



AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria **ATT-DJ-RAR-TL LP 357/2020**

La Paz, 15 de octubre de 2020

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RAR TL 209/2019 de 24 de abril de 2019 (**R.A.R. 209/2019**); el Informe Técnico ATT-DTLTIC-INF TEC LP 320/2020 de 18 de agosto de 2020 (**INFORME TÉCNICO 320/2020**); el Informe Jurídico ATT-DJ-INF-JUR LP 319/2020 de 15 de octubre de 2020 (**INFORME JURÍDICO 319/2020**); la normativa vigente y aplicable, todo lo que convino ver, se tuvo presente y;

CONSIDERANDO 1.- ÁMBITO DE COMPETENCIA

Que las competencias y atribuciones de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), se encuentran definidas por el Decreto Supremo N° 0071 de 09 de abril de 2009, concordante con lo dispuesto en la Disposición Transitoria Novena de la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación (**Ley N° 164**), quedando sometidas a ésta las personas naturales y jurídicas, privadas, comunitarias, públicas, mixtas y cooperativas, garantizando los intereses y derechos de los usuarios o consumidores, promoviendo la economía plural prevista en la Constitución Política del Estado Plurinacional de Bolivia y las leyes en forma efectiva.

CONSIDERANDO 2.- ANTECEDENTES

Que mediante **R.A.R. 209/2019** se aprobó el **ESTÁNDAR TÉCNICO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES**.

Que el **INFORME TÉCNICO 320/2020** justifica la modificación de la **R.A.R. 209/2019** para la inclusión del párrafo IV en el artículo 5; la modificación del inciso b) y la incorporación del inciso c) correspondientes al artículo 8; y la incorporación de la estructura de OID's en el Anexo 3 que forma parte integrante e indivisible de dicha Resolución, con el propósito de promover el uso de la Firma Digital en el Estado Plurinacional de Bolivia".

Que el **INFORME JURÍDICO 319/2020** prescribe que: *"de acuerdo a la norma citada, en particular al Decreto Supremo N° 3527 de 11 de abril de 2018 que modificó en parte el REGLAMENTO A LA LEY N° 164, señala lo siguiente: ARTÍCULO 25.- (TIPOS, FORMATOS Y ESTRUCTURA DE CERTIFICADOS). La ATT, establecerá mediante Resolución Administrativa los tipos, formatos y estructura de certificados digitales que podrán ser emitidos por las Entidades Certificadoras Autorizadas de acuerdo a su uso y conforme a estándares y recomendaciones internacionales aplicables que promuevan la interoperabilidad con otros sistemas.*

En este sentido y en virtud a lo antes descrito, la ATT está facultada para establecer los formatos para los certificados digitales detallados.

CONSIDERANDO 3.- MARCO NORMATIVO

Que el párrafo II del artículo 103 de la Constitución Política del Estado establece que: *"El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación."*

Que los numerales 2 y 5 del artículo 2 de la Ley N° 164, disponen como objetivos asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; y promover el uso de las tecnologías de información y



I-LP-11563

LA PAZ: Calle 13 de Calacoto
N° 8260 entre Av. Los Sauces
y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián
N° 683, Esq. España y La Paz
(El Prado)
Telf./Fax: 4-4581182 - 4-4581184
4-4581185

SANTA CRUZ: Avenida Beni;
entre 4° y 5° anillo, calle 3,
Edificio Gardenia, Condominio
Club Torre Sur, Planta Baja Of. 2,
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Méndez N° 311
esq. Alejandro del Carpio
Barrio Las Panosas
Telf.: 6644135 - 6112611

Línea Gratuita de Protección al
Usuario
800-10-6000
www.att.gob.bo

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 357/2020

comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.

Que el numeral 14 del artículo 14 de la Ley N° 164, establece como atribución de la ATT: *"Otorgar, modificar y renovar autorizaciones y disponer la caducidad o revocatoria de las mismas dentro del marco de la Ley y reglamentos correspondientes"*.

Que el artículo 71 de la 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 la Disposición Transitoria Sexta de la Ley N° 164, estipula que: *"Todos los aspectos que se requieran para la aplicación de la presente Ley, serán reglamentados por el Órgano Ejecutivo y regulados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, en un plazo máximo de ciento veinte días hábiles a partir de la promulgación de la misma."*

Que el artículo 24 del Reglamento a la Ley N° 164, para el Desarrollo de Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013 (**REGLAMENTO A LA LEY N° 164**) establece que: *"Los certificados digitales deben ser emitidos por una entidad certificadora autorizada, 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 contemplar la información necesaria para la verificación de la firma digital."*

Que el numeral 1 del artículo 37 del REGLAMENTO A LA LEY N° 164 estipula que los niveles de organización de la Infraestructura Nacional de Certificado Digital tienen los siguientes niveles: *"Primer nivel: Entidad Certificadora Raíz. La ATT 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 (...)"*

Que el inciso j) del artículo 38 del REGLAMENTO A LA LEY N° 164 dispone: *"Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones."*

Que el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013, tiene por objeto Reglamentar el acceso, uso y desarrollo de las Tecnologías de Información y Comunicación – TIC, en el marco del Título IV de la Ley N° 164.

Que el artículo 2 del Decreto Supremo N° 3527 de 11 de abril de 2018 (**D.S. N° 3527**) modificó en parte el REGLAMENTO A LA LEY N° 164, en particular en lo siguiente: *"ARTÍCULO 25.- (TIPOS, FORMATOS Y ESTRUCTURA DE CERTIFICADOS). La ATT, establecerá mediante Resolución Administrativa los tipos, formatos y estructura de certificados digitales que podrán ser emitidos por las Entidades Certificadoras Autorizadas de acuerdo a su uso y conforme a estándares y recomendaciones internacionales aplicables que promuevan la interoperabilidad con otros sistemas."*

Que la Resolución Ministerial 235/18 de 21 de agosto de 2018, emitida por el Ministerio de Obras Públicas, Servicios y Vivienda, aprueba el "Reglamento para normar el uso de la firma digital respecto a niveles de seguridad, en lo correspondiente al sector público.



I-LP-11563

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 357/2020

CONSIDERANDO 4.- ANÁLISIS TÉCNICO Y LEGAL

Que el **INFORME TÉCNICO 320/2020** concluye: “Mediante la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019 se aprobó el “**ESTÁNDAR TÉCNICO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES**”; que, entre otros, establece el formato para los certificados digitales emitidos por un dispositivo criptográfico basado en software (nivel normal de seguridad), y certificados digitales emitidos por un dispositivo criptográfico basado en hardware (nivel alto de seguridad), asimismo, mediante la misma Resolución se limitó la obtención de los Certificados Digitales exclusivamente para Personas Jurídicas, limitando así el despliegue de la Firma Digital y su utilización dentro del Estado Plurinacional de Bolivia. Las modificaciones e incorporaciones detalladas en el análisis del presente informe promoverán el despliegue de la firma digital dentro del Estado Plurinacional de Bolivia.”; por otra parte, el **INFORME JURÍDICO 319/2020** concluye y recomienda: “que las modificaciones propuestas no vulneran o contravienen norma vigente alguna, por lo que se recomienda la emisión del Acto Administrativo que modifique la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019, conforme al análisis técnico realizado.”

POR TANTO:

El Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, Abg. CARLOS ANDRÉS ALIAGA TÉLLEZ, en virtud a la designación realizada mediante Resolución Suprema No. 26802 de 10 de septiembre de 2020, en ejercicio de sus atribuciones conferidas por Ley y demás normas vigentes, a nombre del Estado Plurinacional de Bolivia;

RESUELVE:

PRIMERO. – Modificar el **ESTÁNDAR TÉCNICO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES**, aprobado mediante Resolución Administrativa Regulatoria ATT-DJ-RAR TL 209/2019 de 24 de abril de 2019 de la siguiente manera:

I. Se incluye el parágrafo IV en el Artículo 5.- (Formato de los certificados) de la siguiente manera:

IV. El formato para los certificados digitales emitidos por un dispositivo criptográfico basado en software (nivel normal de seguridad), para persona natural debe cumplir con la siguiente estructura:

Version (version)	El valor del campo es 2.
Número de Serie (serialNumber)	Número asignado por la ECA
Algoritmo de Firmas (SignatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (iuser)	CN="Entidad Certificadora" y el nombre de la ECA; O= Razón social de la ECA; C= Estándar de acuerdo a ISO 3166 (BO)



I-LP-11563

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 357/2020

Periodo de validez (validity)	Fecha de emisión del Certificado; Fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time)
Nombre del suscriptor (subject)	CN =Nombre completo de la persona natural; C = Estándar de acuerdo a ISO 3166 {BO}; dnQualifier =Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber : Número de NIT {numeral} (opcional). description = Nivel de seguridad
Clave pública del suscriptor (subjectPublicKey)	(subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

Adicionalmente, estos certificados digitales emitidos por un dispositivo criptográfico basado en software (nivel normal de seguridad), para persona natural deben cumplir con las siguientes Extensiones:

Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier)	Valor de la extensión subjectKeyIdentifier del certificado de la ECA emisora
Identificador de la clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey
Uso de Claves (KeyUsage)	digitalSignature=1, nonRepudiation =1, keyEncipherment=1, dataEncipherment=1, keyAgreement=0, keyCertSign= 0, cRLSing=0, encipherOnly=0, decipherOnly=0
Uso de Claves Extendido (Extended Key Usage)	clientAuth, emailProtection, codeSigning
Política de Certificación (certificatePolicies)	URI:(archivo en formato de texto), OID: (identificador de objeto) Identificador de Objeto= OID del certificado {alfanumérico} de acuerdo al Anexo de la presente Resolución Administrativa Regulatoria
Restricciones Básicas (basicConstraints)	CA= FALSE



I-LP-11563

Resolución Administrativa Regulatoria

Punto de distribución de las CRL (cRLDistributionPoints)	URI:(.crl)
Información de Acceso de la ECA (authorityInformationAccess)	URI:(.crt o .pem)
Nombre Alternativo del Suscriptor (subjectAlternativeName):	E=Correo electrónico del suscriptor

II. Se modifica el inciso b) del artículo 8.- (Condiciones de Uso) de la siguiente manera:
b) Certificados digitales emitidos por dispositivos basado en software

Los certificados digitales emitidos a través de dispositivos criptográficos basados en software podrán ser utilizados por Personas Naturales y Jurídicas, siempre y cuando sean administrados en condiciones técnicamente seguras y confiables que eviten su uso por terceros no autorizados.

Los formatos de certificado incluyen el atributo “description” en el campo “Nombre de Suscriptor (subject)” que permite verificar el nivel de seguridad con el cual fue generado y almacenado el par de claves y el certificado digital, de acuerdo al siguiente formato:

Para dispositivos criptográficos basados en hardware:
description = NIVEL DE SEGURIDAD ALTO

Para dispositivos criptográficos basados en software:
description = NIVEL DE SEGURIDAD NORMAL


III. Se incorpora el inciso c) al artículo 8.- (Condiciones de Uso) de la siguiente manera:
c) Límites de uso de Certificados Digitales emitidos por dispositivos basados en hardware y software

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

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



I-LP-11563

IV. Se incorpora la siguiente estructura de OID's en el Anexo 3 IDENTIFICADORES DE OBJETO:

LA PAZ: Calle 13 de Calacoto N° 8260 entre Av. Los Sauces y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-4581184
4-4581185

SANTA CRUZ: Avenida Beni; entre 4° y 5° anillo, calle 3, Edificio Gardenia, Condominio Club Torre Sur, Planta Baja Of. 2,
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Méndez N° 311 esq. Alejandro del Carpio Barrio Las Panosas
Telf.: 6644135 - 6112611

Línea Gratuita de Protección al Usuario
800-10-6000
www.att.gob.bo

Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 357/2020

2.16.68.0.0.0.1.14.1.2.0.X.2.0	"0" Certificado Nivel de Seguridad Normal (Emitido por Software)	2.16.0.0.0.1.14.1.2.0.X.2.0.1	"1" (Certificado de Persona Natural)	2.16.0.0.0.1.14.1.2.0.X.2.0.1.0	"0" Firma Digital Simple
				2.16.0.0.0.1.14.1.2.0.X.2.0.1.1	"1" Firma Digital Automática

Donde "X" es el identificador de la ECA

SEGUNDO. – DISPONER que los demás artículos del "Estándar Técnico para la Emisión de Certificados Digitales" y los anexos aprobados mediante Resolución Administrativa Regulatoria ATT-DJ-RA TL 209/2019 de 24 de abril de 2019, que no hayan sido modificados por la presente Resolución Administrativa, quedan vigentes, firmes y subsistentes.

TERCERO. - INSTRUIR a la Unidad de Tecnologías de Información y Comunicación de esta Autoridad, publicar la presente Resolución Administrativa Regulatoria en la página web de la ATT. Asimismo, conforme a lo dispuesto en el artículo 34 de la Ley N° 2341, de 23 de abril de 2002, de Procedimiento Administrativo, realizar la publicación del presente acto administrativo en un órgano de prensa de circulación nacional.

Regístrese y archívese.



Carlos Andrés Aliaga Téllez
DIRECTOR EJECUTIVO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES



Abg. Carlos Eduardo Rocabado Cornejo
DIRECTOR JURÍDICO a.i.
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES



I-LP-11563