DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Aprobado con Resolución Administrativa
AGETIC/RA/0074/2026, de 31 de julio de 2026

UNIDAD DE GESTIÓN Y ASISTENCIA TECNOLÓGICA (UGAT)

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

Nombre del documento: Declaración de Prácticas 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 Cargo: Consultor en línea Firma Digital	Julio Oswaldo Mujica Quispe Cargo: Profesional de Diseño Conceptual I Firma Digital Jose Rodrigo Quiroz Barrios Cargo: Jefe de la Unidad de Gestión y Asistencia Tecnológica Firma Digital	Everth Rubin de Celis Gallardo Cargo: Responsable de Planificación Firma Digital Gabriela Daniela Quino Melgarejo Cargo: Técnico de Planificación Firma Digital	Carlos Eduardo Rodrigo Prado Cargo: Director General Ejecutivo a.i. 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 del 02 de julio de 2026.

3. Alcance y/o Ámbito de Aplicación

La presente Declaración 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 digital. 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 declaración, se establecen las siguientes definiciones ordenadas alfabéticamente:

- **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:** Es un archivo 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; 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, relativas a las condiciones mismas en que la obligación debía ser cumplida (ataque informático, conmociones civiles, huelgas, bloqueos, revoluciones, etc.);
- **Emisión de Certificados:** La Entidad Certificadora Pública AGETIC emitirá los certificados que se soliciten a través de una Agencia de Registro autorizada mediante un CSR; las solicitudes son remitidas una vez que el Oficial de Registro de la Agencia de Registro haya comprobado el cumplimiento de los requisitos.
- **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 usó para tareas definidas en este.

- **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:** La infraestructura de clave pública es el conjunto de todas las entidades certificadoras y usuarios de los certificados digitales y de las relaciones entre estos actores. Una infraestructura de clave pública es 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. Todos los certificados emitidos en una infraestructura de clave pública pueden ser validados siguiendo un camino lógico hasta la entidad certificadora raíz, en la cual está depositada la confianza en la infraestructura de clave pública. En el caso de la infraestructura de clave pública de Bolivia, la Entidad Certificadora Raíz es la ATT, y la Entidad Certificadora Pública es la AGETIC.
- **Lista de certificados revocados:** Una lista de revocatoria de certificados (en inglés Certificate Revocation List - CRL) es un archivo digital que contiene una lista de certificados revocados. La revocatoria de un certificado corresponde a revocar su validez, por algún motivo, antes de su fecha de expiración. La lista de revocatoria de certificados está firmada por una autoridad reconocida dentro de la infraestructura de clave pública. En el caso de la Entidad Certificadora Pública AGETIC, la lista de revocatoria está firmada con un par de claves y un certificado dedicados de la AGETIC.
- **Lista de confianza:** La lista de confianza establece, mantiene y publica información relativa a las Entidades de Certificación Autorizadas, posee el certificados raíz de la así como los certificados emitidos a las Entidades de Certificación Autorizadas de la INCD, lo que permite y garantiza que las firmas digitales realizadas sean reconocidas como válidas.
- **Módulo criptográfico basado en hardware:** Es un dispositivo de seguridad basado en hardware (Por ejemplo, HSM, token o smartcard) que genera, almacena y protege claves criptográficas. Los dispositivos criptográficos deberán estar homologados por la ATT.
- **Nivel de seguridad:** En caso de que el par de claves sea generado por un dispositivo criptográfico basado en hardware, el certificado tendrá nivel de seguridad alto, en caso de que el par de claves sea generado por software tendrá nivel de seguridad normal.
- **Nota de Débito:** Documento que describe el monto a pagar por el usuario y especifica las cuentas bancarias a las que debe realizar el pago.
- **Par de claves:** Es el conjunto de la clave privada y la clave pública. Las dos claves se generan al mismo tiempo por el mismo mecanismo criptográfico. Estas dos claves son complementarias, y para cualquier operación que implique el uso de una de las dos claves, se necesita la segunda clave para cumplir la operación.
- **Repositorio**: Es el lugar en el sitio web donde se publican los documentos relacionados al servicio de certificación digital, así como los servicios relacionados que se encargan de comprobar el estado de los certificados.
- **Signatario:** Es la usuaria o usuario titular de un certificado digital emitido por una entidad certificadora autorizada, que le permite firmar digitalmente.

- **Solicitud de firma de certificado:** Una solicitud de firma de certificado (en inglés Certificate Signing Request - CSR) es un archivo digital que un solicitante transmite a una Entidad Certificadora para obtener la firma de su certificado. La solicitud de firma de certificado contiene los datos de identidad y la clave pública del solicitante, y está firmada con la clave privada del solicitante para certificar que la solicitud es auténtica.
- **Usuario titular:** El usuario titular para el servicio de certificación digital de la Entidad Certificadora Pública AGETIC es la persona física titular del certificado digital y, en consecuencia, tendrá los derechos de revocación, reemisión y renovación sobre el certificado. El certificado puede ser de persona natural o persona jurídica.
- **Usuario corporativo:** Entidades públicas o privadas que establecen un vínculo contractual o de convenio con la Entidad Certificadora Pública AGETIC, para las operaciones sobre certificados digitales de su personal interno se les habilitará cuentas corporativas.

6. Aprobación, Vigencia, Difusión e Implementación

La aprobación de la presente Declaración 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 Declaración 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 Declaración sea actualizada, deberá darse cumplimiento al punto precedente de Aprobación, Vigencia, Difusión e Implementación.

CAPÍTULO II
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

8. Introducción

8.1. Presentación

La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) es una institución pública descentralizada bajo tuición del Ministerio de la Presidencia, creada mediante el Decreto Supremo N.º 2514. En cumplimiento del Decreto Supremo N.º 5519, la AGETIC asume las funciones de Entidad Certificadora Pública (ECP), asumiendo la responsabilidad de prestar servicios de certificación para el sector público y la población en general a nivel nacional, conforme a lo establecido en la Ley N.º 164.

La AGETIC cuenta con la autorización formal de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) mediante la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL-LP-249-2026 para el suministro de servicios de emisión, validación, renovación y revocación de certificados para Firma Digital.

La presente Declaración de Prácticas de Certificación (DPC) es el instrumento que describe las reglas, procesos y procedimientos específicos bajo los cuales la AGETIC brinda el servicio, garantizando la autenticidad, integridad y el no repudio en las comunicaciones digitales.

La AGETIC contempla la emisión de distintos tipos de certificados, los mismos se encuentran descritos en el documento “Política de Certificación”.

8.1.1. Propósito

El certificado digital para firma digital cumple los siguientes propósitos:

- Acredita la identidad del titular del Certificado Digital.
- Proporciona legitimidad del Certificado en base a los servicios de verificación de revocación de certificados.
- Vincula un documento digital o mensaje electrónico de datos firmado digitalmente con el usuario titular.
- 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 y nombre del documento

Este documento se titula “Declaración de Prácticas de Certificación”. La fecha de entrada en vigor de este documento es a partir de su aprobación por Resolución Administrativa de la Entidad Certificadora Pública AGETIC y permanece vigente hasta la liberación de una nueva versión que será notificada a los interesados.

Nombre: Declaración de Prácticas de Certificación (DPC)
Versión: La versión del presente documento se encuentra establecido en la cabecera del presente documento, vinculado a su respectiva Resolución Administrativa de aprobación.
Descripción: Declaración de Prácticas de Certificación de la Entidad Certificadora Pública AGETIC.
Fecha de emisión: La fecha de elaboración y la última actualización de la presente Declaración se encuentran detalladas en la carátula del presente documento, vinculadas a su respectiva Resolución Administrativa de aprobación.
OID: 2.16.68.0.0.0.1.14.1.2.0.1.0.1
Localización:
https://firmadigital.bo/assets/declaracion-de-practicas-de-certificacion-2026.pdf.

8.3. Participantes de la INCD del Estado

El ARTÍCULO 36.- (JERARQUÍA NACIONAL DE CERTIFICACIÓN DIGITAL) del Decreto Supremo N° 1793, establece los niveles de la Infraestructura Nacional de Certificación Digital (INCD), que se describen a continuación:

8.3.1. Primer nivel: Entidad Certificadora Raíz

La ATT es la entidad de certificación de nivel superior dentro de la Infraestructura Nacional de Certificación Digital que auto firma su certificado y emite certificados digitales a las entidades certificadoras públicas y privadas subordinadas.

8.3.2. Segundo Nivel: Entidad de Certificación

Son las Entidades Certificadoras Pública o Privadas subordinadas de la Entidad Certificadora Raíz. La Entidad Certificadora Pública es la AGETIC y las entidades certificadoras privadas, son todas aquellas autorizadas por la ATT para prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

La Entidad Certificadora Pública AGETIC elaboró los documentos públicos y privados exigidos por la entidad reguladora ATT. Así mismo establece los precios y promociones que se pueden aplicar al servicio de emisión de Certificados Digitales.

8.3.3. Tercer nivel: Agencia de Registro

Es la agencia dependiente de una entidad certificadora, encargada de realizar el registro e identificación del futuro titular del Certificado Digital en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además, es quien se encarga de solicitar la emisión o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital.

8.3.4. Cuarto nivel: Signatarios

También denominados Usuarios titulares, son todos los usuarios y usuarias titulares de un certificado digital emitido por una entidad certificadora autorizada dentro de la INCD y que firman documentos digitalmente.

8.3.5. Terceros aceptantes

Es cualquiera persona física o persona jurídica que valida y confía en los certificados emitidos por una Entidad Certificadora Autorizada de la INCD de Bolivia

8.4. Uso de los certificados

8.4.1. Usos Permitidos de los Certificados

La Entidad Certificadora Pública AGETIC emite certificados digitales para firmar la Lista de Certificados Revocados (CRL) y firmar las respuestas que emite el Protocolo de Comprobación del Estado de un Certificado (OCSP). Los usos de ambos certificados emitidos por la Entidad Certificadora Pública AGETIC se detallan a continuación:

TIPOS DE CERTIFICADO	USO
Lista de Revocación de Certificado (CRL)	Firmar la Lista de Revocación de Certificado
Protocolo de comprobación del Estado de un Certificado (OCSP)	Firmar las respuestas OCSP
Adicionalmente la Entidad Certificadora Pública AGETIC emite diferentes tipos de Certificados Digitales cuyo uso será limitado por la presente “Declaración de Prácticas” y por el documento “Políticas de Certificación” y otros documentos que sean emitidos por autoridades competentes.	

Así mismo, la Entidad Certificadora Pública AGETIC emite diferentes tipos de certificados digitales que se establecen en las Políticas de Certificación, mismos que están limitados en su uso por el ente regulador ATT, de acuerdo a la siguiente descripción:

- **Límite de uso de Certificados Digitales emitidos por dispositivos basados en hardware:**
  Los certificados digitales con seguridad Alta (emitidos por dispositivos basados en hardware) podrán ser utilizados para firmar cualquier documento, de forma simple o automática conforme a las limitaciones establecidas en la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación.

- **Límite de uso de Certificados Digitales emitidos por dispositivos basados en software:**
  Los certificados digitales con seguridad Normal (emitidos por dispositivos basados en software) podrán ser utilizados de acuerdo a lo establecido por las instituciones o empresas que decidan adoptarlas dentro sus procedimientos, exceptuando lo establecido en la Resolución Ministerial N° 235/18 específicamente sobre el uso de los certificados digitales de nivel alto y normal en las entidades del sector público.

8.4.2. Restricciones en el Uso de los Certificados

La restricción de uso se establece bajo los criterios presentes en la sección anterior, considerando además la exclusión en su validez jurídica de los actos descritos en el artículo 79 de la Ley N.º 164:

- Los actos propios de derecho de familia
- Los actos en que la ley requiera la concurrencia personal física de alguna de las partes
- Los actos o negocios jurídicos señalados en la ley que, para su validez o producción de determinados efectos, requieran de documento físico o por acuerdo entre partes.

Es importante destacar que el signatario es el único responsable de cumplir con las normas, reglamentos y leyes vigentes en el Estado Plurinacional de Bolivia. Cualquier violación a estas normas será responsabilidad exclusiva del signatario, incluyendo cualquier daño o perjuicio que pueda ocasionar. La Entidad Certificadora Pública AGETIC cumple con su responsabilidad al emitir el Certificado Digital, asegurando que se hayan cumplido los procedimientos y requisitos correspondientes, sin embargo, a partir de la emisión del Certificado Digital, todas las acciones realizadas por el signatario son de su completa responsabilidad.

Adicionalmente, en caso de incumplimiento de las responsabilidades por parte del signatario, la Entidad Certificadora Pública AGETIC se reserva el derecho de revocar el Certificado Digital emitido.

Asimismo, el signatario será responsable de indemnizar a la Entidad Certificadora Pública AGETIC por cualquier daño o perjuicio ocasionado a terceros como resultado de reclamos legales, acciones legales, pérdidas o daños, incluyendo multas legales, que puedan surgir, debido al uso indebido del Certificado.

Es importante destacar que estas responsabilidades y consecuencias están alineadas con las regulaciones establecidas por el ente regulador ATT y otras entidades competentes. El signatario debe entender y aceptar que el uso inapropiado o ilegal del Certificado puede tener repercusiones legales y financieras tanto para ellos como para la Entidad Certificadora.

8.4.3. Fiabilidad de la firma digital a lo largo del tiempo

La validez de la firma digital está garantizada cuando el documento haya sido firmado con un Certificado Digital vigente dentro de la INCD.

Para una validación en línea de documentos firmados digitalmente, la Entidad Certificadora Pública AGETIC dispuso un sistema de validación accesible desde la siguiente dirección:

https://validar.firmadigital.bo/

8.5. Administración de la Declaración de Prácticas de Certificación

La responsabilidad de la administración de esta “Declaración de Prácticas de Certificación” corresponde a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) en su calidad de Entidad Certificadora Pública.

Cuando la Entidad Certificadora Pública AGETIC realice modificaciones a la presente "Declaración de Prácticas 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 Transportes y Telecomunicaciones.
- **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.
- **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) Modulo de Hardware de Seguridad[1].
- **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 emitido por el Servicio de Impuestos Nacionales.
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **OID:** (ObjectIdentifier) Identificador de Objeto.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.

[1] Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas

- **RFC:** (Request For Comments[2]) 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:** Identificador Uniforme de Recursos
- **UTF:** (Unicode Transformation Format) Formato de codificación de caracteres.

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 mantiene 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 los 7 días de la semana y en caso de presentarse algún incidente en el sitio web, la Entidad Certificadora Pública 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 publicada en:

https://firmadigital.bo/firmadigital_bo3.crl

9.3. Servicio OCSP

El servicio de consulta OCSP se encuentra publicada en:

https://www.firmadigital.bo/ocsp3

[2] Es un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

9.4. Términos y condiciones

La prestación del servicio de Certificación Digital, se encuentra sujeta y sometida al cumplimiento de los Términos y condiciones del servicio vigente se encuentra publicada en:

https://firmadigital.bo/assets/terminos-y-condiciones-del-servicio-2026.pdf

9.5. Políticas de Certificación

La “Política de Certificación” vigente se encuentra publicada en:

https://firmadigital.bo/politicas-de-certificacion-2026.pdf

9.6. Declaración de prácticas de certificación

La Declaración de Prácticas de Certificación vigente se encuentra publicada 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, Entidad Certificadora Raíz 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 compuestos por el presente documento y la Política de Certificación de los diferentes tipos de certificados. 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 alterar la información (al incluir, actualizar o eliminar datos).

10. Identificación y autenticación de los usuarios titulares de los certificados

A continuación, se describen los procedimientos y criterios aplicados por la Entidad Certificadora Pública AGETIC para las Agencias de Registro en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado digital.

10.1. Registro de nombres

10.1.1. Tipos de nombres

Todos los certificados requieren un nombre distinguido conforme al estándar X.500.
En el documento “Políticas de Certificación” se especifican los atributos que conforman el Distinguished Name (DN).

10.1.2. Significado de los nombres

Los usuarios que requieran el servicio deberán suscribirse al servicio de certificación digital con sus nombres y apellidos completos conforme fueron registrados en el SEGIP. Únicamente se consideran los nombres y apellidos (primero y segundo) como atributos para definir la identidad de un usuario titular, tal cual 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. No serán admitidos o procesados por la Entidad Certificadora Pública AGETIC los datos correspondientes a diminutivos de nombres, alias o seudónimos.

10.1.3. Interpretación de formatos de nombres

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

10.1.4. Unicidad de nombres

Se garantiza que los nombres (campo DN) de los certificados son únicos para cada titular porque contienen el atributo de número de documento de identidad y número de complemento asignados por el SEGIP, y que permiten distinguir entre dos identidades cuando existan problemas de duplicidad de nombres (homónimos). Así mismo en el documento “Políticas de Certificación” se establece el contenido del campo DN, que

garantiza que los certificados sean únicos.

10.1.5. Resolución de conflictos relativos a nombres

En el caso de una ocurrencia de conflicto de nombres o duplicidad en la identidad debe ser resuelto ante el SEGIP.

10.2. Validación de la identidad inicial

10.2.1. Métodos de prueba de posesión de la clave privada

La Entidad Certificadora Pública AGETIC, previo a la emisión del certificado digital, requiere que el solicitante de un tipo de certificado genere su clave privada y pública mediante un procedimiento que garantice su confidencialidad y su vinculación con la identidad del solicitante.

El futuro signatario es la única persona autorizada para crear su propio par de claves (clave privada y clave pública), la clave privada permanece exclusivamente en posesión del signatario y en ningún momento es conocida por la Entidad Certificadora Pública AGETIC, mientras que la clave pública si es compartida con la Entidad Certificadora Pública AGETIC porque la misma debe ser incluida en el certificado digital a emitir.

Los Oficiales de Registro de cada Agencia de Registro autorizada podrán apoyar en el proceso de creación del par de claves, asesorando en el manejo de los sistemas y herramientas para tal fin.

El método utilizado para comprobar que el solicitante posee la clave privada que corresponde a la clave pública, para la que se solicita se emita el certificado digital, será mediante el envío del CSR en el cual se incluye la clave pública y está firmada por la clave privada asociada.

La Entidad Certificadora Pública AGETIC emitirá los certificados de acuerdo a estructura aprobada por la ATT en base a la información ingresada por el usuario solicitante.

10.2.2. Autenticación de la identidad de una organización

La Entidad Certificadora Pública AGETIC emite Certificados Digitales a nombre de un titular o persona, de acuerdo al tipo de certificado el mismo contendrá los datos referidos a una organización si corresponde.

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.

Las Agencias de Registros reconocidas por la AGETIC deben validar los datos del representante legal de la Empresa o Entidad mediante el uso de la Plataforma de Interoperabilidad u otros medios digitales que se dispongan.

10.2.3. Autenticación de la identidad del solicitante

Durante el registro, los sistemas de las Agencias de Registro son las encargadas de verificar la información primaria del titular a través de la contrastación de datos con el SEGIP y el uso de la Plataforma de Interoperabilidad u otros medios que se disponga.

Este proceso de registro y validación de la identidad inicial debe alcanzar un Nivel de Confianza Alto, en correspondencia a lo descrito en las “Políticas de Certificación”.

Para emitir un certificado se exige la demostración fehaciente de la identidad del titular mediante los siguientes métodos:

- Presentación de documento de identidad vigente y original para contrastar los datos mediante servicios de interoperabilidad con fuentes oficiales.
- Confirmación de la identidad y prueba de vida, la cual podrá realizarse de forma presencial (verificación física) o mediante modalidad virtual a través de videollamadas asistidas por un Oficial de Registro.
- Generación y resguardo obligatorio de evidencia multimedia de la interacción (fotografías, videos u otros registros) como constancia del proceso de validación y fe de vida.

Las Agencias de Registro se reservan el derecho de rechazar la solicitud de emisión si la documentación no es suficiente para autenticar al solicitante.

Se aplicarán criterios de rechazo inmediato ante inconsistencia de datos con las fuentes oficiales, documentación caducada o alterada, fallos de identificación en la videollamada o detección de intentos de suplantación de identidad.

Los requisitos específicos para cada tipo de Certificado Digital están detallados en el documento “Políticas de Certificación”.

Toda información suministrada será revisada por el Oficial de Registro, quien verificará que sea original, suficiente y adecuada de acuerdo con los procedimientos internos definidos por la AGETIC.

11. Ciclo de Vida de los Certificados

11.1. Requisitos para la obtención de un Certificado Digital

11.1.1. Requisitos documentales

Cada tipo de certificado tiene sus propios requisitos que se encuentran detallados en el documento “Políticas de Certificación”. Las Agencias de Registro tienen la obligación de verificar el cumplimiento de los mismos, conforme a los estándares técnicos y lineamientos establecidos en la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019.

Los documentos requeridos pueden ser cargados en el Sistema de Agencia de Registro o presentados ante un Oficial de Registro para su digitalización y carga.

De manera específica, para certificados de Persona Natural se requiere la última factura de pago de servicios (luz, agua o teléfono) para verificar el domicilio real o laboral del titular.

Para Persona Jurídica, se debe presentar el NIT vigente, la Nota de Autorización firmada por la MAE o Representante Legal y el documento que acredite la relación laboral entre la entidad y el solicitante.

11.1.2. Requisitos Técnicos para Acceder al Servicio

Para que un usuario pueda acceder al servicio de certificación digital deberá:

- Contar con acceso a Internet.
- Darse de alta como usuario en el sistema de Agencia de Registro.

En función al nivel de seguridad del certificado a solicitar, deberá contar con:

- 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. 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 el aplicativo Jacobitus para la generación del par de claves por software, misma que puede ser encontrada en: https://firmadigital.bo/.

11.2. Solicitud del Certificado

Los certificados emitidos por la Entidad Certificadora Pública AGETIC tienen periodos de vigencia según el tipo de Certificado, dicho periodo está especificado en el propio certificado y está definido en el documento “Políticas de Certificación”.
Independientemente del tipo, se pueden emitir certificados por tipo de uso:

Firma Digital Simple: cuando el usuario titular administra el certificado para cada una de las firmas a realizar.

Firma Digital Automática: cuando la firma digital se realiza a través de un sistema informático, donde el titular del certificado delega su uso para tareas definidas en éste.

Así mismo, según el medio donde se genere el par de claves (público y privado), el certificado podrá tener alguno de los siguientes niveles de seguridad:

Nivel de seguridad alto: el par de claves se genera en un dispositivo criptográfico por hardware que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente y además debe estar homologado por la ATT .

Nivel de seguridad normal: el par de claves se genera en un dispositivo criptográfico por software que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente.

La solicitud de un certificado digital puede ser realizada por cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

Los periodos operativos y plazos de vigencia de los certificados digitales se encuentran definidos detalladamente en la “Política de Certificación” vigente.

11.3. Tramitación de solicitud de certificado

El usuario solicitante podrá realizar la solicitud a través del Sistema de Agencia de Registro. También puede realizar la solicitud de manera presencial en cualquier Agencia de Registro con ayuda de un Oficial de Registro. Este proceso de registro y validación de la identidad inicial debe alcanzar obligatoriamente un Nivel de Confianza Alto, en correspondencia con estándares internacionales.

Las Agencias de Registro brindarán mínimamente la siguiente información necesaria sobre los procesos y procedimientos para la solicitud de certificados digitales:

- Documentación necesaria que deben presentar para el procedimiento de obtención de certificado digital y para autenticar la identidad del solicitante.
- Información sobre los procesos y procedimientos de emisión, revocación, reemisión y renovación del certificado digital, así como las condiciones de uso.
- El acceso a los documentos normativos vigentes, al presente documento y a la Políticas de Certificación.

Para iniciar el proceso de solicitud de emisión de certificado digital, el usuario solicitante debe:

- Elegir una Agencia de Registro reconocida por la Entidad Certificadora Pública AGETIC.

- Disponer de una cuenta en el sistema de Agencia de Registro, con todas las validaciones necesarias requeridas por la normativa vigente.
- Solicitar mediante el sistema de la Agencia de Registro el tipo de certificado digital requerido.

El documento “Políticas de Certificación” especifica la documentación adicional requerida para la solicitud de los mismos. El usuario deberá presentar los requisitos establecidos de acuerdo con el tipo de certificado solicitado.

El usuario deberá crear su par de claves y enviar su clave pública a través de mecanismos que garanticen que el procedimiento es seguro. Si el usuario no supiera realizar la operación, los Oficiales de Registro le proporcionarán el soporte necesario, mismo que podrá ser realizado en cualquier Agencia de Registro autorizada siempre y cuando se utilice un Token o Smartcard como medio de almacenamiento del Certificado; en caso de Certificados almacenados en un contenedor de Software o en un HSM, la responsabilidad de la generación del par de claves es del usuario solicitante.

La Entidad Certificadora Pública AGETIC pone a disposición de sus usuarios herramientas que le permiten la generación de par de claves y firma digital bajo diferentes estándares, publicados en:

https://firmadigital.bo/

Es política obligatoria que la generación del par de claves sea realizada bajo el control exclusivo del solicitante, 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.

Las Agencias de Registro deben asegurarse que los usuarios solicitantes han sido plenamente identificados y que la petición de certificado es verificada y completa. Para ello, la Agencia de Registro podrá disponer de diferentes medios para realizar la respectiva verificación de documentos, validación de identidad y prueba de vida.

Para asegurar de forma fehaciente la identidad, la AGETIC aplica el procedimiento de Prueba de Vida, el cual se gestiona mediante la Modalidad de Validación Asistida (Videollamada), consistente en una interacción virtual en tiempo real supervisada por un Oficial de Registro para la confirmación visual y documental del solicitante.

Es requisito obligatorio la generación y resguardo de evidencia multimedia de la interacción (fotografías, videos u otros registros) como prueba de fe de vida y constancia del proceso realizado.

El solicitante asume la responsabilidad por la veracidad y exactitud de la información proporcionada y presentada en el sistema y al Oficial de Registro para la solicitud del certificado.

La Agencia de Registro debe realizar un proceso de validación de la identidad del solicitante con el SEGIP y complementar este proceso con el uso de la Plataforma de Interoperabilidad u otros medios digitales que se dispongan. Asimismo, deben verificar el cumplimiento de los requisitos y verificación del pago correspondiente.

El Oficial de Registro podrá rechazar una solicitud en los siguientes casos:

- Documentación incompleta, no vigente, o que presente alteraciones que no permitan la identificación plena del titular.
- Inconsistencia de datos entre la información declarada y las fuentes oficiales del Estado.
- Suplantación de identidad; en cuyo caso deberá realizarse las gestiones correspondientes según normativa vigente.
- En caso de no poder realizar la confirmación física o virtual de la identidad del solicitante o signatario, o ante fallos de identificación durante la videollamada.

En estos casos el Oficial de Registro debe informar al solicitante los motivos que originaron el rechazo de la solicitud. Las solicitudes creadas se mantendrán en el sistema durante 15 días a la espera de pago o requisitos antes de pasar al estado EXPIRADO.

Una vez verificada la solicitud, el Oficial de Registro deberá firmar digitalmente el CSR y enviar a la Entidad Certificadora Pública AGETIC.

Las Agencias de Registro son responsables de centralizar la información digital generada y obtenida en los procesos de solicitud, renovación, reemisión y revocación de certificados digitales.

Todo CSR registrado y enviado por la Agencia de Registro, que no llegue a ser procesado por la Entidad Certificadora Pública en los plazos establecidos, por casos fortuitos o de fuerza mayor, deberán ser informadas mediante nota oficial al ente regulador ATT para su conocimiento y seguimiento.

Para las entidades públicas se procederá a realizar la emisión de los certificados digitales una vez se cumpla el respectivo procedimiento administrativo de contratación con la Entidad Certificadora Pública AGETIC, según normativa vigente.

Para las entidades privadas se procederá a realizar la emisión de los certificados digitales previa solicitud y constancia de pago o firma de contrato/documento equivalente que garantice el compromiso de pago.

En el caso de las cuentas corporativas, la entidad beneficiada deberá remitir formalmente a la Entidad Certificadora Pública AGETIC mediante nota firmada por el Representante Legal o Máxima Autoridad Ejecutiva de la entidad, el listado del personal autorizado para obtener un certificado digital por el servicio adquirido. Toda revocación corporativa deberá gestionarse obligatoriamente a través del módulo correspondiente del sistema informático oficial. Estas

entidades serán responsables de informar a sus dependientes sobre los procesos de generación de cada solicitud y agotarán esfuerzos de coordinación para que los mismos cumplan con todos los requisitos establecidos.

11.4. Emisión del certificado

La Entidad Certificadora Pública AGETIC será responsable de atender todo CSR remitido por las Agencias de Registro, debidamente firmados por el Oficial de Registro que atendió la solicitud y solicitó la emisión del respectivo certificado digital. Para este fin, se dispone de procedimientos internos que incluyen una Ceremonia de Emisión de Certificados Digitales, la cual constituye un acto protocolar y técnico estrictamente controlado donde el personal autorizado ejecuta las funciones de firma en el hardware criptográfico de la entidad.

La Entidad Certificadora Pública AGETIC, dando cumplimiento a la normativa vigente, tendrá un plazo máximo de 72 horas para la emisión de los certificados y poner a disposición de los solicitantes su certificado digital firmado, salvo en caso fortuito, de coyuntura, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante y al ente regulador. Una vez concluida la emisión, se garantiza la actualización inmediata de los servicios de consulta de estado OCSP.

Asimismo, la Entidad Certificadora Pública AGETIC tiene procedimientos internos para realizar una evaluación por muestreo de los requisitos presentados en cada solicitud de emisión de certificado digital, posterior a la emisión del certificado, a través de un control cruzado de los documentos. Si en la evaluación se comprueba que no se han cumplido los requisitos, la Entidad Certificadora Pública AGETIC procederá a reportar oficialmente a la Agencia de Registro para la respectiva corrección.

11.5. Aceptación del certificado

Los certificados emitidos por la Entidad Certificadora Pública son enviados al sistema de Agencia de Registro, donde los usuarios titulares poseedores de la clave privada podrán descargar el certificado correspondiente, previa autenticación. La vigencia del Certificado Digital inicia al momento de su emisión.

Con la emisión y el envío del certificado a la cuenta del signatario en el sistema de la Agencia de Registro, se considera que la Entidad Certificadora Pública AGETIC ha cumplido con el servicio de Certificación Digital. La disponibilidad del certificado en la plataforma constituye la notificación formal de finalización del servicio.

El contrato de adhesión, que debe ser firmado digitalmente por el signatario, garantiza el reconocimiento de las condiciones de uso, así como las obligaciones y derechos establecidos para éste. Para formalizar la aceptación y activar la plena responsabilidad legal del servicio, el titular debe firmar digitalmente el Contrato de Adhesión dentro de un plazo perentorio de 120 horas (5 días calendario) desde el momento de la emisión.

El incumplimiento de la firma del contrato en el plazo establecido activa un protocolo técnico de revocación automática por falta de aceptación contractual. En estos casos, la AGETIC podrá emitir un nuevo certificado sin costo alguno y sin afectar el conteo de reemisiones permitidas, siempre que el usuario titular realice la solicitud respectiva. Este nuevo certificado mantendrá la vigencia del certificado inicial revocado.

11.6. Uso del certificado y del par de claves

Los certificados digitales podrán ser utilizados según lo estipulado en esta Declaración de Prácticas de Certificación, en las Políticas de Certificación correspondientes y en cualquier otro documento complementario emitido por la Entidad Certificadora Pública AGETIC y aprobado por la ATT.

La generación y resguardo de la clave privada es una acción estrictamente privada y de exclusiva responsabilidad del titular. El uso del certificado es personal e intransferible; el titular tiene la obligación de mantener el control y reserva del método de creación de su firma para evitar usos no autorizados por terceros. Esta restricción no aplica a los certificados de Firma Automática, donde el titular delega técnicamente el uso a un sistema informático bajo su supervisión. Ante cualquier sospecha de pérdida, robo o compromiso de la clave privada, el titular debe proceder a la revocación inmediata de su certificado para evitar consecuencias legales derivadas de un uso indebido.

El uso de la firma digital dentro del sector público está sujeto al "Reglamento para normar el uso de la firma digital respecto a niveles de seguridad" (Resolución Ministerial N° 235/18), el cual define las condiciones técnicas y legales para la emisión y recepción de documentos según el nivel de seguridad del certificado (Alto o Normal). Asimismo, queda estrictamente prohibido el uso del certificado por parte de los suscriptores para la firma de Listas de Revocación de Certificados (CRL) o para generar respuestas de validación OCSP; estas funciones son competencia exclusiva de la Entidad Certificadora Pública AGETIC.

Los terceros aceptantes son las entidades o personas (diferentes al signatario) que deciden aceptar y confiar en un certificado digital emitido por la Entidad Certificadora Pública AGETIC. Es responsabilidad de los terceros aceptantes verificar el documento firmado digitalmente mediante los servicios y herramientas ofrecidos por la Entidad Certificadora Pública AGETIC. Cualquier persona o entidad que confíe en una firma digital generada bajo esta DPC tiene la obligación técnica de verificar la validez y el estado del certificado utilizando el portal oficial de validación (https://validar.firmadigital.bo/) o los servicios permanentes de consulta en tiempo real (OCSP) antes de aceptar el documento.

En caso de verse comprometida su clave privada, el signatario deberá realizar la revocación de su certificado digital de acuerdo con los procedimientos establecidos en el presente documento.

11.7. Renovación del certificado digital

El periodo habilitado para realizar una solicitud de renovación de Certificado Digital es de 30 días calendario antes del término de la vigencia del Certificado Digital actual. La Entidad Certificadora Pública AGETIC enviará recordatorios a los signatarios para que realicen su renovación, de acuerdo al siguiente cronograma:

- Quince (15) días calendario antes de la expiración del Certificado Digital.
- Diez (10) días calendario antes de la expiración del Certificado Digital.
- Cinco (5) días calendario antes de la expiración del Certificado Digital.

Para la renovación el signatario deberá acceder al Sistema de Agencia de Registro con las credenciales que obtuvo al momento de crear la cuenta o su firma digital vigente, y cumplir con las siguientes condiciones:

- La renovación es de exclusiva responsabilidad y autoría del titular, debiendo ejecutarse de forma exclusiva a través del sistema informático autorizado
- Mantener, en la solicitud de renovación, todos los datos y tipo de certificado emitido inicialmente.
- Contar con el Certificado Digital a renovar dentro del periodo de vigencia.
- Realizar una nueva confirmación de identidad o Prueba de Vida, alcanzando un Nivel de Confianza Alto, la cual se gestionará mediante la Modalidad de Validación Asistida (Videollamada).
- Realizar el pago correspondiente de acuerdo a la estructura tarifaria vigente.
- Firmar digitalmente el Contrato de Adhesión correspondiente al nuevo Certificado Digital en un plazo máximo de 120 horas (5 días calendario) una vez el mismo sea emitido; caso contrario, se procederá a la resolución del contrato y a la consecuente revocación automática.
- Concluir la solicitud de renovación antes de la fecha y hora de expiración del Certificado Digital actual, caso contrario se procederá a expirar la solicitud y se deberá proceder a realizar una nueva solicitud como si se tratase de un trámite nuevo, necesitando cumplir todos los procedimientos establecidos por la Entidad Certificadora Pública AGETIC.

En caso de asistencia presencial ante una Agencia de Registro, el Oficial de Registro limitará sus funciones a guiar y orientar técnicamente al usuario, teniendo estrictamente prohibido operar la cuenta o procesar el trámite en su terminal de soporte, por tratarse de un acto de autogestión.

El Oficial de Registro deberá firmar digitalmente la solicitud de firma de certificado (CSR) para enviarlo a la Entidad Certificadora Pública AGETIC.

Se puede realizar la solicitud de renovación hasta en tres (3) oportunidades consecutivas, siempre y cuando el certificado esté vigente. La cuarta renovación consecutiva será tratada como una solicitud nueva, necesitando cumplir todos los procedimientos establecidos por la

Entidad Certificadora Pública AGETIC.

En caso de requerir el cambio de tipo de certificado o alguno de los datos que sean permitidos de acuerdo con las políticas de certificación de cada tipo de certificado, se deberá contactar con el Oficial de Registro para realizar el procedimiento correspondiente.

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.

Las solicitudes de renovación se atenderán en los tiempos establecidos según normativa.

11.8. Reemisión del Certificado Digital

La reemisión de un certificado digital es un procedimiento técnico que se realiza a través del sistema de Agencia de Registro de la AGETIC. Este proceso permite al suscriptor obtener un nuevo certificado con un nuevo par de claves, manteniendo exactamente la misma fecha de expiración y las condiciones de la suscripción inicial.

La solicitud de reemisión deberá realizarse con la generación de un nuevo par de claves (pública y privada). Al igual que en la solicitud inicial, esta acción es estrictamente privada y de exclusiva responsabilidad del titular, debiendo utilizar el aplicativo Jacobitus o un dispositivo de hardware homologado según el nivel de seguridad del certificado. Asimismo, todas las solicitudes de reemisión deberán estar firmadas digitalmente por un Oficial de Registro antes de ser enviadas a la ECP, garantizando la seguridad del proceso.

Al enviar la solicitud de reemisión, el Sistema de Agencia de Registro determinará el periodo de validez correspondiente en base al tiempo restante del certificado digital inicial. La infraestructura técnica procesará la reemisión en los siguientes casos de aplicación:

- Pérdida, robo, deterioro o bloqueo del dispositivo criptográfico (token).
- Sospecha fundada de compromiso de la clave privada, lo cual obliga a la revocación previa del certificado afectado.
- Corrección o actualización de información específica del titular (apellidos, cargos o datos de la organización).
- Cambio en la modalidad de uso (firma simple a automática o viceversa) o en el nivel de seguridad (software a hardware o viceversa).

En caso de extravío o deterioro del dispositivo token, un usuario puede solicitar la reposición del mismo cancelando el costo correspondiente y coordinando la entrega a través de los medios habilitados. La AGETIC permite realizar hasta cuatro (4) reemisiones gratuitas dentro del periodo de vigencia del certificado inicial; superado este límite, el titular deberá iniciar un nuevo proceso de solicitud con el costo de emisión vigente.

En caso de necesitar el cambio de signatario en la reemisión, se deberá proceder como si de

un nuevo certificado digital se tratase; sin embargo, el periodo de vigencia del nuevo certificado será por el tiempo restante del certificado inicial. Por cada reemisión, es obligatorio que el titular firme digitalmente un nuevo Contrato de Adhesión dentro de un plazo perentorio de 120 horas (5 días calendario) desde la emisión; de lo contrario, el sistema procederá a la revocación automática del nuevo certificado.

En el caso de Certificados de Tipo Persona Jurídica que requieran una reemisión con cambio de titular, se deberá presentar la nota de autorización de la MAE o Representante Legal, especificando al nuevo beneficiario.

11.9. Revocación del Certificado

La revocación de un certificado es el acto por el cual se deja sin efecto un certificado antes que alcance su fecha de caducidad. Cualquier firma digital realizada posterior a la revocación no tendrá validez; en cambio los documentos firmados previo a la revocación del certificado seguirán teniendo toda validez legal.

Una vez revocado el certificado, la Entidad Certificadora Pública AGETIC mediante procedimientos internos incluye el mismo en la Lista de Certificados Revocados (CRL) con el fin de notificar a terceros que un certificado ha sido revocado. Los certificados que sean revocados no podrán por ninguna circunstancia volver al estado activo, siendo esta una acción definitiva e irreversible.

La revocación se realizará de acuerdo con los procedimientos internos de la Entidad Certificadora Pública AGETIC y a solicitud del usuario o autoridad competente. Las entidades públicas y privadas tienen toda la responsabilidad de velar por la revocación de los certificados del personal dependiente desvinculado.

Un certificado digital podrá ser revocado debido a las siguientes causas:

- A solicitud del titular debido a robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada.
- Incumplimiento contractual: Por no firmar digitalmente el Contrato de Adhesión en el plazo perentorio de 120 horas (5 días calendario) establecido tras la emisión del certificado.
- Inexactitud de datos: Cuando la información contenida en el certificado (nombres, cargos o pertenencia a una organización) deje de ser correcta o vigente.
- Emisión defectuosa: Si se detectan errores en el proceso de validación, suplantación de identidad o falta de requisitos materiales detectados con posterioridad a la emisión.
- Cese de funciones: En certificados de personas jurídicas, cuando el titular ya no pertenezca a la organización o por decisión de la entidad.
- Revocación de infraestructura: Si el certificado de la Entidad Certificadora Pública AGETIC o de la Entidad Certificadora Raíz ATT es revocado.

- Otros fundamentos técnicos y/o legales mediante Resolución Administrativa de la Máxima Autoridad Ejecutiva.

Las condiciones mínimas para solicitar una revocación son: que el certificado se encuentre vigente y ser el signatario o representante legal de la entidad. La revocación no exime al titular del cumplimiento de las obligaciones contraídas durante la vigencia del certificado.

Canales y Procedimientos de Revocación: La AGETIC garantiza la disponibilidad de un único canal oficial para asegurar que el titular pueda solicitar la revocación de forma ágil y segura:

- Revocación en Línea (Portal AR): Es el método obligatorio y más expedito. El titular accede al sistema (https://solicitud.firmadigital.bo/) con sus credenciales; la autenticación exitosa se considera prueba suficiente de identidad para ejecutar la revocación inmediata y automatizada.
- Revocación Corporativa: Los representantes o administradores autorizados de entidades con convenio podrán revocar los certificados de sus beneficiarios a través del módulo corporativo del sistema informático, registrándose de forma automatizada la trazabilidad y justificación.

En caso de asistencia presencial ante una Agencia de Registro, el Oficial de Registro limitará sus funciones a facilitar orientación metodológica y técnica sobre el uso de la plataforma, teniendo estrictamente prohibido operar la cuenta del usuario o ejecutar la acción de revocación a nombre del titular, garantizando la autoría exclusiva del suscriptor sobre el estado de su certificado.

11.10. 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): El sistema genera y publica automáticamente un archivo firmado que contiene la relación de todos los certificados que han perdido su validez antes de su expiración, con el fin de notificar a terceros sobre dicha revocación. Por su naturaleza crítica, esta lista se actualiza periódicamente cada 15 minutos, siempre y cuando se produzca una nueva revocación.
- Protocolo de Estado de Certificados en Línea (OCSP): La AGETIC mantiene un servicio de consulta en tiempo real disponible las 24 horas del día, los 7 días de la semana. Este protocolo permite a las aplicaciones verificar de forma instantánea y segura si un certificado es válido al momento de realizar una firma, proporcionando una validación inmediata sin necesidad de que el usuario o el sistema descargue la lista completa de revocación.

11.11. Finalización de la suscripción

La suscripción del servicio de certificación digital está vinculada directamente al ciclo de vida y vigencia técnica del certificado emitido. Si bien el período estándar de suscripción es de un (1) año calendario, este plazo se sujeta a la vigencia específica grabada en el certificado según su tipo (pudiendo ser de hasta dos años en modalidades de firma automática), de acuerdo con lo establecido en la Política de Certificación.

La finalización de la suscripción y de la consecuente relación técnica-contractual entre el titular y la AGETIC se produce de manera efectiva bajo los siguientes escenarios.

- Expiración: Al cumplirse el término del periodo de vigencia técnica establecido en el propio certificado digital.
- Revocación Definitiva: Cuando el certificado es dejado sin efecto antes de su fecha de caducidad por cualquiera de las causales normativas, siempre que no se realice una reemisión posterior asociada a la misma suscripción.

11.12. Recuperación de la clave

En estricto cumplimiento del principio de exclusividad y privacidad, la AGETIC no almacena, custodia ni tiene acceso a las claves privadas de los usuarios titulares en ninguna fase de su ciclo de vida; por tanto, no existe un procedimiento técnico ni administrativo de "recuperación de clave privada" dentro de la infraestructura de la Entidad Certificadora Pública.

Sin embargo, en casos excepcionales y a solicitud exclusiva del usuario titular, los Oficiales de Registro brindarán apoyo técnico para el desbloqueo operativo de los dispositivos criptográficos basados en hardware (Tokens) que hayan sido bloqueados por intentos fallidos de contraseña. Este soporte se limita exclusivamente a la rehabilitación del dispositivo, sin que 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 se encuentre resguardada en un contenedor de software o en un módulo criptográfico de hardware (HSM) de la entidad. Ante el olvido de contraseñas, pérdida o compromiso de la clave privada en estas modalidades, la información es técnicamente irrecuperable; en tales casos, el titular deberá proceder obligatoriamente a la reemisión de un nuevo certificado digital mediante la generación de un par de claves completamente nuevo, cumpliendo con los procedimientos de validación establecidos.

12. Controles de seguridad física, gestión y de operaciones

12.1. Controles de seguridad física

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

La Entidad Certificadora Pública AGETIC tiene establecida su política de seguridad e identificados los controles necesarios para proteger sus áreas e instalaciones, sistemas, aplicaciones y servicios implementados de acuerdo a una gestión de riesgos. Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo.

12.1.1. Ubicación y construcción

Las dependencias del Centro de Procesamiento de Datos (CPD) de la Entidad Certificadora Pública AGETIC se encuentran en instalaciones del Edificio de la Vicepresidencia del Estado Plurinacional de Bolivia, en la parte del subsuelo.

La construcción del CPD reúne y mantiene los requisitos de operación, que impone la normativa en materia de seguridad. El CPD opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

La Entidad Certificadora Pública AGETIC cuenta con un CPD alterno, que dispone de los controles de seguridad establecidos en normativa referente para el funcionamiento de un CPD.

12.1.2. Acceso físico

El acceso físico al CPD mantiene medidas de control de acceso tanto lógicas como físicas garantizando la integridad y seguridad de los servicios prestados. Para el control de acceso físico existen cinco (5) niveles de seguridad, desde el exterior hasta el gabinete de la firma digital donde se encuentra la infraestructura necesaria del servicio.

Los procedimientos de seguridad permiten o restringen el acceso al CPD, desde el exterior hasta los servidores. El acceso está permitido solo al personal autorizado mediante: Inicio de sesión y contraseña, accesos biométricos y cerraduras físicas.

Para el acceso al gabinete de la firma digital donde se realizan los procesos criptográficos es necesario la autorización previa de la Entidad Certificadora Pública AGETIC según los planes y procedimientos de ingreso al CPD.

Se cuenta con sistema de vídeo vigilancia y de grabación que monitoriza los elementos con los que la Entidad Certificadora Pública AGETIC presta el servicio de certificación dentro del CPD y áreas o instalaciones destinadas al servicio.

12.1.3. Alimentación eléctrica y aire acondicionado

La construcción donde se encuentran instalados los servidores de la Entidad Certificadora Pública AGETIC cuenta con fuentes de energía ininterrumpida (UPS), las cuales a su vez están conectadas a un sistema de alimentación eléctrica alterna con un grupo electrógeno.

La construcción cuenta con su sistema de aire acondicionado, que recibe el mantenimiento necesario para su uso regular.

Las salas donde se ubican los equipos que componen los sistemas de certificación de la Entidad Certificadora Pública AGETIC y donde se realiza el proceso de emisión de certificados, disponen de suministro eléctrico garantizado por un grupo electrógeno, unidades de alimentación ininterrumpida y aire acondicionado para la operativa normal del servicio; además tienen instalados mecanismos que mantienen controlados el calor y la humedad a niveles acordes con los equipos que se encuentran instalados en el lugar.

12.1.4. Exposición al Agua

Las instalaciones del CPD y Cabina de Firma Digital están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se encuentran ubicados los equipos informáticos disponen de un sistema de detección de humedad.

12.1.5. Protección y prevención de incendios

Las instalaciones del CPD, Cabina de Firma Digital y áreas de trabajo para el servicio, tienen incorporados alarmas y sensores de detección contra fuego y humo, ante cualquier eventualidad que se presente, los cuales son monitorizados mediante un sistema de detección automática. Asimismo, se tienen extintores ubicados en lugares establecidos y adecuados.

12.1.6. Sistema de almacenamiento

La Entidad Certificadora Pública AGETIC cuenta con procedimientos establecidos para garantizar la disponibilidad de copias de seguridad de respaldo de la información crítica relacionada con el servicio. Estas copias de seguridad se almacenan tanto interna como externamente, asegurando su integridad y confidencialidad. Además, se toman medidas para garantizar la seguridad de los soportes utilizados para almacenar estas copias de seguridad.

La Entidad Certificadora Pública AGETIC tiene establecidos procedimientos de respaldo, resguardo y recuperación de las copias de seguridad en un sitio alterno, su transferencia y resguardo está definida según procedimientos, la información enviada y almacenada en soportes de información se encuentra cifrada.

12.1.7. Eliminación de residuos

Los soportes que contengan información confidencial de la Entidad Certificadora Pública AGETIC deberán ser destruidos, de tal manera que la información sea irrecuperable previniendo de esta manera el uso no autorizado y el acceso o divulgación de la información contenida en los desechos.

12.1.8. Copia de Seguridad

La Entidad Certificadora Pública AGETIC dispone de copias de seguridad de la información crítica del servicio en instalaciones seguras fuera del sitio principal, las mismas se enmarcan de acuerdo a los procedimientos de respaldo, resguardo, recuperación y entrega de copias de seguridad en conformidad al plan de contingencias y continuidad.

12.2. Controles de procedimiento

12.2.1. Roles de confianza

La Entidad Certificadora Pública mantendrá un esquema de gestión y operación basado en una estructura plana, sustentada sobre la interacción e interdependencia del personal en sus diversos roles y funciones.

La Entidad Certificadora Pública AGETIC se encuentra dividida en funciones de operación y administración, de acuerdo a los siguientes roles:

- Dirección General Ejecutiva: es la encargada de la toma de decisiones;
- La Unidad de Infraestructura Tecnológica (UIT): es la encargada de la parte operativa y del mantenimiento del CPD.
- Unidad de Producción y Actualización Tecnológica (UPAT): es la encargada del desarrollo y actualización de los sistemas y herramientas que se utilizan.
- Unidad de Gestión y Asistencia Tecnológica (UGAT): es la encargada de la administración y soporte técnico del servicio.

Todas las decisiones que se realizará a las operaciones técnicas y administrativas serán evaluadas por el Comité de Seguridad de la Información.

12.2.2. Número de personas requerida por tarea

El número de personas requeridas por tarea, y el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección Ejecutiva, a través de la emisión del documento legal correspondiente.

12.2.3. Identificación y autenticación para cada rol

La identificación y autenticación de cada rol, así como el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección General Ejecutiva.

12.3. Controles de seguridad del personal

12.3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación

El personal involucrado en el control y operación de la firma y Certificación Digital está suficientemente calificado y dispone de la experiencia necesaria para cumplir con las funciones asignadas a su rol, así mismo recibirá capacitación continua para garantizar los niveles de calidad sobre las políticas de seguridad y los procedimientos.

12.3.2. Procedimientos de comprobación de antecedentes

La calificación, contratación y comprobación de los antecedentes, experiencia y conocimiento del personal permanente, consultoría y eventual se realizará según los procedimientos internos que la Entidad Certificadora Pública AGETIC dispone.

12.3.3. Formación y frecuencia de actualización de la formación

El personal encargado del servicio de Certificación Digital dentro de la Entidad Certificadora Pública AGETIC debe recibir capacitación al menos una vez al año, en áreas asociadas a su labor directa u orientadas al desarrollo de destrezas necesarias para la prestación acorde y conforme de sus funciones.

12.3.4. Frecuencia y secuencia de rotación de tareas

Las asignaciones de roles y funciones dentro de la Entidad Certificadora Pública AGETIC se encuentran asociadas a la descripción del cargo que ocupa cada servidor público dentro de la entidad y al esquema de trabajo marcado en el organigrama interno.

12.3.5. Sanciones por acciones no autorizadas

Todo procedimiento no contemplado en el presente documento, la Política de Certificación y/o documentación interna aprobada, deberá contar con la aprobación expresa de la Dirección General Ejecutiva de la AGETIC, de lo contrario será considerado como incidentes dentro de la Entidad Certificadora Pública AGETIC y podrá ser revisados por el Comité de Calidad, Seguridad de la Información y de Emergencia, para que recomienden la sanción cuando corresponda de acuerdo a reglamentación interna.

12.3.6. Requerimientos de contratación de personal, controles periódicos de cumplimiento, finalización de los contratos

La Entidad Certificadora Pública AGETIC sigue la normativa definida bajo el sistema de contratación de bienes y servicios estipulado por el Estado Plurinacional de Bolivia y cuenta con controles periódicos a través de la presentación de informes internos relacionados a cada acción que deba ser informada.

Todo personal de la Entidad Certificadora Pública AGETIC que finaliza su relación contractual con la entidad, acepta y firma un acuerdo de confidencialidad de la información a la que tuvo acceso en la entidad.

12.4. Procedimientos de Control de Seguridad

12.4.1. Tipos de eventos registrados

La Entidad Certificadora Pública AGETIC almacena registros de los eventos (Logs) de seguridad más significativos relativos a su actividad como Entidad Certificadora Pública. Estos registros son almacenados automáticamente, así mismo en los casos del acceso físico se debe autorizar y registrar de acuerdo a los planes y procedimientos de seguridad de la Entidad Certificadora Pública AGETIC.

Los registros mínimos de los eventos relacionados con la seguridad de la infraestructura de clave pública son los siguientes:

- Instalación y Configuración de los Sistemas Operativos.
- Instalación y Configuración de aplicaciones instaladas
- Instalación y Configuración del Módulo Criptográfico.
- Accesos o intentos de acceso al equipo.
- Actualizaciones.
- Mantenimientos.
- Eventos del software de certificación:
    - Gestión de usuarios.
    - Gestión de Roles.
    - Gestión de Certificados (todo lo contemplado en el ciclo su vida)
- Eventos relacionados con el acceso físico

12.4.2. Frecuencia de procesado de los registros logs

La frecuencia con la que se lleva a cabo el procesado de registros de logs, son en el preciso momento que se realiza la operación en los sistemas, aplicaciones y servicios de la Entidad Certificadora Pública AGETIC.

La Entidad Certificadora Pública AGETIC dispone de herramientas tecnológicas para el monitoreo continuo de las operaciones realizadas en el equipamiento tecnológico de la infraestructura de clave pública.

12.4.3. Periodo de retención para los logs de auditoría

Los periodos de retención de registros se mantienen por un período de dos (2) años.
Los sistemas, aplicaciones y servicios de la Entidad Certificadora Pública AGETIC tendrán periodos de retención de logs de auditoría según el Procedimiento de Gestión de logs definido.

12.4.4. Protección de los logs de auditoría

La Entidad Certificadora Pública AGETIC dispone de medidas para garantizar la disponibilidad, integridad y conservación de los logs de auditoría de los sistemas, aplicaciones y servicios asociados al servicio y la infraestructura tecnológica para a la emisión de certificados digitales

12.4.5. Procedimientos de copia de seguridad de los logs de auditoría

Se generan copias de respaldo incrementales, de acuerdo a la Política de Respaldo, Resguardo y Recuperación y Procedimiento de Gestión de Logs.

12.4.6. Sistema de recogida de información de auditoría

La Entidad Certificadora Pública AGETIC tiene implementado un sistema de centralización de logs el cual monitorea y notifica eventos que se presentan dentro del equipamiento tecnológico del servicio de Certificación Digital, el cual combina procesos automáticos y manuales.

12.4.7. Notificación al sujeto causa del evento

No estipulado.

12.4.8. Análisis de vulnerabilidades

A fin de estar preparados ante contingencias que involucren interrupciones en el servicio de certificación digital y garantizar la continuidad del mismo, se realiza análisis de vulnerabilidades en los sistemas, aplicaciones y servicios críticos relacionadas con la Entidad Certificadora Pública AGETIC.

Los análisis son internos y externos, esta última para tener independencia de valoración en cuanto a la criticidad de la información.

Se tiene un procedimiento de plan de pruebas que incluye la realización de análisis de vulnerabilidades y otros que son necesarios en el CPD.

12.5. Archivo de información y registros

La Entidad Certificadora Pública AGETIC garantiza o toma las acciones para que la información generada producto de la emisión de certificados digitales se almacene durante un periodo de tiempo apropiado.

La documentación confidencial generada por la Entidad Certificadora Pública AGETIC almacenada en soportes de información físicas y digitales contienen niveles de seguridad tanto físicas como lógicas.

Los archivos de registros se mantienen bajo estricto control de acceso y están sujetos a la inspección de auditores, que, para los fines de control, podrá ser verificado por la ATT.

12.5.1. Tipo de información y eventos registrados

La Entidad Certificadora Pública AGETIC archivará la información referente a:

- Registro de usuarios
- Solicitud de certificados
- Renovación de certificados
- Revocación de certificados
- Reemisión de certificados.

12.5.2. Periodo de retención para el archivo

Todos los registros de la Entidad Certificadora Pública AGETIC referentes a la operación de sus servicios de certificación son archivados conforme a la normativa de conservación de documentos del Estado Plurinacional de Bolivia.

12.5.3. Sistema de recogida de información para auditoría

Cada uno de los servidores de certificación posee un módulo para almacenar los registros de eventos de certificación, dicho registro permite ser utilizados para auditorías, verificando los intentos de acceso, los accesos y las operaciones dañinas, sean éstas intencionales o no, como también las operaciones normales realizadas para la firma de certificados.

12.5.4. Procedimientos para obtener y verificar información archivada

La información descrita en el punto anterior se la podrá obtener bajo una solicitud dirigida a la Dirección General Ejecutiva de la AGETIC, explicando los motivos de la solicitud, que tras el análisis de este se aceptará o no el acceso a esta información.

12.6. Cambio de clave de la AGETIC

La Entidad Certificadora Pública AGETIC procederá a la renovación o cambio de su par de claves (pública y privada) ante las siguientes situaciones:

- Compromiso de seguridad: Si se determina o sospecha fundadamente que la clave privada de la ECP ha sido comprometida, robada o perdida.
- Expiración técnica: Al cumplirse el periodo de vigencia del certificado emitido por la Entidad Certificadora Raíz (ATT), el cual tiene una duración máxima de diez (10) años.
- Falla de infraestructura: Ante un desastre o falla crítica de los módulos criptográficos (HSM) que impida la recuperación operativa mediante los planes de contingencia.
- Actualización tecnológica: Por cambios en los estándares criptográficos nacionales o internacionales que exijan la adopción de algoritmos más robustos.

12.7. Recuperación de la clave de la AGETIC

La recuperación de la clave privada de la Entidad Certificadora Pública es un proceso crítico que se rige estrictamente por los Planes y Procedimientos para la Continuidad del Servicio y Plan de Contingencias.

Resguardo en HSM: La clave privada se mantiene siempre cifrada dentro del hardware criptográfico con certificación FIPS 140-2 Nivel 3.

Procedimiento de Restauración: En caso de falla del equipo principal, la recuperación (reconstitución) de las claves se realiza exclusivamente en un equipo de respaldo mediante el uso de las partes del secreto criptográfico distribuidas en dispositivos de activación (tokens PED). Este acto requiere obligatoriamente la concurrencia física y lógica del personal autorizado bajo el esquema de control multipersonal M de N.

12.8. Procedimientos para recuperación de desastres

La Entidad Certificadora Pública AGETIC cuenta con un documento de Planes y Procedimientos para la Continuidad del Servicio y un Plan de Contingencias, mediante el cual se inicia un proceso de recuperación que cubre los datos, el hardware y el software crítico, y de esa manera iniciar nuevamente sus operaciones en caso de un desastre natural o causado por humanos. El documento Planes y Procedimientos para la Continuidad del Servicio es revisado periódicamente según cambios de los riesgos en el ambiente.

El Plan y Procedimiento para la Continuidad del Servicio está orientado a:

- Fallas/corrupción de recursos de computación;
- Compromiso de la integridad de la clave; y
- Desastres naturales y terminación.

La Dirección General Ejecutiva deberá decidir sobre las acciones correctivas y comenzar las actividades necesarias para restablecer el sistema de certificación en el momento de presentarse un escenario de desastre. En el Plan y Procedimiento para la Continuidad del Servicio, se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre.

12.9. Cese de actividades de la Entidad Certificadora Pública AGETIC

El cese de actividades de la AGETIC como Entidad Certificadora Pública se produciría únicamente ante una modificación de la Ley N.º 164 o de los Decretos Supremos que le otorgan esta competencia. El procedimiento garantiza la protección de los titulares mediante los siguientes pasos:

- Notificación y Publicidad: Se informará a la ATT y al público con una antelación mínima de sesenta (60) días calendario mediante el sitio web oficial y medios de

difusión nacional.

- Suspensión de Emisiones: A partir del anuncio, la AGETIC dejará de emitir nuevos certificados, renovaciones o reemisiones.
- Transferencia de Custodia: La entidad gestionará, previa aprobación de la ATT, la transferencia segura de los certificados vigentes, registros de auditoría y documentación de respaldo a la entidad pública que la normativa determine.
- Emisión de CRL Final: Se emitirá una última Lista de Certificados Revocados que permanecerá disponible hasta que expire el último certificado emitido por la entidad.
- Resguardo Histórico: Toda la información técnica y administrativa será conservada por un periodo de cinco (5) años posteriores al cese, conforme a los procedimientos de conservación de documentos del Estado.

12.9.1. Sujetos involucrados

El cese de actividades de la Entidad Certificadora Pública AGETIC involucrará directamente a todos los usuarios titulares de los certificados digitales.

12.9.2. Procedimiento para el cese de actividades

El período de implementación del procedimiento para el cese de actividades se realizará desde la declaración de cese de actividades hasta la inhabilitación lógica y física de la Entidad Certificadora Pública AGETIC, a partir de la declaración de cese de actividades la AGETIC ya no emitirá certificados digitales de solicitudes nuevas, renovaciones y reemisiones, solo publicará la lista de certificados revocados.

12.9.2.1. Publicación

Ante la declaración del cese de actividades de la Entidad Certificadora Pública AGETIC, la primera tarea será publicar la información en el sitio web: **www.firmadigital.bo** y **www.agetic.gob.bo** así mismo se publicará en un medio de difusión nacional para conocimiento de todos los usuarios.

12.9.2.2. Notificación

La Entidad Certificadora Pública AGETIC, notificará a todos los usuarios titulares del cese de actividades cuyos certificados permanezcan en vigencia. La misma se llevará a cabo con una antelación mínima de dos (2) meses.

La notificación se realizará mediante correo electrónico firmado digitalmente y mediante los sitios web **www.firmadigital.bo** y **www.agetic.gob.bo** por el transcurso del tiempo que dure la transición del servicio a otra entidad. Las mismas indicarán las fechas precisas del cese de actividades, señalando además que, de no existir objeción a la transferencia de los certificados digitales dentro del plazo de quince (15) días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido la transferencia de los mismos.

12.9.3. Solicitudes de certificados

Una vez anunciado el cese de actividades de la Entidad Certificadora Pública AGETIC, se rechazará la solicitud de emisión de un nuevo certificado, de cualquier tipo, ya sea por renovación, reemisión o solicitudes nuevas por parte del signatario dentro de los sesenta (60) sesenta días calendarios anteriores a la fecha prevista para el cese.

12.9.4. Revocación de Certificados y Lista de Certificados Revocados

La Entidad Certificadora Pública AGETIC deberá proceder de la siguiente manera para la revocación de los certificados.

a) Se podrá revocar certificados digitales hasta el mismo día y hora del cese de actividades. Solamente podrá efectuar revocaciones a solicitud de los usuarios titulares. Si los usuarios titulares, después de haber sido notificados del cese de actividades de la Entidad Certificadora, dentro del plazo de quince (15) días calendario, se entenderá que el usuario ha consentido la transferencia del certificado digital.
b) Se realizará una transferencia de los certificados emitidos a sus usuarios titulares a favor de otra entidad certificadora, según lo establecido en la Ley 164, previo acuerdo entre ambas entidades certificadoras, con aprobación de la ATT como Entidad Certificadora Raíz.
c) Actualizará la lista del repositorio de los certificados digitales.
d) Emitirá una lista de certificados revocados (CRL) hasta la fecha prevista de cese de actividades.
e) Inmediatamente de revocados los certificados, la Entidad Certificadora Pública AGETIC emitirá una última lista de certificados revocados.
f) La última lista CRL estará disponible para consultas, como mínimo hasta el último día del cese de funciones.

12.9.5. Desactivación y custodia de los equipos

A partir del cese de actividades, los equipos de la Entidad Certificadora Pública AGETIC, incluidos los que soportan a la clave privada, quedarán desafectados de la emisión y revocación de certificados. No obstante, permanecerán en custodia de la AGETIC, para:

a) Satisfacer eventuales requerimientos de información, en caso de que suscitaron conflictos.
b) La posible necesidad de rehacer la última lista de certificados revocados.

Después, del periodo de custodia, la Entidad Certificadora Pública AGETIC podrá disponer libremente de los equipos que hubiese dispuesto para el servicio de la certificación digital.

En forma previa a la desactivación se generarán copias de respaldo de toda la información disponible.

Los equipos de publicación de CRL continuarán prestando el servicio hasta la finalización del último día de la fecha del cese de actividades de la Entidad Certificadora Pública AGETIC, según lo mencionado en el punto “5.9.2.4. Revocación de Certificados y Lista de Certificados Revocados” del presente documento.

12.9.6. Transferencia de certificados

Al producirse el cese de sus actividades, la Entidad Certificadora Pública AGETIC realizará una transferencia de los certificados emitidos a sus signatarios a favor de otra entidad certificadora, establecido en la Ley 164. Para ello se requerirá un acuerdo previo entre ambas entidades certificadoras, con aprobación de la ATT como Entidad Certificadora Raíz, que deberá ser firmado por las máximas autoridades respectivas.

Dicho acuerdo debe indicar que la Entidad Certificadora continuadora recibirá los certificados y toma a su cargo la administración de la totalidad de los certificados emitidos por la Entidad Certificadora Pública AGETIC que cesa sus actividades, que no hubieran sido revocados a la fecha de la transferencia. Se enviará copias del mencionado acuerdo a la ATT para su archivo.

La Entidad Certificadora Pública AGETIC transferirá a la Entidad Certificadora continuadora toda la documentación que obre en su poder y que hubiera generado en el proceso de emisión y administración de certificados, así como la totalidad de los archivos y copias de resguardo, en cualquier formato y toda otra documentación referida a su operatoria.

12.9.7. Procedimientos

Una vez anunciada la fecha del cese de funciones de la Entidad Certificadora Pública AGETIC, se socializará y comunicará a todo el personal, directa o indirectamente involucrado, sobre las acciones a asumir para el cese de actividades de la Entidad Certificadora Pública AGETIC.

El Comité de Calidad, Seguridad de la Información y de Emergencia de la Entidad Certificadora ejercerá la supervisión de las operaciones relacionadas, tomando en cuenta el resguardo de la información generada.

12.9.8. Resguardo de información histórica

Al finalizar el cese de actividades, la Entidad Certificadora Pública AGETIC deberá resguardar una importante cantidad de información. Los plazos para la conservación de documentos están detallados en el documento de Procedimientos y Condiciones para la Conservación de Documentos Físicos y Digitalizados de la Entidad Certificadora.

Asimismo, la Entidad Certificadora Pública AGETIC conservará toda la información relacionada con su servicio de certificación digital, detalladas a continuación:

- Los archivos de documentación presentada por solicitantes y usuarios titulares.
- La documentación relacionada con pedidos de revocación.
- La documentación generada en las ceremonias digitales.
- La última lista de certificados revocados.El respaldo de los servidores y de su configuración.
- Los libros de Actas.

13. Controles de Seguridad Técnica

13.1. Generación e instalación de par de claves

13.1.1. Generación del par de claves

La Entidad Certificadora Pública AGETIC genera su par de claves (pública y privada) bajo los procedimientos establecidos en la entidad y en cumplimiento de la normativa vigente con respecto a la certificación digital y las regulaciones de la ATT como ente regulador.

El resguardo de la clave privada se desarrolla conforme a la regulación establecida por la ATT.

13.1.2. Entrega de la clave privada y pública a la AGETIC

La Entidad Certificadora Pública AGETIC dispone de los procedimientos para la generación de su propio par de claves (pública y privada), por lo que no se realiza la entrega de estos bajo los procedimientos actuales.

13.1.3. Entrega de la clave pública y privada a los usuarios titulares

Las claves serán generadas por el solicitante, utilizando aplicaciones y/o herramientas proveídas por la Agencia de Registro o Entidad Certificadora Pública AGETIC, por lo que la responsabilidad de la clave privada es del signatario.

13.1.4. Tamaño de las claves

Los módulos de la raíz de certificación y las claves tienen una longitud de al menos 4096 bits y utiliza el algoritmo RSA.

El tamaño de las claves RSA de los signatarios será de 2048 bits para los certificados para persona natural y persona jurídica.

13.1.5. Parámetros de generación de la clave pública y comprobación de la calidad de los parámetros

Los parámetros utilizados se basan en el estándar ITU X.509 “Information Technology – Open System Interconnection – The Directory: Public Key and attribute certificate frameworks” y en el RFC 5280.

13.1.6. Hardware y software de generación de claves

El hardware criptográfico utilizado por la Entidad Certificadora Pública AGETIC cumple con el estándar FIPS 140-2 nivel 3.

El software utilizado por la Entidad Certificadora Pública AGETIC para la generación del par de claves y certificados es “Enterprise Java Beans Certificate Authority” (EJBCA), software libre mantenido por PrimeKey bajo una licencia GNU General Public License.

13.1.7. Fines del uso de la clave

La clave privada de la Entidad Certificadora Pública AGETIC puede ser usada para:

- Firma de Certificados Digitales establecidos en la presente Declaración de Prácticas de Certificación y en la Políticas de Certificación.
- Firma de Certificados Digitales para la firma de listas de Certificados Revocados (CRL) y OCSP.
- Firma de Certificados Digitales para la certificación cruzada.

13.2. Protección de la clave privada

13.2.1. Estándares para los módulos criptográficos

Los módulos criptográficos utilizados por la Entidad Certificadora Pública AGETIC cumplen con el estándar FIPS 140-2 nivel 3.

13.2.2. Controles Multipersonales de la clave privada

Se utiliza un control multipersonal para el acceso a la clave privada, según los roles asignados a los funcionarios de la Entidad Certificadora Pública AGETIC y que participan de las ceremonias de firma de certificados.

El control multipersonal es la implementación de la autenticación M de N, que implica una división de la contraseña de autenticación en múltiples partes o divisiones. La contraseña compartida se distribuye entre varios tokens PED, donde es necesario contar con M=2 de N=4 para poder acceder al par de claves situado en el HSM.

La autenticación M de N permite hacer cumplir el control de acceso multipersona donde ninguna persona puede acceder al HSM sin la cooperación de otros titulares.

13.2.3. Custodia de la clave privada

La Entidad Certificadora Pública AGETIC ha generado su par de claves (pública y privada) en un módulo HSM certificado por el estándar FIPS 140-2 nivel 3.

13.2.4. Copia de seguridad de la clave privada

Copia de la clave privada de la Entidad Certificadora Pública AGETIC está resguardada en módulos HSM certificado por el estándar FIPS 140-2 nivel 3 protegidos física y lógicamente.

13.2.5. Archivo de la clave privada

La clave privada de la Entidad Certificadora Pública AGETIC se encuentra almacenada en un componente de hardware denominado HSM, certificado por el estándar FIPS 140-2 nivel 3, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son almacenados, por lo que la AGETIC se asegura de mantener en resguardo en un lugar seguro y en un ambiente controlado dentro del CPD.

13.2.6. Introducción de la clave privada al módulo criptográfico

La Entidad Certificadora Pública AGETIC dispone de lineamientos donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico, las mismas se detallan a continuación:

- Genera el nuevo par de claves en el nuevo Módulo de Seguridad.
- Instala el software necesario para generar el CSR utilizando el par de claves generados anteriormente.
- La ATT emite el certificado digital, para el CSR enviado.
- Instala el certificado digital emitido por la ATT.

13.2.7. Método de activación de la clave privada

Para la activación de la clave privada es necesario utilizar los dispositivos tokens PED, se requiere dos de los cuatro tokens de administrador y una de dos tokens de Oficiales, adicionalmente es necesario el acceso al sistema operativo del servidor de certificación.

13.2.8. Método de destrucción de la clave privada

Una vez finalizada la firma de certificados el módulo criptográfico y el servidor HSM son desactivados.

La destrucción de la clave privada implica, generalmente, la revocación del certificado correspondiente.

La clave privada será destruida de forma segura conforme a los procedimientos y dentro del HSM, junto con todas las copias de seguridad.

13.2.9. Clasificación de los módulos criptográficos

La Entidad Certificadora Pública AGETIC utiliza módulos criptográficos HSM certificados con FIPS-2 nivel 3.

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

13.3.1. Archivo de la clave pública

La Entidad Certificadora Pública AGETIC realiza la respectiva publicación de su clave pública hasta el vencimiento del último certificado emitido que deba verificarse con esta.

13.3.2. Períodos operativos de los certificados y período de uso para el par de claves

El par de claves de la Entidad Certificadora Pública AGETIC tendrá la misma duración del certificado correspondiente emitido por la ATT que tiene una validez de diez (10) años. Para proseguir con sus operaciones la AGETIC emitirá un nuevo (o utilizara) el par de claves y solicitará el certificado correspondiente a la ATT, conforme a procedimiento.

13.4. Datos de activación

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

13.5. Controles de seguridad informática

La Entidad Certificadora Pública AGETIC tiene definido 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 sobre el ciclo de vida de los sistemas

El software de la Entidad Certificadora Pública AGETIC usado por la clave pública para la emisión de certificado 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 clave pública de la Entidad Certificadora Pública AGETIC cumple con los requerimientos FIPS 140-2 nivel 3. 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 los sistemas, se tienen implementados controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la Entidad Certificadora Pública AGETIC.

Existen controles de seguridad para 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 de la interna de la Unidad de Infraestructura de Servicios de. 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 que alberga 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. Perfiles de Certificado y de la lista de certificados revocados

El perfil de los certificados corresponde con el propuesto en las políticas de certificación particulares y son coherentes con la normativa internacional.

14.1. Perfil del Certificado de la Entidad Certificadora Raíz (ECR)

El formato para el Certificado Digital de la ECR tendrá los siguientes atributos y contenidos:

NOMBRE	VALOR
Versión (versión)	2
Número de Serie (serialNumber)	Asignado por la ECR valor hasta de 20 octetos.
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)

Nombre del Emisor (issuer)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Periodo de validez (validity)	Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Información de la clave pública del suscriptor (subjectPublicKey)	Algoritmo: RSA, Longitud: 4096 bits.

Las extensiones del Certificado Digital de la ECR serán las siguientes:

NOMBRE	VALOR
Identificador de la clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey.
Uso de Claves (keyUsage)	digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
Política de Certificación (certificatePolicies)	URI: (archivo en formato de texto)
Restricciones Básicas (basicConstraints)	CA = TRUE, pathLenConstraint = “1”.
Punto de distribución de las CRL (cRLDistributionPoints)	URI: (.crl).

14.2. Perfil del Certificado de la Entidad Certificadora Pública AGETIC

El formato para el Certificado Digital de la Entidad Certificadora Pública AGETIC tendrá los siguientes atributos y contenidos:

NOMBRE	VALOR
Versión (version)	2
Número de Serie (serialNumber)	Asignado por la ECR
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Periodo de validez (validity)	Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = “Entidad Certificadora Pública AGETIC”; O = “AGETIC”; C = “BO”.
Información de la clave pública del suscriptor (subjectPublicKey)	Algoritmo: RSA, Longitud: 4096 bits.

Las extensiones del Certificado Digital de una ECA serán las siguientes:

NOMBRE	VALOR
Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier)	Identificador de la clave pública de la ECR
Identificador de la clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey.
Uso de Claves (keyUsage)	digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
Política de Certificación (certificatePolicies)	URI: (archivo en formato de texto)

Restricciones Básicas (basicConstraints)	CA = TRUE, pathLenConstraint = “1”.
Punto de distribución de las CRL (cRLDistributionPoints)	URI: (.crl).
Información de Acceso de la ECA (authorityInformationAccess)	URI: (.crt).

14.3. Perfil de la CRL de la Entidad Certificadora Pública

El formato de las Listas de Certificados Revocados tendrá los siguientes contenidos y atributos mínimos:

NOMBRE	VALOR
Versión (version)	1 (corresponde a la versión 2 del estándar)
Algoritmo de firmas (signatureAlgorithm)	Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Pública para firmar la Lista de Certificados Revocados
Nombre del Emisor (issuer)	CN = “Entidad Certificadora Pública AGETIC”; O = “AGETIC”; C = “BO”.
Día y Hora de Vigencia (This Update)	Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
Próxima actualización (Next Update)	Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
Certificados Revocados (Revoked Certificates)	contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas

Las extensiones de la Lista de Certificados Revocados serán, como mínimo, las siguientes:

NOMBRE	VALOR
Identificador de la Clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey (clave pública correspondiente a la clave privada usada para firmar la Lista de Certificados Revocados)
Número de Lista de Certificados	número entero de secuencia

Revocados (CRL Number)	incremental para una CRL y una Entidad Certificadora determinadas.
Extensiones de un elemento de la Lista de Certificados Revocados.	
Código de motivo (Reason code)	indica la razón de revocación de un elemento de la CRL

14.4. Perfil del OCSP de la Entidad Certificadora Pública

La adhesión en cuanto a definiciones, implementación y formatos, a los RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” y 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

1. El requerimiento de inclusión de los siguientes datos en las consultas OCSP:

   a) Versión (version)
   b) Requerimiento de servicio (service request).
   c) Identificador del certificado bajo consulta (target certificate identifier).
   d) Extensiones que puedan incluirse en forma opcional (optional extensions) para su procesamiento por quién responde. Cuando se recibe una consulta OCSP, quien responde debe considerar al menos los siguientes aspectos:

      - Que el formato de la consulta sea el apropiado
      - Que el emisor sea una entidad autorizada para responder la consulta.
      - Que la consulta contenga la información que necesita quien responde
      - Si estas condiciones son verificadas, se devuelve una respuesta. De lo contrario, si alguna de estas condiciones no se cumpliera, se deberá emitir un mensaje de error.

2. Cuando se emite una respuesta OCSP, se sugiere requerir que se consideren los siguientes datos:

   a) Versión.
   b) Identificador de la Entidad Certificadora Autorizada o de la entidad habilitada que emite la respuesta.
   c) Fecha y hora correspondiente a la generación de la respuesta.
   d) Respuesta sobre el estado del certificado.
   e) Extensiones opcionales.
   f) Identificador de objeto (OID) del algoritmo de firma.
   g) Firma de respuesta.

3. Una respuesta a una consulta OCSP debería contener:

   a) Identificador del certificado.

b) Valor correspondiente al estado del certificado, pudiendo este ser de acuerdo con el RFC 5280.
c) Válido (good), respuesta positiva a la consulta lo que implica que no existe un certificado digital revocado con el número de serie contenido en la consulta.
d) Revocado (revoked), es decir certificado revocado.
e) Desconocido (unknown), es decir sin reconocer el número de serie del certificado.
f) Período de validez de la respuesta.
g) Extensiones opcionales.

Las respuestas OCSP están firmadas digitalmente por la Entidad Certificadora Pública AGETIC en el marco de la Infraestructura de Clave Pública de Bolivia.

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

15. Auditoría de Conformidad

La Entidad Certificadora Pública AGETIC está sujeta a auditorías de control y seguimiento establecidas en el marco normativo vigente y son implementadas por la ATT como ente regulador.

15.1. Frecuencia de los controles de conformidad para la AGETIC

La Entidad Certificadora Pública AGETIC está sujeta a las disposiciones de la ATT como Entidad Certificadora Raíz, por lo que la frecuencia de los controles de conformidad está definida por la ATT.

15.2. Relación entre el auditor y la entidad auditada

La relación entre el auditor y la Entidad Certificadora Pública AGETIC como entidad certificadora pública se detalla en el Decreto Supremo 1793 del 13 de noviembre de 2013, que establece en su artículo 46:

- Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.

15.3. Comunicación de resultados

La Entidad Certificadora Pública AGETIC está sujeta a las disposiciones de la ATT como Entidad Certificadora Raíz, por lo que la comunicación de los resultados de las auditorías será definida por la ATT.

16. Otras cuestiones legales y de actividad

16.1. Contrato de adhesión

Los certificados emitidos por la Entidad Certificadora Pública AGETIC, está asociado 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 los plazos establecidos según el documento “Políticas de Certificación”, caso contrario se procederá a la revocación automática del mismo.

16.2. Tarifas

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

El acceso a la información relativa al estado de los certificados o de los certificados revocados es gratuito, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

Las tarifas aplicables a otros servicios relacionados a la certificación digital se negociarán entre la Entidad Certificadora Pública AGETIC y el solicitante del servicio, misma que se pondrá en conocimiento y aprobación de la ATT como ente regulador.

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 presente documento.

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

A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado.
b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas, las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, que requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo con las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.

La Entidad Certificadora Pública AGETIC adoptará las medidas de índole técnica y organizativa necesaria que permitan garantizar la seguridad de los datos personales y eviten su alteración, pérdida y tratamiento no autorizado que deberán ajustarse de conformidad con el estado de la tecnología.

El usuario que se adhiere al servicio de certificación digital de la Entidad Certificadora Pública AGETIC, acepta la publicación por parte de la AGETIC de la información contenida en su clave pública y el certificado firmado por la AGETIC.

16.6. Derechos y Obligaciones de los participantes de la INCD

16.6.1. Derechos y Obligaciones de la Entidad Certificadora Pública

16.6.1.1. Derechos de la Entidad Certificadora Pública

De conformidad a lo establecido en el Artículo 58 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, la Entidad Certificadora Pública tiene los siguientes derechos:

a) Recibir oportunamente el pago por los servicios provistos, de conformidad con los precios o tarifas establecidas.
b) Cortar el servicio provisto por falta de pago por parte de las usuarias o usuarios, previa comunicación, conforme a lo establecido por reglamento.
c) Recibir protección frente a interferencias perjudiciales a operaciones debidamente autorizadas.
d) Otros que se deriven de la aplicación de la Constitución Política del Estado, la Ley N° 164 y demás normas aplicables.

16.6.1.2. Obligaciones de la Entidad Certificadora Pública

De conformidad a lo establecido en el Artículo 59 de la Ley N° 164 Ley General de

Telecomunicaciones, Tecnologías de Información y Comunicación, la Entidad Certificadora Pública tiene las siguientes obligaciones:

a) Someterse a la jurisdicción y competencia de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
b) Proveer en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida, los servicios de telecomunicaciones y tecnologías de información y comunicación.
c) Proporcionar información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a las usuarias o los usuarios.
d) Proporcionar información clara, precisa, cierta, completa y oportuna a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
e) Proveer gratuitamente los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, que determine la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
f) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación según los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
g) Efectuar el reintegro o devolución de montos que resulten a favor de las usuarias o los usuarios por errores de facturación, deficiencias o corte del servicio, con los respectivos intereses legales.
h) Atender las solicitudes y las reclamaciones realizadas por las usuarias o los usuarios.
i) Informar oportunamente la desconexión o cortes programados de los servicios.
j) Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley.
k) Facilitar a las usuarias o usuarios en situación de discapacidad y personas de la tercera edad, el acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en reglamento.
l) Proveer servicios que no causen daños a la salud y al medio ambiente.
m) Actualizar periódicamente su plataforma tecnológica y los procesos de atención a las usuarias y los usuarios.
n) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

Para garantizar la publicidad, seguridad, integridad y eficacia del certificado digital, la Entidad Certificadora Pública tiene las siguientes obligaciones según a lo establecido en el Artículo 43 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;

b) Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT;
c) Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web entre otros medios;
d) Mantener el control, reserva y cuidado de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Cualquier anomalía que pueda comprometer su confidencialidad deberá ser comunicada inmediatamente a la ATT;
e) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
f) Mantener un sistema de información de acceso libre, permanente y actualizado donde se publiquen los procedimientos de certificación digital, así como los certificados digitales emitidos consignando, su número único de serie, su fecha de emisión, vigencia y restricciones aplicables, así como el detalle de los certificados digitales suspendidos y revocados;
g) Las entidades certificadoras que derivan de la certificadora raíz (ATT) deberán mantener un sistema de información con las mismas características mencionadas en el punto anterior, ubicado en territorio y bajo legislación del Estado Plurinacional de Bolivia;
h) Revocar el certificado digital al producirse alguna de las causales señaladas en los puntos anteriores;
i) Mantener la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso;
j) Mantener la información relativa a los certificados digitales emitidos, por un período mínimo de cinco (5) años posteriores al periodo de su validez o vigencia;
k) Facilitar información y prestar la colaboración debida al personal autorizado por la ATT, en el ejercicio de sus funciones, para efectos de control, seguimiento, supervisión y fiscalización del servicio de certificación digital, demostrando que los controles técnicos que emplea son adecuados y efectivos cuando así sea requerido;
l) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
m) Notificar a la ATT cualquier cambio en la personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos o correo electrónico;
n) Verificar toda la información proporcionada por el solicitante del servicio, bajo su exclusiva responsabilidad;
o) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;
p) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidos que administra.

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

De conformidad a lo establecido en el Artículo 44 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación y la Resolución Administrativa RAR-DJ-RA TL LP 845/2018 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, la Responsabilidad de la Entidad Certificadora Pública ante terceros, se da en los siguientes casos:

a) Será responsable por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus usuarios.
b) La entidad certificadora se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.
c) La entidad certificadora responderá por posibles perjuicios que se causen al usuario titular o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

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

Casos Programados

La Entidad Certificadora Pública AGETIC no podrá interrumpir sus servicios, o parte de los mismos, sin la autorización previa y por escrito de la ATT y después de haber informado a los usuarios que resultaren afectados a través de comunicación directa o de un medio de comunicación masivo, por lo menos con cinco (5) días de anticipación, sobre los siguientes casos:

- Interrupción del servicio de generación de Listas de Certificados Revocados (CRL), de más de un (1) día hábil.
- Interrupción de registros, de más de tres (3) días hábiles.
- Interrupción de certificación, de más de tres (3) días hábiles.

Casos no programados

En casos de emergencia, eventos de fuerza mayor o caso fortuito, que justifiquen la interrupción del servicio por más de tres (3) horas continuas por parte de La Entidad Certificadora Pública AGETIC, deberá reportar el cese o interrupción del servicio en el menor plazo posible a la ATT; que en ningún caso podrá exceder los tres (3) días hábiles de ocurrido el hecho.

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 jurídicas que hayan solicitado por sí y para sí una certificación que acredite su firma digital.

16.6.2.1. Responsabilidad del titular

Según lo establecido en el Artículo 53 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular será responsable en los siguientes casos:

a) Por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como titular.
b) El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
c) Asimismo, acorde a los procedimientos de la Entidad Certificadora Pública AGETIC, la entidad no podrá acceder en ningún momento a la clave privada del usuario, por lo que éste es el único responsable de su generación, administración, uso y custodia. En caso de verse comprometida por cualquier razón dicha clave, el usuario deberá informar a la Entidad Certificadora Pública AGETIC a la brevedad posible y solicitar la revocación del certificado digital. Todos los efectos o daños que pudieran ocasionarse al usuario o a terceros, en el transcurso comprendido entre la generación del certificado y su revocatoria, son de exclusiva responsabilidad del usuario.

16.6.2.2. Derechos del Titular del Certificado

De conformidad a lo señalado en el Artículo 54 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular del certificado digital tiene los siguientes derechos:

a) A ser informado por la entidad certificadora de las características generales, de los procedimientos de creación y verificación de firma digital, así como de las reglas sobre prácticas de certificación y toda información generada que guarde relación con la prestación del servicio con carácter previo al inicio del mismo, así como de toda modificación posterior,
b) A la confidencialidad de la información proporcionada a la entidad certificadora;
c) A recibir información de las características generales del servicio, con carácter previo al inicio de la prestación del mismo;
d) A ser informado, antes de la suscripción del contrato para la emisión de certificados digitales, acerca del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, de las condiciones precisas para la utilización del certificado, de las limitaciones de uso, de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o los que se acordaren;
e) A que la entidad certificadora le proporcione la información sobre su domicilio legal en el país y sobre todos los medios a los que el titular pueda acudir para solicitar

aclaraciones, dar cuenta del mal funcionamiento del servicio contratado, o la forma en que presentará sus reclamos;

f) A ser informado, al menos con dos (2) meses de anticipación, por la entidad certificadora del cese de sus actividades, con el fin de hacer valer su aceptación u oposición al traspaso de los datos de sus certificados a otra entidad certificadora.

16.6.2.3. Obligaciones del Titular del certificado

De conformidad a lo señalado en el Artículo 55 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular del certificado digital tiene las siguientes obligaciones:

1. El titular de la firma digital mediante el certificado digital correspondiente tiene las siguientes obligaciones:
   a) Proporcionar información fidedigna y susceptible de verificación a la entidad certificadora;
   b) Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado;
   c) Observar las condiciones establecidas por la entidad certificadora para la utilización del certificado digital y la generación de la firma digital;
   d) Notificar oportunamente a la certificadora que los datos de creación de su firma digital han sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada, en este caso deberá solicitar la baja de su certificado digital;
   e) Actuar con diligencia y tomar medidas de seguridad necesarias para mantener los datos de generación de la firma digital bajo su estricto control, evitando la utilización no autorizada del certificado digital;
   f) Comunicar a la entidad certificadora cuando exista el riesgo de que los datos de su firma digital sean de conocimiento no autorizado de terceros, por el titular y pueda ser utilizada indebidamente;
   g) No utilizar los datos de creación de firma digital cuando haya expirado el período de validez del certificado digital; o la entidad de certificación le notifique la suspensión de su vigencia o la conclusión de su validez;
   h) No delegar el uso del Certificado a terceras personas ni a intermediarios, dado que la responsabilidad por los documentos firmados se asigna directamente al titular del Certificado Digital. Este aspecto no aplica a los Certificados emitidos para Firma Automática.
2. El incumplimiento de las obligaciones antes detalladas, hará responsable al titular de la firma digital de las consecuencias generadas por el uso indebido de su firma digital.

16.6.3. Derechos y Obligaciones de los Usuarios

16.6.3.1. Derechos de las usuarias y usuarios

De conformidad a lo señalado en el Artículo 54 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, las usuarias y usuarios

tienen los siguientes derechos:

a) Acceder en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida a los servicios de telecomunicaciones y tecnologías de información y comunicación.
b) Acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a ser proporcionada por la Entidad Certificadora Pública.
c) Acceder gratuitamente a los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, de acuerdo a determinación de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
d) Recibir de forma oportuna, comprensible y veraz la factura mensual desglosada de todos los cargos y servicios del cual es usuario, en la forma y por el medio en que se garantice su privacidad.
e) Exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.
f) Conocer los indicadores de calidad de prestación de los servicios al público de los proveedores de telecomunicaciones y tecnologías de información y comunicación.
g) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación según los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
h) Ser informado por la Entidad Certificadora Pública oportunamente, cuando se produzca un cambio de los precios, las tarifas o los planes contratados previamente.
i) Recibir el reintegro o devolución de montos que resulten a su favor por errores de facturación, deficiencias, corte del servicio o modificación de tarifas por vigencia de una nueva estructura tarifaría en la venta de dispositivos criptográficos.
j) Obtener respuesta efectiva a las solicitudes realizadas a la Entidad Certificadora Pública.
k) Reclamar ante la Entidad Certificadora Pública y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna.
l) Disponer, como usuaria o usuario en situación de discapacidad y persona de la tercera edad, facilidades de acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en un reglamento especial.
m) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

16.6.3.2. Obligaciones de las usuarias y usuarios

De conformidad a lo establecido en el Artículo 55 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, las usuarias y usuarios tienen las siguientes obligaciones:

a) Pagar sus facturas por los servicios recibidos, de conformidad con los precios o tarifas establecidas.
b) Responder por la utilización de los servicios por parte de todas las personas que tienen acceso al mismo, en sus instalaciones o que hacen uso del servicio bajo su supervisión o control.
c) No causar daño a las instalaciones, redes y equipos de la Entidad Certificadora Pública.
d) Cumplir con las instrucciones y planes que emita la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes en casos de emergencia y seguridad del Estado.
e) No causar interferencias perjudiciales a operaciones debidamente autorizadas.
f) Otros que se deriven de la aplicación de la Constitución Política del Estado, las leyes y demás normas aplicables. Asimismo, en lo que corresponda, se aplicará lo establecido en los Artículos 52 al 55 del Decreto Supremo N° 1793, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

16.7. Obligaciones de los participantes de la INCD

La Entidad Certificadora Pública AGETIC se obliga según lo dispuesto en este documento, así como lo dispuesto en las normativas y reglamentaciones vigentes sobre la prestación del servicio de certificación digital a:

a) Cumplir y hacer cumplir con lo dispuesto en la presente Declaración de Prácticas de Certificación.
b) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT.
c) Publicar esta Declaración de Prácticas de Certificación y las “Políticas de Certificación” en el sitio web de la Entidad Certificadora Pública AGETIC
d) Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, reemisión, tarifas y uso vigentes establecidos para sus certificados digitales, el mismo que deberá ser publicado en el sitio web de la Entidad Certificadora Pública AGETIC.
e) Informar sobre las modificaciones aprobadas de esta Declaración de Prácticas de Certificación a los usuarios y Agencias de Registro que estén vinculadas a la Entidad Certificadora Pública AGETIC, mediante la publicación de éstas y sus respectivas modificaciones en el sitio web de la AGETIC.
f) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario.
g) Revocar el certificado digital al producirse alguna de las causales establecidas en la presente Declaración de Prácticas de Certificación.
h) Mantener la información relativa a los certificados digitales emitidos, por un periodo mínimo de 5 (cinco) años posteriores al periodo de vigencia.

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.

16.8. Modificaciones al presente documento

La responsabilidad de la administración y modificación del presente documento “Declaración de Prácticas de Certificación” corresponde a la Entidad Certificadora Pública AGETIC.

Cuando la Entidad Certificadora Pública AGETIC realice modificaciones a la presente Declaración de Prácticas, estas deberán ser aprobadas por el ente regulador ATT con la correspondiente justificación, la ATT evaluará la solicitud y en caso de aprobarla, realizará la modificación y posterior publicación de la nueva versión.

16.9. Resolución de Conflictos

Toda controversia o conflicto que se derive del presente documento se resolverá mediante una negociación entre el titular y la AGETIC dentro de quince (15) días hábiles después de iniciado el conflicto, posteriormente se someterá dicha controversia a la autoridad de fiscalización y telecomunicaciones ATT como ente regulador de la Entidad Certificadora Pública AGETIC. En caso de no llegar a ningún acuerdo quedará libre la vía de reclamo por proceso legal.

La Entidad Certificadora Pública AGETIC, salvo orden judicial de la autoridad competente, no intervendrá en manera alguna en la resolución de conflictos relacionados con el uso del certificado digital de los titulares con terceros.

El personal de la Entidad Certificadora Pública AGETIC no tendrá en ningún momento acceso a la clave privada de los titulares, por lo mismo se exime de cualquier responsabilidad con respecto a cualquier evento que comprometa dicha clave y las consecuencias derivadas de su uso.

16.10. Legislación aplicable

Las políticas de certificación de la Entidad Certificadora Pública AGETIC fueron elaboradas en el marco de:

- Constitución Política del Estado Plurinacional de Bolivia
- Decreto Supremo 26553 de Creación de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- La Ley N°164 General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- El Decreto Supremo 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- El Decreto Supremo 3527 que modifica el Decreto Supremo 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Las recomendaciones de la (Request for comments) RFC 3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) como encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras según la Ley N.º 164 emite una serie de Resoluciones Administrativas Regulatorias y que fueron consideradas para la elaboración del presente documento:

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, información técnica y legal contenida en el presente documento de Declaración de Prácticas de Certificación, se encuentra elaborado en conformidad a todo lo establecido en la normativa legal vigente, así como en las Resoluciones Administrativas Regulatorias emitidas por la ATT como ente regulador.