipulación o control de la clave privada por parte del personal de la AGETIC. La política de recuperación de claves privadas no aplica bajo ninguna circunstancia cuando la clave esté resguardada en un módulo criptográfico de hardware (HSM) o almacenamiento por software; ante la pérdida o compromiso de la clave, el titular deberá proceder obligatoriamente a la reemisión o nueva emisión de un certificado digital mediante la generación de un nuevo par de claves.

### 11.14. Depósito de claves y recuperación.

La Entidad Certificadora Pública AGETIC no realiza, bajo ninguna circunstancia, el depósito, custodia, ni almacenamiento de las claves privadas de los usuarios titulares.

## 12. Controles operacionales o de gestión.

### 12.1. Controles de seguridad física.

Los controles de seguridad física se enmarcan estrictamente en los lineamientos establecidos en la Resolución Administrativa Regulatoria RAR-DJ-RA TL LP 202/2019 emitida por la ATT.

La Entidad Certificadora Pública AGETIC mantiene una política de seguridad física perimetral orientada a mitigar los riesgos de acceso no autorizado, daño e interferencia a las instalaciones que albergan la infraestructura de clave pública. Para ello, se define como política obligatoria la segregación de áreas críticas mediante zonas de seguridad concéntricas, la implementación de mecanismos de autenticación biométrica y el monitoreo continuo para proteger el Centro de Procesamiento de Datos (CPD), las aplicaciones y los servicios criptográficos institucionales.

Las instalaciones de la AGETIC deben contar de forma permanente con sistemas e infraestructura de respaldo ambiental que garanticen la continuidad operativa mediante esquemas de climatización redundante, sistemas de supresión de incendios no destructivos y provisión de energía eléctrica ininterrumpible.

### 12.2. Controles de procedimiento.

Es política mandatoria de la AGETIC que la ejecución de funciones críticas de la infraestructura de firma digital se base en el principio de separación de funciones y segregación de roles de confianza, impidiendo que un solo individuo pueda controlar o vulnerar la integridad de los sistemas criptográficos de forma unilateral.

Las operaciones de alta criticidad, tales como la generación de la llave raíz, la exportación/respaldo de llaves privadas y la inicialización de Módulos de Seguridad de Hardware (HSM), requieren obligatoriamente la aplicación de esquemas de control multipartita bajo la regla de umbral de n de m custodios autorizados. Todos los roles operativos y de confianza dentro de la PKI deben estar formalmente asignados por la máxima autoridad del área técnica competente de la AGETIC, garantizando la trazabilidad e imputabilidad de cada acción de procedimiento.

### 12.3. Controles de seguridad del personal.

Es política obligatoria de la Entidad Certificadora Pública AGETIC asegurar que todo el personal asignado a roles de confianza o con acceso a los sistemas criptográficos posea el más alto grado de idoneidad, competencia técnica, integridad y cualificación profesional para el desempeño de sus funciones.

Todo el personal seleccionado debe someterse de forma obligatoria a una verificación rigurosa de antecedentes penales, judiciales y profesionales previa a su designación, así como a evaluaciones periódicas de cumplimiento y capacitación continua en materia de seguridad informática y PKI. Las acciones que contravengan las políticas de seguridad de la entidad o impliquen un uso no autorizado de los sistemas, serán sujetas de forma inmediata al régimen de sanciones institucionales y a las acciones legales penales o civiles que correspondan bajo el ordenamiento jurídico vigente en el Estado Plurinacional de Bolivia.

### 12.4. Procedimientos de Control de Seguridad.

La Entidad Certificadora Pública AGETIC mantiene una política de registro y auditoría exhaustiva de todos los eventos significativos relacionados con la seguridad, operación y ciclo de vida de los certificados digitales.

Todos los registros de auditoría (logs) generados de manera automatizada por el software de certificación, sistemas operativos, bases de datos y dispositivos de red perimetral, deben ser protegidos mediante controles lógicos estrictos contra modificaciones, borrados, alteraciones o accesos no autorizados. Esta infraestructura garantiza la inmutabilidad, trazabilidad e integridad de la pista de auditoría para fines de control interno y fiscalización posterior por parte de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT). Asimismo, la entidad implementará de forma permanente sistemas de análisis de vulnerabilidades sobre toda la plataforma PKI.

### 12.5. Archivo de información y registros.

La Entidad Certificadora Pública AGETIC garantiza el archivo seguro, la inmutabilidad y la disponibilidad a largo plazo de toda la información y registros relacionados con las solicitudes, validaciones, emisiones y revocaciones de certificados digitales, incluyendo las pistas de auditoría críticas del sistema.

La política de archivo establece que estos registros históricos se conservarán de forma íntegra y bajo estrictas medidas de confidencialidad por el periodo legal mínimo establecido en la normativa regulatoria boliviana vigente. El archivo de información estará estructurado de modo que permita atender de manera oportuna los requerimientos de auditorías externas oficiales y servir como respaldo probatorio legal ante controversias jurídicas, asegurando la verificación de la validez histórica de las firmas digitales emitidas por la entidad.

### 12.6. Cambio de clave de la AGETIC.

La Entidad Certificadora Pública AGETIC cambiará su par de claves bajo las siguientes causales:

- De algún modo se ha visto comprometida la clave privada de la Entidad Certificadora Pública AGETIC.
- Por la caducidad del certificado firmado por la ATT para las operaciones de la Entidad Certificadora Pública AGETIC.
- Por falla o desastre de los equipos necesarios para la firma y que no sea posible habilitar los planes y procedimientos de continuidad del servicio.

### 12.7. Recuperación de la clave de la AGETIC.

La Entidad Certificadora Pública AGETIC establece que su clave privada raíz o subordinada únicamente podrá ser recuperada (reconstituida) en caso de fallas de hardware mediante el uso de las partes del secreto criptográfico compartidas bajo control dual estricto, empleando los dispositivos criptográficos (HSM) autorizados. Este proceso se ejecutará exclusivamente bajo los lineamientos institucionales definidos en los “Planes y Procedimientos para la Continuidad del Servicio y Plan de Contingencias”.

### 12.8. Procedimientos para recuperación de desastres.

La Entidad Certificadora Pública AGETIC mantiene como política prioritaria garantizar la disponibilidad, resiliencia y continuidad operativa de sus servicios críticos de certificación ante contingencias, fallas tecnológicas, desastres naturales o eventos de fuerza mayor.

En caso de un desastre que afecte la infraestructura principal, la entidad se compromete a priorizar de forma inmediata el restablecimiento del servicio de publicación del estado de revocación de certificados (CRL y servicio OCSP), asegurando que el periodo máximo de interrupción no comprometa la seguridad del ecosistema de firma digital del Estado Plurinacional de Bolivia. Todas las operaciones críticas de la entidad, incluyendo los sistemas de respaldo y copias de seguridad de datos de auditoría y bases de datos de certificados, están sujetas a un esquema de redundancia geográfica y lógica rigurosa. Los planes operativos específicos de contingencia ante desastres poseen carácter reservado por razones de seguridad del Estado.

### 12.9. Cese de actividades de la Entidad Certificadora Pública AGETIC.

En caso de un cese planificado o imprevisto de las actividades de la Entidad Certificadora Pública AGETIC, motivado por causales legales, la disolución o modificación del mandato institucional de la entidad, retiro de la autorización por parte del ente regulador, o por fuerza mayor o caso fortuito que impida la continuidad operativa, el procedimiento se regirá estrictamente por lo dispuesto en la Ley N.° 164, el Decreto Supremo N.° 1793 y la normativa

regulatoria vigente emitida por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

La AGETIC garantiza que notificará formalmente a la ATT, a sus usuarios y a las entidades relacionadas con una anticipación mínima de dos (2) meses antes de la fecha prevista para el cese efectivo. Asimismo, la entidad establece la obligatoriedad de revocar todos los certificados digitales vigentes a la fecha del cese y dispone la transferencia segura de la custodia de todos los archivos históricos, registros de auditoría y pistas de verificación a la entidad pública que la normativa legal determine o que la ATT designe, con el fin de preservar la validez histórica de las firmas digitales y garantizar la no afectación a los administrados.

## 13. Controles de Seguridad Técnica.

### 13.1. Generación e instalación de par de claves

La Entidad Certificadora Pública AGETIC garantiza que la generación de sus pares de claves se realiza mediante procedimientos seguros y controlados, utilizando algoritmos criptográficos robustos reconocidos internacionalmente y longitudes de clave que aseguran su resistencia frente a ataques de computación y criptoanálisis durante su periodo de vigencia.

En el documento “Declaración de Prácticas de Certificación” se detalla procedimentalmente la generación del par de claves de la Entidad Certificadora Pública AGETIC, la gestión del par de claves, tamaño de claves, parámetros de generación de clave pública, hardware y software de generación de claves y los fines de uso de las claves.

### 13.2. Protección de la clave privada.

La Entidad Certificadora Pública AGETIC posee una copia de seguridad de su clave privada bajo las mismas condiciones de seguridad que la original, comprometiéndose a resguardar su confidencialidad e integridad mediante el uso de hardware criptográfico de alta seguridad y esquemas de control multipersonal.

En el documento “Declaración de Prácticas de Certificación” se detalla operativamente la información sobre los módulos criptográficos, su gestión, sus controles y custodia.

### 13.3. Otros aspectos de la gestión del par de claves.

La Entidad Certificadora Pública AGETIC establece el uso exclusivo de los pares de claves asignados a sus funciones específicas de confianza y determina límites temporales estrictos para la validez operativa de los certificados y el uso de las claves criptográficas, con el fin de mitigar riesgos de compromiso.

En el documento “Declaración de Prácticas de Certificación” se detallan los aspectos técnicos y operativos generales del par de claves, los periodos operativos de los certificados y el período de uso para el par de claves.

### 13.4. Datos de activación.

La Entidad Certificadora Pública AGETIC dispone de procedimientos para la generación de la clave privada del módulo criptográfico, basado en un procedimiento multipersonal, donde solo el personal autorizado posee las claves necesarias descritas en estos procedimientos.

### 13.5. Controles de seguridad informática.

La Entidad Certificadora Pública AGETIC tiene definida una serie de controles de seguridad aplicables a los equipos informáticos, tales como el uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y pruebas de seguridad.

El acceso a los sistemas de la Entidad Certificadora Pública AGETIC está restringido al personal autorizado según los roles asignados, bajo los procedimientos y controles establecidos.

### 13.6. Controles de seguridad del ciclo de vida.

El software de la Entidad Certificadora Pública AGETIC que utiliza la clave pública para la emisión de los certificados y el manejo del ciclo de vida ha sido desarrollado de acuerdo con los requerimientos de la Resolución Administrativa de la ATT-DJ-RA TL LP 202/2019.

El HSM utilizado por la Entidad Certificadora Pública AGETIC para firmar los Certificados cumple con los requerimientos FIPS 140-2. Los controles para el manejo de la seguridad se cumplen mediante una separación adecuada de roles mismos que definen el cumplimiento de los requerimientos descritos en la política de seguridad establecida, durante todo el ciclo de vida de las claves se tienen implementados controles de seguridad permitiendo instrumentar y auditar cada fase de los sistemas de la Entidad Certificadora Pública AGETIC.

Existen controles de seguridad para la operativa y el ciclo de vida de los sistemas de la entidad, incluyendo:

a) Registro y reporte de acceso físico
b) Registro y reporte de acceso lógico.
c) Procedimientos de actualización e implementación de sistemas

### 13.7. Controles de seguridad de la red.

El hardware y software para la infraestructura de clave pública de la Entidad Certificadora Pública AGETIC para la emisión de certificados digitales están sujetos a estrictos controles de seguridad y únicamente son accesibles desde la red interna de la Unidad de Infraestructura Tecnológica (UIT). La red se encuentra segmentada y protegida por firewalls en alta disponibilidad, los sistemas de información están protegidos contra virus y software malicioso.

La infraestructura tecnológica necesaria para el procedimiento de Certificación Digital tiene implementado un sistema de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso.

### 13.8. Controles de módulos criptográficos.

La Entidad Certificadora Pública AGETIC únicamente utiliza módulos criptográficos bajo el estándar FIPS 140-2 nivel 3.

### 13.9. Sincronización horaria.

El gabinete de la firma digital de la Entidad Certificadora Pública AGETIC que contiene la infraestructura de clave pública se mantiene "off-line", por lo que, la sincronización horaria en línea no se lleva a cabo.

## 14. Perfil de los Certificados, CRL y OCSP.

### 14.1. Perfil de Certificado según tipo del certificado.

La ATT es la entidad encargada de definir y delimitar los Tipos de Certificado a emitirse por las Entidades Certificadoras Autorizadas. Según el tipo de Certificado digital solicitado por cada usuario, el perfil varía en cumplimiento a normativa y reglamentación vigente.

Los perfiles de cada tipo de Certificado se encuentran especificados en reglamentación vigente, publicadas en el portal de la ATT, en su rol de Entidad Certificadora Raíz: https://ecrb.att.gob.bo/

Asimismo, los perfiles de los certificados digitales emitidos por la Entidad Certificadora Pública AGETIC se encuentran detallados en las siguientes secciones del presente documento:

- **Anexo 1:** Secciones “Formato para Certificado Digital de tipo Persona Jurídica” y “Extensión para Certificado Digital de tipo Persona Jurídica”.
- **Anexo 2:** Secciones “Formatos para los Certificados Digitales para persona natural o Física” y “Extensión para Certificado Digital persona natural”.

### 14.2. Perfil del Certificado de la Entidad Certificadora Raíz (ECR) ATT

La Entidad de Certificación Pública de la AGETIC reconoce, adopta y se subordina políticamente al perfil de certificado establecido por la Entidad Certificadora Raíz (ECR) administrada por la ATT, asegurando la total interoperabilidad técnica y legal dentro de la Infraestructura Nacional de Certificación Digital. El documento “Declaración de Prácticas de Certificación” detalla la composición técnica y campos específicos del perfil del Certificado de la Entidad Certificadora Raíz (ECR).

### 14.3. Perfil del Certificado de la Entidad Certificadora Pública AGETIC

La AGETIC establece que todos los certificados digitales emitidos bajo su infraestructura técnica deben cumplir estrictamente con el estándar internacional ITU-T X.509 versión 3 y las recomendaciones del RFC 5280, incorporando de forma obligatoria las extensiones críticas y no críticas exigidas por la regulación sectorial boliviana para garantizar su validez jurídica. En el documento “Declaración de Prácticas de Certificación” se detalla el mapa de bits, extensiones, OIDs y la estructura técnica detallada del perfil del Certificado de la Entidad Certificadora Pública AGETIC.

### 14.4. Perfiles de la CRL

La ECP-AGETIC garantiza la publicación de Listas de Revocación de Certificados (CRL) que cumplen estrictamente con el estándar ITU-T X.509 v2 y el perfil definido en el RFC 5280. Es política institucional asegurar que las CRLs contengan de forma inequívoca el número de serie de los certificados revocados, la fecha y hora de la revocación, y la firma digital de la entidad emisora para garantizar su integridad.

La estructura técnica detallada de los campos y las extensiones específicas utilizadas se encuentran definidas en el documento "Declaración de Prácticas de Certificación”.

### 14.5. Perfiles de la OCSP

La ECP-AGETIC establece que el servicio de respuesta de estado de certificados en línea seguirá el protocolo OCSP conforme al RFC 6960. La política de la entidad asegura que

todas las respuestas OCSP sean firmadas mediante un certificado dedicado para tal fin, garantizando que los terceros que confían reciban información veraz y actualizada en tiempo real sobre la validez de los certificados.

Los parámetros técnicos de las solicitudes, respuestas y extensiones del protocolo se detallan en el documento "Declaración de Prácticas de Certificación"

El certificado utilizado para la verificación de una respuesta OCSP contiene en el campo “extendedKeyUsage” con el valor “id-kp-OCSPSigning”, cuyo OID es 1.3.6.1.5.5.7.3.9.

## 15. Administración Documental.

La responsabilidad de la administración de esta “Política de Certificación” corresponde a la Entidad Certificadora Pública AGETIC.

La publicación de las revisiones de esta “Política de Certificación” deberá ser presentada a la ATT **para su aprobación previa.**

### 15.1. Procedimiento para cambio de especificaciones.

La Entidad Certificadora Pública AGETIC cuenta con procedimientos internos para la administración de los cambios sobre la presente Política de Certificación.

En caso de que la Entidad Certificadora Pública AGETIC desee realizar alguna corrección o modificación en la presente política, deberá realizar la solicitud a la ATT con la correspondiente justificación. La ATT evaluará la solicitud y, en caso de aprobar mediante la resolución correspondiente, la Entidad Certificadora Pública AGETIC procederá a la actualización del documento, control de versiones y posterior publicación de la nueva versión en su repositorio oficial.

### 15.2. Frecuencia de actualización

La revisión de la “Política de Certificación”, se realiza en base a la experiencia institucional de la Entidad Certificadora Pública AGETIC en su aplicación, a la efectividad y oportunidad de sus procesos, su interrelación con otros sistemas, la dinámica administrativa y la situación de la normativa vigente. Producto de la revisión, se podrá actualizar el documento para que sea presentado a la ATT con fines de aprobación.

### 15.3. Procedimiento de Publicación y Notificaciones

La Entidad Certificadora Pública AGETIC presentará a la ATT las modificaciones solicitadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos reemplazados. Una vez aprobadas, se procederá junto con la publicación de la nueva versión.

La Entidad Certificadora Pública AGETIC deberá notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación. De la misma forma, la Entidad Certificadora Pública deberá publicar en su sitio web cualquier modificación aprobada por la ATT y notificar a los usuarios finales de los cambios realizados.

En ningún caso la Entidad Certificadora Pública AGETIC será responsable por la pérdida de las comunicaciones enviadas al titular, cuando esta situación sea atribuible a la inexactitud, falta de actualización o error en los datos de contacto (correo electrónico, teléfono, otros) suministrados por el propio usuario.

## 16. Otras cuestiones legales y de actividad.

### 16.1. Contrato de adhesión.

Los certificados emitidos por la Entidad Certificadora Pública AGETIC, están asociadas a la aceptación del Contrato de Adhesión del servicio, el mismo que está interpretado como un contrato condicional y sus características son:

- La eficacia o la resolución de un contrato puede estar subordinada a un acontecimiento futuro e incierto.
- Toda condición debe cumplirse de la manera que las partes han querido y entendido que se cumpla.

El contrato de adhesión debe firmarse digitalmente en el plazo establecido en el punto 4.6, caso contrario se procederá a la resolución del contrato y a la consecuente revocación automática del certificado digital correspondiente.

### 16.2. Tarifas.

Las tarifas establecidas para la emisión de Certificados Digitales están enmarcadas bajo la normativa vigente, y serán publicadas en el sitio web de la Entidad Certificadora Pública AGETIC.

#### 16.2.1. Pago y Facturación.

Para realizar el pago del certificado digital, la Entidad Certificadora Pública AGETIC brinda diversas modalidades de pago, mismas se encuentran disponibles en el sitio web de la Entidad Certificadora Pública, asimismo la forma de pago recomendada se establecerá en la nota de débito que sea generado en el momento de la solicitud del certificado.

La Entidad Certificadora Pública AGETIC, emite facturas electrónicas a nombre y número de identificación tributaria definida por el titular, una vez emitido el certificado digital. En caso de cuentas corporativas la factura electrónica será emitida según coordinación realizada entre partes.

#### 16.2.2. Reembolso.

La Entidad Certificadora Pública, realizará reembolsos a depósitos realizados por aquellos servicios no prestados, considerando los siguientes aspectos:

- Exista una solicitud formal por parte del depositante,
- No se hubiera emitido un certificado asociado a la nota de débito o comprobante.

Todo depósito no asociado a una solicitud de emisión de certificado digital que no sea utilizado en un plazo de noventa (90) días calendario será considerado como "depósito no identificado"; durante ese tiempo el depositante podrá solicitar su utilización en la emisión de certificados digitales. Concluido ese plazo será registrado como Otros Ingresos de la Entidad Certificadora Pública AGETIC y podrá ser sujeto de restitución a requerimiento del depositante.

Los depósitos "no identificados" serán publicados en el sitio web de la Entidad Certificadora Pública AGETIC por un lapso de 60 (sesenta) días calendario.

### 16.3. Política de confidencialidad.

Toda la recopilación y uso de la información compilada por la Entidad Certificadora Pública AGETIC es realizada cumpliendo con la normativa vigente relacionada a certificación digital y protección de datos cumpliendo lo descrito en el artículo 56 del Decreto Supremo N.º 1793, basándose en las distinciones suministradas en el documento de Declaración de Prácticas de Certificación.

### 16.4. Ámbito de la Información confidencial.

La Entidad Certificadora Pública AGETIC considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial a no ser que exista una imposición legal.

### 16.5. Protección de Datos Personales.

La Entidad Certificadora Pública AGETIC garantiza el derecho a la privacidad y la protección de los datos personales de los solicitantes y titulares, en estricto cumplimiento del Artículo 56 del Decreto Supremo N° 1793.

El tratamiento de la información de carácter privado se rige bajo los siguientes lineamientos:

- **Respeto a Derechos Fundamentales:** El tratamiento de los datos personales se realizará respetando los derechos y garantías establecidos en la Constitución Política del Estado.
- **Consentimiento Expreso e Informado**: Toda actividad de recolección y uso de datos requiere del conocimiento previo y el consentimiento expreso del titular. Dicho consentimiento se obtiene de manera formal mediante la suscripción del Contrato de Adhesión y la aceptación de los Términos y Condiciones del Servicio.
- **Transparencia y Finalidad Pública**: Los datos personales no podrán ser utilizados para finalidades distintas a las expresadas al momento de su registro. Se informa al titular que, por la naturaleza técnica del servicio y para permitir la identificación unívoca del signatario ante terceros, los datos de Nombre Completo y Número de Documento de Identidad (C.I.) son de carácter público y se encuentran incorporados en el certificado digital, así como en los servicios de consulta de estado de revocación CRL y OCSP.
- **Ejercicio de Derechos**: Se garantiza a los titulares la posibilidad de ejercer sus derechos de acceso, rectificación, actualización, cancelación, objeción y revocación de sus datos personales ante la ECP-AGETIC.
- **Seguridad, Confidencialidad e Integridad**: La AGETIC adoptará las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos y evitar su alteración o tratamiento no autorizado. Ninguna información de carácter privado será revelada o comercializada a terceros, salvo consentimiento expreso o mandato judicial fundamentado.

Los presentes lineamientos están estrictamente alineados al Contrato de Adhesión suscrito por el titular. La firma de dicho instrumento constituye la manifestación de voluntad y el consentimiento informado del usuario para el tratamiento de sus datos conforme a ley.

En el documento “Declaración de Prácticas de Certificación” se detallan los mecanismos técnicos y operativos para salvaguardar dicha información.

### 16.6. Derechos y Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital.

#### 16.6.1. Derechos y Obligaciones de la Entidad Certificadora Pública.

##### 16.6.1.1. Derechos de la Entidad Certificadora Pública.

La Entidad Certificadora Pública AGETIC tiene derecho a exigir a los solicitantes y titulares el cumplimiento estricto de los requisitos legales y técnicos vigentes, a suspender o revocar certificados de oficio ante la verificación de causales normativas, y rechazar las solicitudes de emisión que no se ajusten a la presente Política de Certificación. En el documento “Declaración de Prácticas de Certificación” se detalla de forma operativa el ejercicio de estos derechos.

##### 16.6.1.2. Obligaciones de la Entidad Certificadora Pública.

La Entidad Certificadora Pública AGETIC se obliga a operar la infraestructura tecnológica y proveer los servicios de certificación digital en estricto cumplimiento de la Ley N.° 164, el Decreto Supremo N.° 1793 y las directrices de la ATT; a mantener la disponibilidad permanente del repositorio público, el estado de vigencia y revocación de certificados (CRL y OCSP); y garantizar el resguardo e integridad absoluta de sus claves privadas operativas. En el documento “Declaración de Prácticas de Certificación” se detalla el procedimiento técnico de ejecución de estas obligaciones.

##### 16.6.1.3. Derechos y Obligaciones de la Entidad Certificadora Pública y ante Terceros que confían.

La Entidad Certificadora Pública AGETIC tiene la obligación de poner a disposición de los Terceros que confían mecanismos de consulta gratuitos para verificar la validez de los certificados emitidos. Los terceros que confían tienen la obligación de comprobar el estado de vigencia, revocación y las restricciones de uso del certificado digital antes de asegurar su confianza en una firma. En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los métodos técnicos asociados.

##### 16.6.1.4. Obligaciones de la Entidad Certificadora Pública ante Corte del Servicio

En caso de interrupción programada o imprevista del servicio, la Entidad Certificadora Pública AGETIC tiene la obligación de ejecutar los planes de contingencia aprobados, notificar inmediatamente a la ATT y desplegar avisos públicos dirigidos a los usuarios para mitigar impactos. En el documento “Declaración de Prácticas de Certificación” se detallan los procedimientos operativos y plazos ante el corte del servicio.

### 16.6.2. Derechos y Obligaciones de los Titulares del Certificado Digital.

Según lo establecido en el Artículo 52 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, son titulares de la firma digital y del certificado digital las personas que hayan solicitado por sí y para sí una certificación que acredite su firma digital.

#### 16.6.2.1. Responsabilidad del titular.

El titular es el único y exclusivo responsable de la generación segura, el resguardo confidencial y el control del dispositivo de creación de firma que contiene su clave privada, asumiendo total responsabilidad legal por las firmas generadas. En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre la Responsabilidad del Titular.

#### 16.6.2.2. Derechos del Titular del Certificado.

El titular tiene derecho a recibir el servicio bajo los estándares de seguridad normados, a exigir la confidencialidad de sus datos y a solicitar la revocación inmediata de su certificado digital en cualquier momento. En el documento “Declaración de Prácticas de Certificación” se detalla el procedimiento correspondiente.

#### 16.6.2.3. Obligaciones del Titular del certificado.

El titular está obligado a proporcionar información verídica y exacta durante su registro, a utilizar el certificado únicamente para los fines permitidos en esta política, y a solicitar de forma inmediata la revocación de su certificado digital ante cualquier sospecha de pérdida, robo o compromiso de confidencialidad de su clave privada. En el documento “Declaración de Prácticas de Certificación” se detallan las pautas operativas asociadas.

### 16.6.3. Derechos y Obligaciones de los Usuarios.

#### 16.6.3.1. Derechos de las usuarias y usuarios.

Los usuarios y terceros que confían tienen derecho a acceder libremente a la información pública del repositorio de la Entidad Certificadora y a consultar el estado de validez de cualquier certificado emitido por la AGETIC. En el documento “Declaración de Prácticas de Certificación” se detalla más información.

#### 16.6.3.2. Obligaciones de las usuarias y usuarios.

Los usuarios y terceros están obligados a verificar la validez técnica de la firma digital, la cadena de certificación y el estado de revocación del certificado a través de los servicios CRL u OCSP proporcionados por AGETIC antes de dar validez al acto jurídico. En el documento “Declaración de Prácticas de Certificación” se detalla el procedimiento técnico.

### 16.7. Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital.

Todos los participantes del ecosistema quedan obligados al cumplimiento irrestricto de las condiciones técnicas fijadas en la normativa boliviana y en la presente política. En el documento “Declaración de Prácticas de Certificación” se detalla de manera específica el alcance procedimental de estas obligaciones.

### 16.8. Infracciones y Sanciones.

Las infracciones y sanciones son establecidas por la Autoridad que regula el servicio que brinda la Entidad Certificadora Pública AGETIC.

### 16.9. Resolución de Conflictos.

Toda controversia derivada del presente documento procurará resolverse mediante negociación entre el titular y la Entidad Certificadora Pública AGETIC, dentro del plazo de quince (15) días hábiles.

De no alcanzarse un acuerdo, el titular podrá presentar su reclamación ante la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), en el marco de sus competencias.

Sin perjuicio de lo anterior, quedará expedita la vía legal correspondiente.
La Entidad Certificadora Pública AGETIC, salvo orden emitida por autoridad competente, no intervendrá en la resolución de controversias derivadas del uso del certificado digital entre los titulares y terceros.

El personal de la Entidad Certificadora Pública AGETIC no tendrá acceso a la clave privada de los titulares; en consecuencia, no será responsable por su compromiso, uso indebido o las consecuencias derivadas de ello.

### 16.10. Legislación aplicable.

Las Políticas de Certificación de la Entidad Certificadora Pública AGETIC se sustentan en la siguiente normativa:

- Constitución Política del Estado.
- Ley N.º 164, General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- Decreto Supremo N.º 2514, de creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), y sus modificaciones.
- Decreto Supremo N.º 1793, que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Decreto Supremo N.º 3527, que modifica el Decreto Supremo N.º 1793, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Las recomendaciones de la RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Asimismo, se consideraron las Resoluciones Administrativas Regulatorias emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), en el marco de sus competencias establecidas por la Ley N.º 164:

- ATT-DJ-RAR-TL LP 272/2017, Estándar Técnico para el Funcionamiento de Agencias de Registro.
- ATT-DJ-RA TL LP 245/2018, Documentos Públicos de la Entidad Certificadora Raíz.
- ATT-DJ-RA TL LP 202/2019, Requisitos y otros aspectos para la prestación del servicio de Certificación Digital.
- ATT-DJ-RA TL LP 209/2019, Estándar Técnico para la Emisión de Certificados Digitales.
- ATT-DJ-RAR-TL LP 357/2020, Modificación al "Estándar Técnico para la Emisión de Certificados Digitales".

### 16.11. Conformidad con la ley aplicable.

Todos los procesos, procedimientos y la información técnica y legal contenida en la presente Política de Certificación se encuentran elaborados de conformidad con la normativa legal vigente y las Resoluciones Administrativas Regulatorias emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), en el marco de sus competencias.

## ANEXO 1: Particularidades del Certificado Digital de tipo Persona Jurídica

### Usos apropiados del Certificado Digital

Se permite el uso de estos certificados digitales, en las relaciones del titular en representación de una entidad con particulares mediante la firma digital y el uso de sistemas que estén adecuados para el uso de la firma digital. El propósito principal es vincular la identidad del signatario con la personería jurídica de la entidad que representa, garantizando la integridad y el no repudio en transacciones institucionales.

Un certificado digital de tipo Persona Jurídica tendrá los usos permitidos y limitaciones de acuerdo a normativa vigente.

### Usos no autorizados de los certificados de persona jurídica.

Los certificados de Persona Jurídica no podrán utilizarse para trámites de carácter estrictamente personal del titular que no guarden relación con sus funciones o atribuciones dentro de la entidad representada.

Asimismo, queda prohibido su uso para la firma de Listas de Revocación de Certificados (CRL) o respuestas OCSP.

### Requisitos para la obtención de certificado digital.

Además de los requisitos generales establecidos en la sección 4.1 del cuerpo principal, para el tipo Persona Jurídica se requiere:

- Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributaria) del solicitante vigente.
- Nota de Autorización original para el solicitante, firmada por la Máxima Autoridad Ejecutiva o el Representante Legal de la Empresa.
- Documento vigente y legalmente aplicable en el que se establezca la relación laboral entre la empresa o entidad y el solicitante.
- Validación de Identidad: Conforme a la sección 3.2 de esta Política, se realizará la confirmación de identidad mediante modalidad presencial o modalidad virtual asistida (videollamada). En ambos casos, es obligatoria la generación de evidencia multimedia de la interacción (fotografía o grabación) como respaldo de la prueba de vida

  En función al nivel de seguridad, deberá contar:

- **Para Certificados Digitales con seguridad alta:** Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2 nivel 2 mínimamente. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web (https://www.att.gob.bo/homologados). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud
- **Para Certificados Digitales con seguridad normal:** Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos. La Entidad Certificadora Pública AGETIC provee una herramienta homologada por la ATT para la generación del par de claves por software, misma que puede ser encontrada en:

**https://firmadigital.bo**

**Formato para Certificado Digital de tipo Persona Jurídica**

El formato para los certificados digitales para persona jurídica tanto de seguridad alta como normal (generación de par de claves en dispositivo de seguridad hardware o software) deben cumplir con la siguiente estructura:

| NOMBRE | DESCRIPCIÓN |
|---|---|
| Versión (version) | 2 |
| Número de Serie (serialNumber) | Número asignado por la Entidad Certificadora Pública AGETIC |
| Algoritmo de firmas (signatureAlgorithm) | OID: 1.2.840.113549.1.15 (SHA256withRSA) |
| Nombre del Emisor (issuer) | **CN** = “Entidad Certificadora” y el nombre de la Entidad Certificadora Pública ;<br>**O** = Razón social de la Entidad Certificadora Pública;<br>**C**=BO (de acuerdo a ISO3166). |
| Periodo de validez (validity) | Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time) |
| Nombre suscriptor (subject) | **CN** = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones;<br>**O** = Razón social de la empresa o institución a la que representa la persona jurídica; |

| | |
|---|---|
| | **OU** = Unidad Organizacional de la que depende (opcional);<br>**T** = Cargo del representante legal;<br>**C** = estándar de acuerdo con ISO 3166 {BO};<br>**dnQualifier** = Tipo de documento {CI/CE};<br>**uidNumber** = Nro. de documento {numeral};<br>**uid** = número de complemento {alfanumérico} (opcional);<br>**serialNumber** = Número de NIT {numeral} (opcional);<br>**description** = Nivel de seguridad. |
| Clave pública del suscriptor (subjectPublicKey) | Algoritmo: RSA, Longitud: mínimo 2048 bits |

El campo Descripción (description) puede tomar uno de los siguientes valores:

| Campo Descripción (description) | Normativa |
|---|---|
| Persona Jurídica Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| Persona Jurídica Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |
| Persona Jurídica Seguridad Normal Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| Persona Jurídica Seguridad Normal Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |

**Extensión para Certificado Digital de tipo Persona Jurídica.**

Las extensiones del Certificado Digital de una Persona Jurídica serán las siguientes:

| NOMBRE | DESCRIPCIÓN |
|---|---|
| Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier) | Valor de la Extensión subjectKeyIdentifier del certificado de la Entidad Certificadora Pública AGETIC |
| Identificador de la clave del suscriptor (subjectKeyIdentifier) | Función Hash (SHA1) del atributo subjectPublicKey |
| Uso de Claves (keyUsage) | ddigitalSignature = 1,<br>nonRepudiation = 1,<br>keyEncipherment = 1,<br>dataEncipherment = 1,<br>keyAgreement = 0,<br>keyCertSign = 0,<br>cRLSign = 0, |

| | |
|---|---|
| | encipherOnly = 0,<br>decipherOnly = 0. |
| Uso de Claves Extendido (Extended Key Usage) | clientAuth, EmailProtection, codeSigning |
| Política de Certificación (certificatePolicies) | URI: (archivo en formato de texto)<br><br>**Identificador de Objeto**= OID del certificado {alfanumérico} |
| Restricciones Básicas (basicConstraints) | CA = FALSE |
| Punto de distribución de las CRL (cRLDistributionPoints) | URI: (.crl) |
| Información de Acceso de la ECA (authorityInformationAccess) | URI:(.crt) |
| Nombre Alternativo del Suscriptor (subjectAlternativeName) | E = Correo electrónico del suscriptor |

El campo Política de Certificación (certificatePolicies), además de contener la dirección de la Política de Certificación, debe contener el OID del tipo de Certificado relacionado al campo Descripción (description) y puede tomar los siguientes valores:

| Campo Descripción (description) | Normativa |
|---|---|
| **2.16.68.0.0.0.1.14.1.2.0.1.2.1.0.0**<br>Persona Jurídica Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.1.0.1**<br>Persona Jurídica Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.0**<br>Persona Jurídica Seguridad Normal Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.1**<br>Persona Jurídica Seguridad Normal Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |

## ANEXO 2: Particularidades del Certificado Digital de tipo Persona Natural

### Usos apropiados del Certificado Digital

Se permite el uso de estos certificados digitales, en las relaciones del titular con particulares mediante la firma digital, y el uso de sistemas que estén adecuados para el uso de la firma digital.

Un certificado digital de tipo Persona Natural tendrá los usos permitidos y limitaciones de acuerdo a normativa vigente.

### Usos no autorizados de los certificados.

Los certificados digitales de tipo Personal Natural sólo pueden ser utilizados conforme a normativa y reglamentación vigente.

### Requisitos para la obtención de certificado digital.

Los requisitos para la obtención de un Certificado Digital de tipo Persona Natural son:

- Última factura de pago de luz, agua o teléfono u otro servicio que permita verificar su dirección actual del titular o solicitante. La dirección podrá referirse a su domicilio real o laboral.
- Validación de Identidad: Conforme a la sección 3.2 de esta Política, se realizará la confirmación de identidad mediante modalidad presencial o modalidad virtual asistida (videollamada). En ambos casos, es obligatoria la generación de evidencia multimedia de la interacción (fotografía o grabación) como respaldo de la prueba de vida

  En función al nivel de seguridad, deberá contar:

  - **Para Certificados Digitales con seguridad alta:** Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2 nivel 2 mínimamente. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web (https://www.att.gob.bo/homologados). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud
  - **Para Certificados Digitales con seguridad normal:** Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave

privada para permitir la firma de documentos. La Entidad Certificadora Pública AGETIC provee una herramienta homologada por la ATT para la generación del par de claves por software, misma que puede ser encontrada en:

**https://firmadigital.bo**

Se debe resaltar que la dirección declarada por el usuario solicitante debe ser similar a la que se encuentra descrita en la factura del servicio que se presenta como parte de los requisitos.

**Formatos para los Certificados Digitales para persona natural o Física**

El formato para los certificados digitales para persona natural debe cumplir con la siguiente estructura

| NOMBRE | DESCRIPCIÓN |
|---|---|
| Versión (versión) | 2 |
| Número de Serie (serialNumber) | Número asignado por la Entidad Certificadora Pública AGETIC |
| Algoritmo de firmas (signatureAlgorithm) | OID: 1.2.840.113549.1.15 (SHA256withRSA) |
| Nombre del Emisor (issuer) | **CN** = “Entidad Certificadora” y el nombre de la Entidad Certificadora Pública;<br>**O** = Razón social de la Entidad Certificadora Pública;<br>**C**=BO (de acuerdo a ISO3166). |
| Periodo de validez (validity) | Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time) |
| Nombre suscriptor (subject) | **CN** = Nombres y Apellidos de la persona natural;<br>**C** = estándar de acuerdo con ISO 3166 {BO};<br>**dnQualifier** = Tipo de documento {CI/CE};<br>**uidNumber** = Nro. de documento {numeral};<br>**uid** = número de complemento {alfanumérico} (opcional);<br>**serialNumber** = Número de NIT {numeral} (opcional);<br>**description** = Nivel de seguridad. |
| Clave pública del suscriptor (subjectPublicKey) | Algoritmo: RSA, Longitud: mínimo 2048 bits |

El campo Descripción (description) puede tomar uno de los siguientes valores:

| Campo Descripción (description) | Normativa |
|---|---|

| | |
|---|---|
| Persona Natural Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| Persona Natural Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |
| Persona Natural Seguridad Normal Firma Simple | RAR **ATT-DJ-RAR-TL LP 357/2020** |
| Persona Natural Seguridad Normal Firma Automática | RAR **ATT-DJ-RAR-TL LP 357/2020** |

**Extensión para Certificado Digital persona natural**

Las extensiones del Certificado Digital de una Persona Natural o Física serán las siguientes:

| NOMBRE | DESCRIPCIÓN |
|---|---|
| Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier) | Valor de la Extensión subjectKeyIdentifier del certificado de la Entidad Certificadora Pública AGETIC |
| Identificador de la clave del suscriptor (subjectKeyIdentifier) | Función Hash (SHA1) del atributo subjectPublicKey |
| Uso de Claves (keyUsage) | digitalSignature = 1,<br>nonRepudiation = 1,<br>keyEncipherment = 1,<br>dataEncipherment = 1,<br>keyAgreement = 0,<br>keyCertSign = 0,<br>cRLSign = 0,<br>encipherOnly = 0,<br>decipherOnly = 0. |
| Uso de Claves Extendido (Extended Key Usage) | clientAuth, EmailProtection, codeSigning |
| Política de Certificación (certificatePolicies) | URI: (archivo en formato de texto)<br><br>Identificador de Objeto= OID del certificado {alfanumérico} |
| Restricciones Básicas (basicConstraints) | CA = FALSE |
| Punto de distribución de las CRL (cRLDistributionPoints) | URI: (.crl) |

| | |
|---|---|
| Información de Acceso de la ECA (authorityInformationAccess) | URI:(.crt) |
| Nombre Alternativo del Suscriptor (subjectAlternativeName) | E = Correo electrónico del suscriptor |

El campo Política de Certificación (certificatePolicies), además de contener la dirección de la Política de Certificación, debe contener el OID del tipo de Certificado relacionado al campo Descripción (description) y puede tomar los siguientes valores:

| Campo Política de Certificación (certificatePolicies) | Normativa |
|---|---|
| **2.16.68.0.0.0.1.14.1.2.0.1.2.1.1.0** Persona Natural Firma Simple | RAR ATT-DJ-RA TL LP 209/2019 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.1.1.1** Persona Natural Firma Automática | RAR ATT-DJ-RA TL LP 209/2019 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.0** Persona Natural Seguridad Normal Firma Simple | RAR ATT-DJ-RAR-TL LP 357/2020 |
| **2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.1** Persona Natural Seguridad Normal Firma Automática | RAR ATT-DJ-RAR-TL LP 357/2020 |