



AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria **ATT-DJ-RAR-TL LP 249/2026**

La Paz, 01 de abril de 2026

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 61/2026 de 14 de enero de 2026 (**RAR 61/2026**); la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 201/2026 de 04 de marzo de 2026 (**RAR 201/2026**); el Informe Técnico ATT-DTLTIC-INF TEC LP 306/2026 de 10 de marzo de 2026 (**INFORME TÉCNICO I**); el Informe Jurídico ATT-DJ-INF-JUR LP 442/2026 de 20 de marzo de 2026 (**INFORME JURÍDICO I**); el Informe Técnico ATT-DTLTIC-INF TEC LP 1819/2025 de 09 de diciembre de 2025 (**INFORME TÉCNICO II**); el Informe Jurídico ATT-DJ-INF-JUR LP 483/2026 de 01 de abril de 2026 (**INFORME JURÍDICO II**); los antecedentes del caso, la demás normativa vigente y aplicable, todo lo que convino ver, se tuvo presente, y:

CONSIDERANDO 1.- (ANTECEDENTES).

Que a través de Decreto Supremo N° 5519 de 13 de enero de 2026 (**DS N° 5519**), se realizaron modificaciones e incorporaciones en el Decreto Supremo N° 2514, de 9 de septiembre de 2015, modificado por el Decreto Supremo N° 3900, de 15 de mayo de 2019. El inciso a) del Parágrafo I de la Disposición Adicional Cuarta del **DS N° 5519** establece que, a partir del 15 de enero de 2026, la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC asumirá las funciones de la ADSIB, establecidas en normativa vigente.

Que la Disposición Final Única del **DS N° 5519** establece que, a partir de la entrada en vigencia del referido Decreto Supremo, se adecua en toda la normativa vigente la denominación de Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB por Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC.

Que mediante **RAR 61/2026**, la ATT permitió a la AGETIC, de manera excepcional, la administración y el ejercicio de la autorización para la prestación de servicios de certificación digital otorgada a la ADSIB, mediante la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 43/2021 de 05 de marzo de 2021 (**RAR 43/2021**) y el Contrato de Autorización para la Prestación de Servicios de Certificación Digital ATT-DJ-CON SCD 1/2021 de 05 de marzo de 2021 (**CTTO. SCD 1/2021**), durante el tiempo de su vigencia, es decir hasta el 04 de marzo de 2026, en cumplimiento a lo instruido por el **DS N° 5519**; asimismo, en su Resolución Sexto instruyó a la AGETIC el debido cumplimiento de los requisitos técnicos, legales y económicos a efectos de recabar una nueva licencia al vencimiento de aquellas otorgadas mediante **RAR 43/2021** y el **CTTO. SCD 1/2021**.

Que a través de nota con cite AGETIC/NE/0564/2026, presentada en fecha 26 de febrero de 2026, la AGETIC remitió los requisitos para el servicio de Certificación Digital, considerando que, en el marco de lo establecido en el **DS N° 5519**, la AGETIC asumió funciones de la ex ADSIB, la cual fungía como Entidad Certificadora Autorizada.

Que mediante nota ATT-DTLTIC-N LP 249/2026 de 27 de febrero de 2026, la Dirección Técnica Sectorial de Telecomunicaciones y TIC informó a la AGETIC que, de acuerdo a lo dispuesto en el procedimiento de autorización de entidades certificadoras – AEC, aprobado mediante Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 845/2018, que en su numeral 4.3. Revisión de la Documentación establece que: *"Dicho personal (...) realiza también una evaluación de las capacidades económicas y técnicas para el cumplimiento de las funciones de emisión de certificados, según el alcance establecido en la presentación de la EC solicitante"*. En ese sentido, comunicó que la ATT tiene programada una Auditoría de Cumplimiento presencial a la AGETIC.



Que a través de Informe Técnico ATT-DTLTIC-INF TEC LP 277/2026 de 27 de febrero de 2026, la Dirección Técnica Sectorial de Telecomunicaciones y TIC concluyó que se ha realizado la planificación de Auditoría a la AGETIC, como parte del proceso de revisión de cumplimiento de los requisitos Técnicos y Económicos presentados en su solicitud de autorización de Licencia como Entidad Certificadora Pública.

Que mediante RAR 201/2026, la ATT permitió a la AGETIC, de manera excepcional, la prestación de servicios de certificación digital, a efectos de garantizar su continuidad durante el procedimiento de transferencia iniciado mediante DS N° 5519, hasta la obtención formal de la Autorización para la Prestación de Servicios de Certificación Digital, en su condición de Entidad Certificadora Pública, dentro del plazo de ampliación solicitado; y aceptó la solicitud presentada por la AGETIC otorgándole un plazo de veinte (20) días hábiles administrativos a efectos de que pueda concluir con el trámite para la obtención de la autorización de prestación de servicios de certificación digital, mediante la presentación de la totalidad de los requisitos en la normativa aplicable vigente.

Que a través de INFORME TÉCNICO I, la Dirección Técnica Sectorial de Telecomunicaciones y TIC concluyó que: "(...) Como parte de las atribuciones ejercidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT en su calidad de Entidad Certificadora Raíz, la Unidad de Regulación de TIC ha llevado a cabo la Auditoría de Cumplimiento In Situ de los requisitos remitidos por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC en su solicitud de autorización para la prestación del servicio de certificación digital, de acuerdo a lo establecido en el Decreto Supremo N° 1793 y su modificación Decreto Supremo N° 3527. (...) Como parte de la auditoría de cumplimiento in situ de los requisitos exigidos, la Entidad Certificadora Raíz ha verificado la ejecución de los procedimientos expuestos en los documentos internos de la AGETIC. (...) Del análisis realizado en el presente informe, se establece que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC cumplió con todos los requisitos técnicos y económicos establecidos por la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019 de 16 de abril de 2019. (...) De la revisión técnica al documento de Términos y Condiciones presentado, se determina que el mismo se encuentra acorde al modelo descrito en el "Anexo 3: Contenido Mínimo de los Términos y Condiciones de las Entidades Certificadoras" de la Resolución Administrativa Regulatoria ATT DJ-RAR-TL LP 202/2019 de 16 de abril de 2019, mismo que se adjunta en el ANEXO B del presente informe (...)".

Que, en ese sentido, el INFORME TÉCNICO I recomendó a la Dirección Jurídica, realizar el análisis legal correspondiente a la solicitud de autorización, así como la revisión de los documentos de "Términos y Condiciones" y el "Modelo de Contrato", conforme normativa vigente, para que, en caso de no existir observaciones por la parte legal, continuar el procesamiento del trámite de solicitud de Licencia; posteriormente, remitir el informe de revisión de documentos legales a la Unidad de Tecnologías de Información con la emisión de un informe legal de cumplimiento para continuar con el proceso de Auditoría Técnica de seguimiento en el proceso de autorización y la emisión de la nota a la AGETIC requiriendo la presentación de la respectiva Garantía de cumplimiento de Contrato y el pago por concepto de Tasa de Fiscalización y Regulación.

Que mediante INFORME JURÍDICO I, la Dirección Jurídica concluyó que: "(...) De la revisión del marco normativo legal se tiene que, la AGETIC presentó toda la documentación legal exigida por la ATT y la normativa aplicable para la solicitud de Autorización de Funcionamiento como Entidad Certificadora Pública. De igual manera, no se tienen observaciones al Contrato de Adhesión ni a los Términos y Condiciones presentados, por tanto, se recomienda continuar con el trámite y remitir el presente Informe Jurídico a la Dirección Técnica Sectorial de Telecomunicaciones y TIC. (...)".

CONSIDERANDO 2.- (MARCO NORMATIVO).

Que el numeral 2 del Parágrafo II del Artículo 298 de la Constitución Política del Estado determina que son competencias exclusivas del nivel central del Estado, el régimen general de las comunicaciones y las telecomunicaciones.



Que el Artículo 71 de la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación (**LEY N° 164**), declara como prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos.

Que el Artículo 81 de la **LEY N° 164**, establece que la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras de acuerdo a lo establecido en la presente Ley y su reglamentación.

Que el Artículo 82 de la **LEY N° 164** dispone que pueden constituirse y operar como entidades certificadoras, las personas jurídicas de derecho público o privado en la prestación de servicios de certificación digital, las que deben cumplir con los requisitos técnicos, económicos y legales establecidos en la Ley y su reglamento.

Que el Artículo 83 de **LEY N° 164**, señala que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB, prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la citada Ley y velará por la autenticidad, integridad y no repudio entre las partes; no obstante, a través de **DS N° 5519**, se dispuso en el inciso a) del Parágrafo I de la Disposición Adicional Cuarta que, a partir del 15 de enero de 2026, la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC asumirá las funciones de la ADSIB, establecidas en normativa vigente.

Que el Decreto Supremo N° 2514 de 09 de septiembre de 2026 crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC; así como los Comités Interinstitucionales de Simplificación de Trámites.

Que el Artículo Único del Decreto Supremo N° 1793 de 13 de noviembre de 2013, aprueba el Reglamento a la Ley N° 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación (**REGLAMENTO TIC**), modificado a través de Decreto Supremo N° 3527 de 11 de abril de 2018.

Que el Artículo 24 del **REGLAMENTO TIC** establece que los certificados digitales deben ser emitidos por la entidad certificadora, responder a formatos y estándares reconocidos internacionalmente y fijados por la ATT, contener como mínimo los datos que permitan identificar a su titular, a la entidad certificadora que lo emitió, su periodo de vigencia y completar la información necesaria para la verificación de la firma digital.

Que el Parágrafo II del Artículo 27 del **REGLAMENTO TIC** dispone que la ATT mediante Resolución Administrativa establecerá el formato y estructura de los certificados digitales tanto para personas naturales como para personas jurídicas.

Que el Parágrafo II del Artículo 28 del **REGLAMENTO TIC** señala que los requisitos mínimos para la obtención del Certificado Digital serán establecidos por la ATT, mediante Resolución Administrativa de acuerdo al tipo de Certificado.

Que el Parágrafo IV del Artículo 32 del **REGLAMENTO TIC** establece que la ATT mediante Resolución Administrativa determinará el procedimiento y las condiciones que deberán cumplir las entidades certificadoras para la conservación de los documentos físicos y digitalizados, asegurando el almacenamiento de los mismos en servidores ubicados en el territorio y bajo la legislación del Estado Plurinacional de Bolivia.

Que el numeral 1 el artículo 37 del **REGLAMENTO TIC**, dispone que, la organización de la Infraestructura Nacional de Certificación Digital, tiene como Primer nivel a la Entidad Certificadora Raíz, a la ATT, que es la entidad de certificación de nivel superior dentro de la Jerarquía Nacional de Certificación Digital que auto firmará su certificado y emitirá certificados digitales a las entidades certificadoras públicas y privadas subordinadas. Por su parte, el numeral 2 del Artículo 37 señala como segundo nivel a las Entidades Certificadoras como aquellas entidades certificadoras pública o privadas subordinadas de la Entidad Certificadora Raíz. La entidad certificadora pública es la ADSIB (Ahora AGETIC) y las entidades



E-LP-1883/2026

certificadoras privadas, son todas aquellas autorizadas por ATT a prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

Que el inciso a) del Artículo 38 del **REGLAMENTO TIC** establece dentro de las funciones de la ATT, el autorizar la operación de entidades de certificación.

Que el Artículo 47 del **REGLAMENTO TIC** señala que, la ATT, mediante la firma de un contrato, otorgará la autorización para la prestación de servicios de certificación digital, con una vigencia de cinco (5) años, renovables por periodos similares, a personas naturales o jurídicas que así lo soliciten, previo cumplimiento de los requisitos y condiciones establecidos en Resolución Administrativa por la ATT.

Que a través de Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 845/2018 de 13 de noviembre de 2018 (**RAR 845/2018**), la ATT aprobó los Documentos Públicos de la Entidad Certificadora Raíz – ECR en cumplimiento de lo establecido por el Decreto Supremo N° 3527, que modificó el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

Que mediante Resolución Administrativa Regulatoria RAR ATT-DJ-RAR-TL LP 202/2019 de 16 de abril de 2019 (**RAR 202/2019**), la ATT aprobó los Estándares Técnicos y otros Lineamientos establecidos para el Funcionamiento de las Entidades Certificadoras, en cumplimiento de lo establecido por el Decreto Supremo N° 3527 de 11 de abril de 2018 que modificó el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

CONSIDERANDO 3.- (FUNDAMENTOS).

Que a través del Informe Técnico ATT-DTLTIC-INF TEC LP 1819/2025 de 09 de diciembre de 2025 (**INFORME TÉCNICO II**), la Dirección Técnica Sectorial de Telecomunicaciones y TIC señaló que "(...) la AGETIC mediante nota AGETIC/NE/0776/2026 ha manifestado la necesidad de efectuar adecuaciones adicionales tanto en los componentes de software como en los procesos de producción asociados a la emisión, validación y gestión del ciclo de vida de los certificados digitales que mantiene activos transferidos por la exADSIB, solicitando un plazo de adecuación hasta el 31 de julio de 2026 con el propósito de concluir de manera integral y controlada las tareas técnicas y operativas en curso para la puesta en producción del nuevo certificado a su nombre. (...) Hasta que ello ocurra, la AGETIC solicita continuar operando con el certificado digital otorgado a la exADSIB. Este certificado fue generado en abril del 2025, y tiene una vigencia operativa de 10 años, por lo que técnicamente no se tiene riesgo de afectación del servicio de certificación digital manteniendo el uso de dicho certificado. (...) Esta situación responde a la necesidad operativa de mantener la continuidad del servicio de firma digital durante el período de transición, atendiendo solicitudes de renovación, revocación y reemisión de certificados a suscriptores, en cumplimiento de la Disposición Adicional Sexta del Decreto Supremo D.S. 5519 de 13 de enero de 2026, que establece la plena validez y vigencia de las certificaciones, registros, acuerdos, convenios y contratos suscritos por la ADSIB con personas naturales, jurídicas, instituciones y entidades públicas y privadas, nacionales e internacionales. (...)".

Que, en ese sentido, el **INFORME TÉCNICO** concluyó que: "(...) La AGETIC habría remitido los requisitos técnicos y económicos verificados mediante informe técnico ATT-DTLTIC-INF TEC LP 306/2026, y requisitos jurídicos verificados mediante informe jurídico ATT-DJ-INF JUR LP 442/2026 que se establecen en el proceso de autorización de entidades certificadora aprobado por las RAR ATT-DJ-RAR-TL LP 202/2019 y ATT DJ-RAR-TL LP 845/2018 cumpliendo además las políticas, procesos y procedimientos requeridos verificados mediante informe de auditoría ATT-DTLTIC-INF TEC LP 361/2026. (...)". En ese sentido, recomendó remitir el presente informe a Dirección Jurídica para la evaluación legal a la solicitud realizada por la AGETIC en su nota AGETIC/NE/0776/2026 y la emisión del acto administrativo correspondiente para la Autorización de Prestación de Servicios de Certificación Digital y la firma del Contrato de Autorización para la prestación de servicios de Certificación Digital por parte de la AGETIC de



acuerdo a lo establecido en el procedimiento de autorización aprobado como parte de los documentos públicos de la Entidad Certificadora Raíz por la ATT-DJ-RAR-TL LP 845/2018.

Que mediante **INFORME JURÍDICO II**, la Dirección Jurídica señaló que: "(...) *Por los argumentos precedentemente señalados, en concordancia con lo determinado en el INFORME TÉCNICO, se concluye que, de la revisión del marco normativo legal, la AGETIC presentó toda la documentación exigida por la ATT y la normativa aplicable para el otorgamiento de autorización para la prestación de servicios de Certificación Digital como Entidad Certificadora Pública. En ese sentido, se recomienda la emisión de la correspondiente Resolución Administrativa Regulatoria de autorización, así como la aprobación del Contrato de Adhesión, Términos y Condiciones y formalización de Contrato de autorización para la prestación de servicios de certificación digital a favor de la AGETIC, de acuerdo a lo establecido por el Artículo 47 del REGLAMENTO TIC. (...)*".

POR TANTO:

El Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, Lic. CARLOS ALBERTO AGREDA LEMA, designado mediante Resolución Suprema N° 32097 de 13 de noviembre de 2025, en ejercicio de sus atribuciones conferidas por ley y demás normas vigentes;

RESUELVE:

PRIMERO. - DISPONER el otorgamiento de Autorización para la prestación de servicios de Certificación Digital como Entidad Certificadora Pública, a través de la formalización de Contrato a favor de la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - AGETIC**, de acuerdo a lo establecido por el artículo 47 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

SEGUNDO. - INSTRUIR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - AGETIC** concluir hasta el 31 de julio de 2026, de manera integral y controlada las tareas técnicas y operativas en curso para la puesta en producción del nuevo certificado a su nombre, en tanto, los certificados digitales podrán ser emitidos o renovados operando el certificado digital otorgado a la ex **AGENCIA PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN EN BOLIVIA - ADSIB**, excepcionalmente.

TERCERO. - ESTABLECER que la Autorización otorgada a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - AGETIC**, tendrá una vigencia de cinco (5) años computables a partir de la fecha de suscripción del Contrato.

CUARTO. - APROBAR el Contrato de Adhesión y los Términos y Condiciones para la provisión de servicios de certificación digital, presentados por la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - AGETIC**, de conformidad a lo previsto por el numeral 14 del Artículo 14 de la Ley N° 164 y el Artículo 28 del Reglamento a la Ley N° 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación aprobado por Decreto Supremo N° 1793 de 13 de noviembre de 2013, de acuerdo a lo establecido en el Anexo A y Anexo B respectivamente, que forman parte integrante e indivisible de la presente Resolución Administrativa Regulatoria, de conformidad a lo previsto por el numeral 14 del Artículo 14 de la Ley N° 164.

QUINTO. - INSTRUIR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - AGETIC** que cualquier modificación de la Autorización otorgada deberá ser solicitada de manera previa a la ATT, para la emisión del acto administrativo que autorice la misma, en el marco de lo establecido por la normativa vigente y aplicable



SEXTO. - INSTRUIR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – AGETIC** la presentación anual de la Boleta de Garantía de Contrato, conforme lo establece el artículo 45 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

SÉPTIMO. - INSTRUIR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – AGETIC** efectuar el pago anual correspondiente a la Tasa de Fiscalización y Regulación conforme lo establece el artículo 48 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

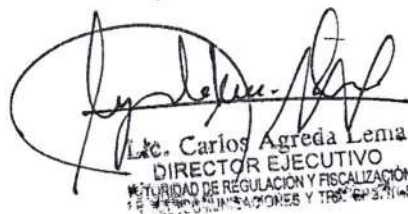
OCTAVO. - DISPONER que la Autorización otorgada a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – AGETIC** permanecerá sujeta a las disposiciones administrativas emergentes de la jurisdicción y competencia de la ATT, que emanan de la Ley N° 164, su Reglamento aprobado mediante Decreto Supremo N° 1793 y demás disposiciones legales vigentes.

NOVENO. - OCTAVO. - INSTRUIR a la Unidad de Regulación de Tecnologías de Información y Comunicación dependiente de la Dirección Técnica Sectorial de Telecomunicaciones y TIC registrar la presente Resolución Administrativa Regulatoria.

DÉCIMO. - INSTRUIR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – AGETIC**, en atención a la normativa vigente y aplicable, deberá realizar su aporte al Programa Nacional de Telecomunicaciones de Inclusión Social PRONTIS.

DÉCIMO PRIMERO. - NOTIFICAR a la **AGENCIA DE GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – AGETIC**, en la Calle Pedro Salazar N° 631 esq. Andrés Muñoz, Zona San Sopocachi de La Paz, Teléf. (s): 2184026, de conformidad a lo establecido por el inciso b) del artículo 13 del Reglamento a la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial – SIRESE, aprobado mediante Decreto Supremo N° 27172 de 15 de septiembre de 2003.

Regístrese y archívese.


Lic. Carlos Agreda Lema
DIRECTOR EJECUTIVO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES



E-LP-1883/2026



AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES
Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026

**ANEXO A
CONTRATO DE ADHESIÓN**

CONTRATO DE ADHESIÓN PARA LA PROVISIÓN DE SERVICIOS DE CERTIFICACIÓN DIGITAL

Conste por el presente Contrato de Adhesión para la **PROVISIÓN DE SERVICIOS DE CERTIFICACIÓN DIGITAL**, que con el reconocimiento de firmas y rúbricas surtirá efectos de documento público, sujeto a las siguientes cláusulas:

PRIMERA (PARTES CONTRATANTES). -

Intervienen en la suscripción del presente Contrato:

1.1.- ENTIDAD CERTIFICADORA (EC): Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, representada legalmente por el Lic. Carlos Eduardo Rodrigo Prado con Cédula de Identidad N° 4455831 expedida en La Paz, designado como Director General Ejecutivo interino, en mérito a la Resolución Suprema N° 32131 de 24 de noviembre de 2025, que para efectos de este Contrato se denominará **EC**.

1.2.- LLENAR EN CASO DE PERSONA NATURAL

El/la Sr./ra..... con C.I. N°....., con domicilio legal en....., que en lo sucesivo se denominará el **USUARIO(A)**.

LLENAR EN CASO DE PERSONA JURÍDICA

La [Empresa o Entidad Pública]....., con NIT: [Nro NIT]....., representada por el/la [nombres y apellidos].....[cargo]....., quien acredita y autoriza a [Nombres **USUARIO(A)** titular]..... con C.I. N° [C.I. **USUARIO(A)** titular]..... para la obtención, uso del Certificado Digital y la suscripción del presente Contrato de Adhesión, mediante [tipo nota, contrato u otro documento] de fecha [FECHA NOTA- DIA, MES Y AÑO]....., con domicilio legal en [dirección **USUARIO(A)** titular]....., que en lo sucesivo se denominará **USUARIO(A)**.

Los datos del **USUARIO(A)** que se encuentran en el sistema de registro de Certificación Digital, forman parte integrante e inseparable del presente contrato para todos los efectos legales.

SEGUNDA (ANTECEDENTES). -

- Constitución Política del Estado.
- Ley N° 1178 de 20 de julio de 1990, de Administración y Control Gubernamentales.
- Ley del Presupuesto General aprobado para la gestión.
- Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación de 8 de agosto de 2011.
- Decreto Supremo N° 1793 de 13 de noviembre de 2013, que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Decreto Supremo N° 3527 de 11 de abril de 2018, que modifica el Decreto Supremo N° 1793 de 13 de noviembre de 2013, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Resolución Administrativa Regulatoria ATT-DJ-RAR TL LP 202/2019 de 16 de abril de 2019, de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes ATT, modificada por la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 267/2025 de 04 de abril de 2025.
- Resolución Administrativa Regulatoria ATT-DJ-RA-TL LP 209/2019 de 24 de abril de 2019, de la



E-LP-1883/2026

Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes ATT.

- i) Políticas y prácticas de Certificación Digital de la Entidad Certificadora.
- j) El Contrato de Autorización para la Prestación de Servicios de Certificación Digital vigente.
- k) Decreto Supremo N° 2451 de 09 de septiembre de 2015, creación de la AGETIC, modificado por Decreto Supremo N° 3900 de 15 de mayo de 2019.
- l) Decreto Supremo N° 5519 de 13 de enero de 2026, cierre de ADSIB y asumir funciones de la AGETIC.
- m) Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 61/2026 de 14 de enero de 2026, permite a la AGETIC excepcionalmente ejercer, administrar y prestar el servicio de certificación digital otorgado a la ex ADSIB.

TERCERA (OBJETO DEL CONTRATO). -

El presente contrato tiene por objeto la prestación del Servicio de Certificación Digital y de servicios relacionados, en sujeción estricta y absoluta a las cláusulas del presente Contrato, los Términos y Condiciones y las Políticas y prácticas de certificación digital que forman parte indivisible del mismo.

CUARTA (TÉRMINOS Y CONDICIONES). -

Se establece que el servicio contratado se somete a los Términos y Condiciones, referidos a la descripción, provisión del servicio de certificado digital, alcance, características y otros aspectos importantes de su funcionamiento; que forman parte indivisible e inseparable del presente Contrato.

QUINTA (PLAZO, VIGENCIA Y RENOVACIÓN DEL CONTRATO). -

El presente contrato tendrá una vigencia de 1 año computable a partir de la emisión del certificado digital.

5.1.- El plazo de vigencia del certificado digital, es desde XX/XX/XXX hasta XX/XX/XXX. El contrato estará vigente mientras el Certificado Digital emitido por la EC sea válido.

5.2.- Como se establece en la cláusula octava, por tratarse el presente contrato de adhesión de un documento digital, el **USUARIO(A)**, debe firmar el mismo digitalmente, conforme se establece en la Cláusula Octava del presente Contrato.

5.3.- En caso de revocación y posterior solicitud de reemisión del Certificado Digital del **USUARIO(A)**, por las causales establecidas en el Decreto Supremo N° 1793 se deberá suscribir un nuevo contrato por el plazo que resulte de la diferencia del plazo del certificado digital primigenio y el plazo restante de validez del Certificado Digital emitido. 5.4.- En caso de renovación, se deberá suscribir un nuevo contrato, que debe ser firmado digitalmente por el **USUARIO(A)** con el Certificado Digital emitido y vigente al amparo del presente contrato, mismo que entrará en vigencia a la extinción del certificado digital primigenio.

SEXTA (PLAZOS PARA LA PRESTACIÓN DEL SERVICIO). -

La EC emitirá el Certificado Digital hasta 72 horas a partir del cumplimiento de los requisitos y el pago efectuado cuando corresponda.

SÉPTIMA (TITULARIDAD). -

Se denomina **USUARIO(A)** al titular del Certificado Digital y es quien se adhiere al fiel cumplimiento del presente Contrato y lo establecido en las Políticas de Certificación y los Términos y Condiciones.

OCTAVA (EFICACIA CONTRACTUAL). -

Conforme lo establecen las Políticas de Certificación y los Términos y Condiciones el **USUARIO(A)** está obligado a firmar digitalmente el presente contrato bajo las siguientes condiciones:

- a) Que la firma sea realizada en un plazo perentorio de **120 Horas** a partir de la Emisión Reemisión y/o Renovación del Certificado Digital, para lo cual la EC notificará al **USUARIO(A)** en el correo electrónico provisto por el mismo, pudiendo la EC utilizar además otros medios de notificación.
- b) Que la firma del presente contrato por parte del **USUARIO(A)**, sea realizada como primer acto de uso de su Certificado Digital, caso contrario el **USUARIO(A)**, responderá unilateralmente por los daños que pudiese ocasionar a la EC y/o a terceros.



Ante el incumplimiento del **USUARIO(A)**, de las condiciones descritas en la presente cláusula, la **EC** revocará el Certificado Digital emitido a favor del **USUARIO(A)**, quedando resuelto de pleno derecho el presente contrato.

NOVENA (ESTRUCTURA TARIFARIA). -

El **USUARIO(A)** acepta la estructura tarifaria vigente y registrada ante la ATT, la misma se encuentra publicada en el sitio web: www.firmadigital.bo o www.agetec.gob.bo

DÉCIMA (PAGO Y FACTURACIÓN). -

El pago correspondiente al certificado se realizará de acuerdo a procedimientos y formas habilitadas por la **EC**, los que serán publicados en el sitio web de la **EC** (www.firmadigital.bo).

La emisión de la factura se realizará por medio digital, al correo electrónico del **USUARIO(A)**, a nombre y número de identificación tributaria definidos en el sistema de solicitudes, una vez realizado el pago; excepcionalmente y cuando así se requiera se emitirán facturas manuales.

En caso de cuentas corporativas la factura será emitida según disposiciones normativas vigentes.

DÉCIMA PRIMERA (DERECHOS Y/O OBLIGACIONES DEL USUARIO(A) Y DE LA EC). - Los derechos y obligaciones del **USUARIO(A)** y de la **EC**, se encuentran descritos en las Políticas de Certificación y los Términos y Condiciones.

DÉCIMA SEGUNDA (EXENCIONES DE RESPONSABILIDAD). -

La **EC** no se hará responsable, ni responderá por daño alguno, en caso de la suspensión del servicio por cualquier causa que no esté bajo control directo de la **EC**, como eventos de fuerza mayor o caso fortuito, conmoción civil, cortes de energía prolongados, desastres naturales, interrupción en el servicio de Internet por parte del proveedor del servicio de internet, orden de suspensión emanada por autoridad competente u otros.

La **EC** tampoco se hace responsable por fallas o pérdidas de datos resultado de ataques informáticos u otros, que logren sobrepasar las medidas de seguridad y procedimientos establecidos y aprobados por la Entidad Certificadora Raíz.

La **EC** se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de posibles reclamaciones; deslindando todo tipo de responsabilidad civil y/o penal.

DÉCIMA TERCERA (ATENCIÓN DE RECLAMOS). -

Las Políticas de Certificación establecen en la parte final del subnumeral 1.4.2., que la AGETIC no opera como mediadora, ni entidad sancionadora en ningún caso; únicamente será la entidad encargada de facilitar información y ofrecer servicios que permitan validar los certificados y la integridad de los documentos firmados digitalmente. Los procedimientos de atención de reclamos, plazos y demás actuaciones administrativas para garantizar los derechos de los **USUARIO(A)s**, se regirán por el Reglamento a la Ley N° 2341 de 23 de abril de 2002, aprobado mediante Decreto Supremo N° 27172 de 15 de septiembre de 2003, así como por lo establecido en el numeral 9.9 Resolución de Conflictos, de las Políticas de Certificación para Persona Natural y Jurídica, respectivamente. Por otra parte, ante cualquier modificación futura a la normativa vigente del sector, la **EC** deberá proceder a la adecuación del Contrato de Adhesión y Términos y Condiciones, para la correspondiente aprobación por la Autoridad respectiva.

DÉCIMA CUARTA (SERVICIOS DE INFORMACIÓN Y ASISTENCIA). -

La **EC** atenderá las consultas y brindará información referente al servicio que presta en la cuenta de correo electrónico, números de teléfono y sistema de consultas establecidos en el sitio web www.firmadigital.bo o www.agetec.gob.bo, así como de forma presencial en sus oficinas, o en cualquiera de las Agencias de Registro autorizadas.



DÉCIMA QUINTA (DECLARACIÓN EXPRESA). -

El **USUARIO(A)** declara su plena aceptación y conformidad con todas las cláusulas del presente contrato, sin que medie vicio del consentimiento alguno; igualmente declara conocer las Políticas de Certificación y aceptar los Términos y Condiciones.

Por otro lado, el **USUARIO(A)** acepta y autoriza expresamente a la **EC** a proceder a la publicación de la solicitud de firma del Certificado Digital y/o el Certificado Digital, como toda información incluida en ellos, a petición expresa por autoridad competente en el marco de lo establecido en la Constitución Política del Estado, la normativa vigente y aquella referida a la privacidad de los **USUARIO(A)**, así como a la Cláusula Décima Sexta del presente Contrato.

DÉCIMA SEXTA (PROTECCIÓN DE LOS DATOS DEL USUARIO(A)). -

La **EC** adopta e implementa medidas y procedimientos efectivos para proteger los datos del **USUARIO(A)**, en virtud lo dispuesto sobre Protección de Datos e Información de Certificados Digitales, en las Políticas de Certificación, y de conformidad con lo dispuesto en la normativa vigente, y el presente Contrato.

Asimismo, bajo el Principio de Confidencialidad establecido en las mencionadas Políticas de Certificación, los dependientes de la **EC** que intervengan en el tratamiento de datos personales, están obligados a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo laboral.

DÉCIMA SÉPTIMA (DE INFRACCIONES Y SANCIONES). -

El régimen de infracciones y sanciones contra los Derechos del **USUARIO(A)** se encuentran regulados por los Artículos 37 y 38 del Capítulo II (Contra los Derechos de las Usuarías o Usuarios del Servicio de Certificación Digital) del Título III (Régimen de Infracciones y Sanciones del Servicio de Certificación Digital) del Anexo aprobado por el Decreto Supremo N.º 4326 de 7 de septiembre de 2020 que aprueba el Reglamento de Infracciones y Sanciones para el Sector de Telecomunicaciones, Tecnologías de Información y Comunicación.

DÉCIMA OCTAVA (RESOLUCIÓN DEL CONTRATO). -

Se resolverá el presente contrato por una de las siguientes causas:

- **Por Cumplimiento del Contrato:** De forma normal, tanto la **EC** como el **USUARIO(A)** darán por terminado el presente Contrato, una vez que ambas partes hayan dado cumplimiento a todas las condiciones y estipulaciones contenidas en el mismo.
- **Por Incumplimiento de Contrato:** Si se diera el caso y como una forma excepcional de terminar el Contrato, a los efectos legales correspondientes, la **EC** y el **USUARIO(A)** acuerdan que procederán a la resolución del Contrato por incumplimiento a lo estipulado en el Contrato, las Políticas de Certificación y los Términos y Condiciones, así como a cualquiera de sus documentos integrantes.

Asimismo, se establece que el **USUARIO(A)** acepta que toda la información que proporciona es cierta. En caso de verificarse la falsedad y/o alteración de la documentación y/o información, sea por denuncia o de oficio, la **EC** podrá iniciar las acciones que considere pertinentes, caso en el cual la **EC** podrá revocar de manera inmediata el certificado digital emitido como la cuenta generada y en consecuencia se resolverá el presente Contrato.

• **Por causas de fuerza mayor o caso fortuito que afecten a la EC o al USUARIO(A).** - Si en cualquier momento antes de la terminación de la provisión del servicio, objeto del presente Contrato, la **EC** o el **USUARIO(A)** se encontrase con situaciones fuera de control, por causas de fuerza mayor o caso fortuito que imposibiliten la conclusión de la provisión del servicio o vayan contra los intereses del Estado, la parte afectada, comunicará por escrito su intención de resolver el Contrato, justificando la causa.

La **EC**, comunicará al **USUARIO(A)** que la resolución del Contrato se ha hecho efectiva y cesará la



E-LP-1883/2026

provisión del servicio. La resolución por cualquiera de las causales establecidas en la presente Cláusula no generará obligaciones futuras a favor ni en contra de la EC y el **USUARIO(A)**.

DÉCIMA NOVENA (CLÁUSULA DE INTERPRETACIÓN). -

Se establece que en caso de duda sobre la interpretación del presente Contrato, se aplicará lo más favorable al **USUARIO(A)**, siendo parte del contrato las Políticas de Certificación y los Términos y Condiciones y todo otro documento vinculante al servicio.

VIGÉSIMA (DOMICILIO DE LAS PARTES). -

A los efectos de cualquier aviso o notificación que las partes deban realizar en virtud del presente, las direcciones de las partes son las siguientes:

• **EC: AGETIC**

◦ Dirección: Sopocachi Calle Pedro Salazar N° 631, Esquina Andrés Muñoz Edificio del Fondo Nacional de Desarrollo Regional (FNDR) Pisos 3, 4 y 5, La Paz - Bolivia

◦ Teléfono: (+591 2) 2184026

◦ Correo Electrónico: soporte@firmadigital.bo

• **USUARIO(A): XXXXXX**

◦ Dirección: XXXXX

◦ Teléfono: XXXXX

◦ Correo Electrónico: XXXXX

Cualquier cambio de dirección deberá ser notificado a la otra parte para que surta efectos legales; de lo contrario tendrán validez los avisos efectuados a las direcciones antes indicadas.

VIGÉSIMA PRIMERA (ACEPTACIÓN). -

La EC y el **USUARIO(A)** expresan su libre, plena y absoluta conformidad con todas las cláusulas del presente contrato de adhesión y los documentos que lo conforman, asimismo, se comprometen a su fiel y estricto cumplimiento.

La Paz, XX/XX/XXXX





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026

ANEXO B
TÉRMINOS Y CONDICIONES
PROVISIÓN DEL SERVICIO DE CERTIFICACIÓN DIGITAL

Introducción

El Artículo 83. (CERTIFICADOS DIGITALES PARA EL SECTOR PÚBLICO) de la Ley N°164, establece: La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB, en el marco del Decreto Supremo N.º 5519, mediante el cual se establece la transferencia de funciones, activos y responsabilidades de la ADSIB a la Agencia de Gobierno Electrónico y Tecnologías de Información – AGETIC, prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la presente Ley, y velará por la autenticidad, integridad y no repudio entre las partes.

En fecha 05 de marzo de 2021 la ADSIB, ahora AGETIC firma el contrato ATT-DJ-CON SCD 1/21 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 para el Desarrollo de la Sociedad de la Información en Bolivia.

Los Términos y Condiciones para la Provisión de la Certificación Digital contemplan la descripción del servicio que presta la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (AGETIC) como Entidad Certificadora Pública.

Descripción del servicio y aspectos asociados

Un certificado digital emitido por la Entidad Certificadora Pública AGETIC le permite al signatario realizar firmas digitales y autenticar su identidad con la validez legal, vincula un documento digital o mensaje electrónico de datos y garantiza la integridad del documento digital o mensaje electrónico con firma digital.

El servicio de certificación Digital responde a formatos y procedimientos de calidad y estándares reconocidos internacionalmente y fijados por la ATT, conteniendo la información necesaria para la identificación, vigencia y verificación de la firma digital.

A nivel conceptual, la Firma Digital consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos digitales. La clave privada siempre se encuentra en custodia del firmante y es la utilizada para realizar firmas. La clave pública es la que se divulga y es utilizada por los terceros aceptantes para verificar la validez de una firma digital.

Alcance o cobertura de la prestación del servicio

El alcance de la prestación del servicio de certificación digital contempla:

- Emitir, reemitir, validar, renovar, denegar, suspender o revocar 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 del solicitante;
- Reconocer y validar los certificados digitales emitidos en el exterior;
- Otras funciones relacionadas con la prestación de servicios de certificación digital.

La Entidad Certificadora Pública AGETIC emite certificados digitales a:

- Personas naturales
- Personas jurídicas

La Ley N° 164, Ley General de Telecomunicaciones, establece la validez jurídica y probatoria de:



E-LP-1883/2026



@ATTBolivia

| www.att.gob.bo

ATT. Te cuida, Te protege.

12 de 28

1. El acto o negocio jurídico realizado por persona natural o jurídica en documento digital y aprobado por las partes a través de firma digital, celebrado por medio electrónico u otro de mayor avance tecnológico.
2. El mensaje electrónico de datos.
3. La firma digital.

La misma ley realiza excepciones en los siguientes actos y hechos jurídicos de su celebración por medios electrónicos:

- Los actos propios del 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 expreso de partes.

Modalidades de prestación del servicio

La Entidad Certificadora Pública AGETIC ofertará el siguiente servicio:

- Contratación por la emisión del Certificado Digital.

La Entidad Certificadora Pública AGETIC emite dos tipos de certificados digitales conforme a lo establecido por el ente regulador ATT:

- a) Persona jurídica: Certificado expedido únicamente a personas bajo relación jurídica con una persona jurídica, a solicitud expresa del representante legal de dicha persona.
- b) Persona natural: Certificado expedido a cualquier ciudadana o ciudadano mayor de edad y hábil por derecho para realizar actos jurídicamente válidos.

Independientemente del tipo de certificado, se pueden emitir certificados por el tipo de uso:

- a) Firma Digital Simple
- b) Firma Digital Automática

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

- a) Nivel de seguridad alto: El par de claves se genera en un dispositivo criptográfico por hardware.
- b) Nivel de seguridad normal: El par de claves se genera en un dispositivo criptográfico por software.

Por cada certificado emitido, se cobra una tarifa aprobada por el ente regulador y es determinada de acuerdo al tipo de certificado digital emitido, los certificados emitidos por la Entidad Certificadora Pública AGETIC tienen una vigencia máxima de un (1) año (365 días calendario) con un máximo de cuatro reemisiones de certificado digital, que incluye:

- a) Emisión del certificado digital correspondiente, incluyendo la información establecida en la reglamentación técnica de la ATT (*).
- b) Derecho a mantener una cuenta de usuario en el sistema de solicitud de certificados digitales de la Entidad Certificadora Pública AGETIC, que le permitirá al usuario:
 1. Acceder a cualquiera de los certificados emitidos a su nombre y la información correspondiente a su validez, estado y vigencia.



E-LP-1883/2026

2. Solicitar la revocatoria de un certificado
 3. Solicitar la renovación de un certificado sin cambio de clave privada. (**)
 4. Reportar incidentes con respecto a sus certificados
 5. Acceder al servicio de soporte técnico en línea, en los horarios establecidos por la Entidad Certificadora Pública AGETIC y según sus procedimientos
 6. Solicitar la reemisión de certificados por pérdida o cambio del dispositivo criptográfico (HSM, token o smartcard) o encontrarse comprometida su clave privada por un máximo de tres veces, al cabo de las cuales deberá cancelar nuevamente por el servicio de certificación digital. (**)
- c) Acceso al servicio de soporte técnico presencial en oficinas de la Entidad Certificadora Pública AGETIC, en los horarios y bajo los procedimientos establecidos por la misma.
 - d) Derecho a solicitar la renovación, revocatoria o reemisión de sus certificados en oficinas de la Entidad Certificadora Pública AGETIC, en los horarios y bajo los procedimientos establecidos por la misma. (**)
 - e) Derecho a que cualquier persona pueda establecer el estado actual de sus certificados (válido, revocado) a través de los servicios de Listas de Revocatoria de Certificados (CRL) o servicio OCSP, conforme a lo dispuesto por la Entidad Certificadora Pública AGETIC.
 - f) Derecho a participar de las promociones o beneficios adicionales que pueda establecer la Entidad Certificadora Pública AGETIC.

Donde:

(*) La emisión del certificado no incluye el dispositivo criptográfico (token o HSM) para la preservación de las claves pública y privada y certificado del usuario.

(**) La renovación, revocación y/o reemisión de certificados se realizarán conforme a los procedimientos establecidos por la Entidad Certificadora Pública AGETIC.

El usuario es responsable de la generación del par de claves en dispositivos criptográficos seguros. En caso de usarse dispositivos criptográficos basados en hardware, los mismos deben estar homologados por la ATT, que dispone de la lista de todos los dispositivos homologados en su sitio web.

Definiciones

Definiciones aplicadas para el presente el documento:

- **Certificado digital:** Es un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.
- **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.
- **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.
- **Firma digital:** Es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital.
- **Firma Digital Automática:** Firma digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en éste.



E-LP-1883/2026

- **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.
- **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.
- **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 esta 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.
- **Módulo criptográfico basado en token:** 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.
- **Usuario titular:** El usuario titular para el servicio de certificación digital de la AGETIC es la persona física poseedora 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:** Las cuentas corporativas son las entidades que establecen un vínculo contractual o de convenio con la Entidad Certificadora Pública AGETIC para adquirir certificados digitales para su personal interno.
- **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.
- **Emisión de Certificados:** La Entidad Certificadora Pública AGETIC emitirá los certificados que se le soliciten a través de una Agencia de Registro autorizada, una vez que se hayan aprobado dichas solicitudes mediante la comprobación del cumplimiento de los correspondientes requisitos.

Requisitos técnicos necesarios para acceder al servicio

Para que un usuario pueda acceder al servicio de certificación digital deberá contar con las especificaciones técnicas detalladas a continuación:

- Contar con acceso a Internet.
- Darse de alta como usuario en el sistema de Agencia de Registro.
- En función al nivel de seguridad, 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 (<https://www.att.gob.bo/homologados>). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud.



- Para Certificados Digitales con Seguridad Normal: Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos. La Entidad Certificadora Pública AGETIC provee una herramienta homologada por la ATT para la generación del par de claves por software, misma que puede ser encontrada en: <https://firmadigital.bo/>
- El usuario deberá generar 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. Para

La Entidad Certificadora Pública AGETIC, las Agencias de Registro y los Oficiales de Registro autorizados harán todos los esfuerzos por brindar un servicio de calidad a los usuarios, tanto en los aspectos técnicos como humanos, enmarcada en una política de satisfacción de sus suscriptores. En ese contexto, la Entidad Certificadora Pública AGETIC no se hará responsable de la suspensión del servicio por cualquier causa que no esté bajo control directo de la entidad, como eventos de fuerza mayor o caso fortuito, cortes de energía prolongados, desastres naturales, interrupción en el servicio de internet por parte del proveedor del servicio, orden de revocatoria por autoridad competente u otros.

La Entidad Certificadora Pública AGETIC tampoco se hace responsable por fallas o pérdidas de datos fruto de ataques informáticos u otros que logren sobrepasar las medidas de seguridad y procedimientos establecidos y aprobados por la Entidad Certificadora Raíz.

Los servicios de la Entidad Certificadora Pública AGETIC en favor del usuario, en cuanto a la certificación digital, se limitan a la firma de los certificados y publicación de la Lista de Certificados Revocados (CRL), el servicio OCSP, así como brindar los mecanismos necesarios para la renovación, reemisión y revocación de los certificados firmados. De ser posible y a criterio de la Entidad Certificadora Pública AGETIC, la misma ofrecerá soporte técnico a los usuarios, en el marco de lo que considere pertinente y bajo los alcances que establezca. La atención de reclamos se realizará conforme a la normativa vigente y el procedimiento establecido.

Habilitación y plazo para la provisión del servicio

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

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 la toma de Fotografía para la verificación visual con el documento de identidad. 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.



E-LP-1883/2026



AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026

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 una vez verificada la solicitud, 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.

La Entidad Certificadora Pública AGETIC será responsable de atender todo CSR remitido por la Agencia de Registro debidamente firmado por el Oficial de Registro que atendió la solicitud y emitir el certificado digital solicitado, para ello dispone de procedimientos internos que incluyen una Ceremonia de Emisión de los Certificados Digitales que garantizan la seguridad e integridad de los datos.

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.

Tarifas

La Entidad Certificadora Pública AGETIC, tiene su estructura tarifaria aprobada por la ATT del servicio de certificación digital y esta publicada en el sitio Web: <https://firmadigital.bo/>

Obtención, revocación, vigencia y conservación del certificado digital

De conformidad a lo señalado en el Artículos 28, 29, 30 y 31 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, se establecen los siguientes requisitos:

Obtención del certificado digital

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 los documentos de Políticas de Certificación de cada tipo de certificado.

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, 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
- **Nivel de seguridad normal:** El par de claves se genera en un dispositivo criptográfico por software.



E-LP-1883/2026

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

Para la obtención del Certificado Digital el SIGNATARIO (A) o USUARIO (A) deberá acreditar su identidad, siendo la solicitud personal, la misma podrá ser realizada de forma presencial o por otros medios establecidos, siempre que se garantice la identidad del usuario; debiendo cumplir con los siguientes requisitos.

Requisitos para personas naturales

Los requisitos para personas naturales son:

- a) Documento de Identidad vigente (Carnet de identidad o extranjero, según corresponda).
- b) Última factura de un servicio básico (Luz o agua) que permita verificar su dirección actual.
- c) Registro y solicitud de un certificado digital de tipo persona natural en el sistema de la Agencia de registro.
- d) En función al nivel de seguridad del certificado a solicitar 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 (<https://www.att.gob.bo/homologados>). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud.
 - Para Certificados Digitales con Seguridad Normal: Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos.

Requisitos para personas jurídicas

Los requisitos para personas jurídicas son:

- a) Documento de Identidad vigente (carnet de identidad o de Extranjero, según corresponda).
- b) Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributaria) del solicitante vigente.
- c) Nota de Autorización original para el solicitante por la Máxima Autoridad Ejecutiva o el Representante Legal de la Empresa.
- d) Registro y solicitud de un certificado digital de tipo persona jurídica en el sistema de la Agencia de registro.
- e) En función al nivel de seguridad del certificado a solicitar, deberá contar con:
 1. Para Certificados Digitales con Seguridad alta: Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2 nivel 2 mínimamente. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web (<https://www.att.gob.bo/homologados>). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud.
 2. 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.

Renovación de un certificado digital

Para ese procedimiento el usuario titular deberá acceder al Sistema de la Agencia de Registro con las credenciales de usuario que obtuvo al momento de crear la cuenta y decidir si desea generar un nuevo par de claves o conservar el par de claves para la renovación del Certificado, finalmente deberá coordinar la vídeo llamada de verificación fotográfica y carnet de identidad. Se puede realizar la solicitud de renovación hasta en



B-LP-1883/2026

tres (3) oportunidades, siempre y cuando el certificado este vigente. Si se ha excedido el periodo de vigencia del certificado, se debe realizar una solicitud de un nuevo certificado. La cuarta renovación consecutiva también será tratada como una solicitud nueva, necesitando cumplir todos los procedimientos establecidos por la Entidad Certificadora Pública AGETIC.

Reemisión de un certificado digital

La solicitud de reemisión de certificado digital debe aplicarse a un certificado revocado, y podrá generarse un nuevo par de claves para el nuevo certificado digital.

Al enviar el archivo CSR de reemisión a la Entidad Certificadora Pública, el Sistema de Agencia de Registro especificará el periodo de validez correspondiente en base al tiempo restante del certificado digital inicial.

Cuando un usuario con Certificado Digital con Token solicite una reemisión, puede solicitar también la reposición del token. Para ello debe apersonarse a una Agencia de registro para la entrega del dispositivo, previa cancelación del costo de reposición del dispositivo y proceder según lo establecido para una reemisión de certificado digital.

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

En caso que se solicite una reemisión sin cambio de titular también será necesario firmar un nuevo contrato de adhesión.

Revocación de un certificado digital

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

- a) A solicitud del titular debido a robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- b) Emisión defectuosa de un certificado debido a que:
 1. No se ha cumplido un requisito material para la emisión del certificado.
 2. Un dato fundamental relativo al certificado es falso.
 3. Identificación de un error de entrada de datos u otro error de proceso.
- c) No se firme el contrato de adhesión al servicio en el plazo establecido posterior a su emisión.
- d) La información contenida en el certificado o utilizada para realizar la solicitud cambió.
- e) El certificado de la Entidad Certificadora Pública AGETIC o Entidad Certificadora Raíz ATT es revocado.
- f) Otros fundamentos técnicos y/o legales, de interés nacional, por resguardo de la seguridad del Estado Plurinacional de Bolivia o de interés del pueblo boliviano, mediante Resolución Administrativa de su Máxima Autoridad Ejecutiva.

II. La revocación del certificado digital no exime a su titular del cumplimiento de las obligaciones contraídas durante la vigencia del certificado.

Vigencia de los certificados

La vigencia de los certificados digitales emitidos no será superior a un (1) año.

Conservación del certificado digital

La conservación del certificado digital es de entera responsabilidad del usuario titular, y debe ser almacenado adecuadamente en el dispositivo criptográfico para el que fue emitido según la generación de su par de claves (hardware o software).



Derechos y obligaciones del titular del certificado digital

Documentos de referencia

- Ley N°164, artículo 54 y artículo 55
- Decreto Supremo N°1793, artículo 52, 53, 54 y artículo 55

Titular del certificado digital

De acuerdo a 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 naturales y las personas jurídicas que a través de sus representantes legales hayan solicitado por sí y para sí una certificación que acredite su firma digital.

Responsabilidad del titular

De acuerdo a 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:

- Por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como titular.
- Los datos de creación de la firma digital vinculado a cada certificado digital de una persona jurídica, será responsabilidad del titular del certificado, cuya identificación se incluirá en el certificado digital.
- El documento con firma digital le otorga al titular del certificado la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
- Asimismo, acorde a los procedimientos de la 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 AGETIC o a alguna Agencia de Registro autorizada a la brevedad posible y solicitar su revocatoria. 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.

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 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;
- A la confidencialidad de la información proporcionada a la entidad certificadora;
- A recibir información de las características generales del servicio, con carácter previo al inicio de la prestación del mismo;
- 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;
- 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.

De conformidad a lo señalado en el Artículo 54 de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, el titular del certificado digital tiene 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) Elegir y cambiar libremente de operador o proveedor de los servicios y de los planes de acceso a los mismos, salvo las condiciones pactadas libremente en el contrato, las cuales deben ser explícitas, claras y previamente informadas a las usuarias y los usuarios.
- c) 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 los operadores o proveedores de los servicios.
- d) Acceder gratuitamente a 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
- e) 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.
- f) Exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.
- g) Conocer los indicadores de calidad de prestación de los servicios al público de los proveedores de telecomunicaciones y tecnologías de información y comunicación.
- h) Acceder gratuitamente a las guías telefónicas a nivel nacional y a un servicio nacional gratuito de información de voz, sobre sus contenidos.
- i) Solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas. Las usuarias o usuarios podrán decidir cuáles datos personales se incluyen, así como comprobarlos,
- j) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- k) Ser informado por el proveedor oportunamente, cuando se produzca un cambio de los precios, las tarifas o los planes contratados previamente.
- l) Recibir el reintegro o devolución de montos que resulten a su favor por errores de facturación, deficiencias o corte del servicio.
- m) Ser informado sobre los plazos de vigencia de las ofertas y promociones de los servicios.
- n) Obtener respuesta efectiva a las solicitudes realizadas al proveedor.
- o) Ser informado oportunamente de la desconexión o corte programado de los servicios.
- p) Reclamar ante los proveedores de servicios y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna.
- q) Recibir protección del proveedor del servicio sobre los datos personales contra la publicidad no autorizada por la usuaria o usuario, en el marco de la Constitución Política del Estado y la presente Ley.
- r) 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 reglamento.
- s) Exigir la protección de la niñez, adolescencia y juventud en la prestación de los servicios.
- t) Recibir servicios que no causen daños a la salud y al medio ambiente, conforme a normas establecidas.
- u) Participar en los mecanismos de control social.
- v) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales,





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026

las leyes y demás normas aplicables.

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:

- I. 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 revocación del certificado.
- II. 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.

De conformidad a lo señalado en el 55 de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, el titular del certificado digital tiene 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 los operadores y proveedores.
- 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.

Derechos y obligaciones de la ECA o Agencia de Registro

Documentos de referencia

- Ley N°164, artículo 59
- Decreto Supremo N°1793, artículo 43, artículo 45, artículo 46 y artículo 56



E-LP-1883/2026

Derechos de la entidad certificadora publica

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.

Obligaciones de la entidad certificadora publica

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 de acuerdo a 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) Cumplir las instrucciones y planes que se emitan en casos de emergencia y seguridad del Estado.
- n) Actualizar periódicamente su plataforma tecnológica y los procesos de atención a las usuarias y los usuarios.
- o) 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 de la firma y certificado digital, la Entidad Certificadora Pública tiene las siguientes obligaciones de acuerdo a lo establecido en el Artículo 43 del Decreto Supremo N°1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026



- 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 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.
- q) En caso de emitir certificados por software, proveer al menos una solución de software libre para la generación del par de claves por software, homologada por la ATT y publicada en el repositorio estatal de software libre.

Garantía

Para garantizar la garantía de la firma y certificado digital, la Entidad Certificadora Pública tiene las siguientes obligaciones de acuerdo a lo establecido en el Artículo 45 del Decreto Supremo N°1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:

- a) Las entidades certificadoras deberán obtener y mantener vigente una boleta de garantía de cumplimiento de contrato, por el siete por ciento (7%) de sus ingresos brutos de la gestión inmediata anterior, o sobre sus proyecciones para el primer año, que respalde su actividad durante la vigencia de la autorización para prestación de servicios de certificación digital.
- b) El incumplimiento de este requisito dará lugar a las acciones correspondientes en el marco de las competencias de la ATT.





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026



Auditorías

Las auditorías de la firma y certificado digital, la Entidad Certificadora Pública de acuerdo a lo establecido en el Artículo 46 del Decreto Supremo N°1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:

- a) Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.
- b) La ATT, podrá implementar el sistema de auditoría, que debe como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, el cumplimiento de los estándares nacionales e internacionales sobre certificación y firma digital, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento de las políticas de certificación definidas por la autoridad, su declaración de prácticas de certificación y los planes de seguridad y de contingencia aprobados.

Protección de datos personales

A fin de garantizar los datos personales y la seguridad informática de los mismos, de acuerdo a lo establecido en el Artículo 56 del Decreto Supremo N°1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, 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, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;
- c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;
- d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;
- e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

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:

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

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, 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 signatarios o 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 signatario o terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

Atención de consultas, reclamaciones y emergencias y/o servicios de información y asistencia

Atención de consultas y emergencias y/o servicios de información

La Entidad Certificadora Pública – AGETIC atenderá las consultas referentes a los servicios que presta en la cuenta de correo electrónico sopORTE@firmadigital.bo, al número de teléfono (591-2) 2184026, WhatsApp (591) 71555590 y sistema de consultas establecidos en el sitio web <https://firmadigital.bo/>. Las consultas serán atendidas de lunes a viernes, de 08:30 a 16:30 (Horario continuo, GMT -4), o en los horarios de trabajo establecidos por las autoridades competentes en el territorio del Estado Plurinacional de Bolivia para la administración pública.

Procedimiento de reclamaciones

El procedimiento de Reclamaciones se registrará de conformidad a lo establecido en el Decreto Supremo 27172 Reglamento de la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial (vigente a la fecha).

Reclamación directa

El usuario tiene el derecho de recibir por parte de la Entidad Certificadora Pública AGETIC, a través de su Oficina de Atención al Consumidor – ODECO, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación del servicio. Así mismo puede solicitar la devolución de los importes indebidamente pagados.

Asimismo, el usuario o un tercero por él, previa identificación, presentará su reclamación, en una primera instancia ante la Entidad Certificadora Pública.

Por otro lado, la reclamación será presentada en forma escrita o verbal, gratuita, por cualquier medio de comunicación, dentro de los veinte (20) días del conocimiento del hecho, acto u omisión que la motiva.

El plazo que la Entidad Certificadora Pública tiene para resolver la reclamación se registrará de acuerdo a lo establecido en el Artículo 57 del Decreto Supremo N° 27172:

- a) A los tres (3) días de su recepción, en casos de interrupción del servicio o de alteraciones graves derivadas de su prestación; o
- b) A los quince (15) días en los demás casos.



La Entidad Certificadora Pública se pronunciará por la procedencia o improcedencia de la reclamación, dejando constancia escrita de su decisión. Si decide la procedencia de la reclamación adoptará todas las medidas necesarias para devolver los importes indebidamente cobrados, reparar o reponer cuando corresponda, y en general, asumirá toda medida destinada a evitar perjuicios a los usuarios. La decisión deberá cumplirse en un plazo máximo de veinte (20) días.

La Entidad Certificadora Pública comunicará al reclamante/usuario la resolución que decide la reclamación dentro de los cinco (5) días siguientes a su pronunciamiento, informando al reclamante, en caso de ser improcedente su reclamación, sobre su derecho a presentarla en la correspondiente instancia.

Por otro lado, se establece que la carga de la prueba será de la Entidad Certificadora Pública.

Reclamación administrativa

Por otro lado, en cuanto al procedimiento de la Reclamación Administrativa se establece que, si la Entidad Certificadora Pública declara improcedente la reclamación o no la resuelve dentro del plazo establecido al efecto, el usuario o un tercero por él, podrán presentarlo a la Autoridad competente en el plazo de quince (15) días.

El usuario presentará su reclamación de manera escrita o verbal, por cualquier medio de comunicación, acreditando que con anterioridad realizó la reclamación directa en la entidad o, en su defecto, expresando las razones por las que realiza su reclamación en esta instancia.

Asimismo, en esta etapa el usuario podrá acompañar las pruebas documentales de que intentare valerse y ofrecer las restantes; y la ATT registrará su Reclamación Administrativa.

Medidas para salvaguardar la inviolabilidad de las telecomunicaciones y protección de la información

De conformidad a lo señalado en el Artículo 56 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación y en el marco de lo establecido en la Constitución Política del Estado, la Entidad Certificadora Pública garantizará la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.

Cambio o modificaciones en la ley o reglamentos de telecomunicaciones

Los presentes Términos y Condiciones se encuentran enmarcados en la Ley General de Telecomunicaciones y sus Reglamentos vigentes. Cualquier modificación futura a estas disposiciones legales será de aplicación inmediata en lo concerniente a los Términos y Condiciones.

Versiones

Versión	Fecha de Revisión	Descripción del cambio	Revisado por	Aprobado por	RES. ADM.	Fecha de aprobación
1.0	12/01/2015	Elaboración del documento considerando la elaboración de Políticas separadas por tipo de certificado	Sylvain Lesage	Nicolas Laguna	RA ADSIB No. 04/2015	12/01/2015
2.0	8/11/2018	Elaboración del documento. Se considera versión 2 debido a que los cambios anteriores realizados fueron cambios menores	Reynaldo Alonzo Vera Arias	María Jannett Ibañez Flores	ADSIB/RA/ 0074/2018	31/12/2018



Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 249/2026

2.1	24/06/2019	Ajustes al documento en base a la nueva reglamentación según Resolución ATT-DJ-RA TL LP 209/2019 emitida por la ATT	Reynaldo Alonzo Vera Arias	José Luis Machicado	ADSIB/RA/0026/2019	24/06/2019
2.2	11/2020	Ajustes al documento en el marco de reglamentación aprobada mediante Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 209/2019, y las recomendaciones realizadas por la ATT	Miguel Choque	Bladimir Magne Molina	ADSIB/RA/0027/2020	08/12/2020
2.3	11/2024	Actualización de documentos	Comité de Calidad, Seguridad de la Información y de Emergencia	Bladimir Magne Molina		

