



AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 311/2019

La Paz, 08 de julio de 2019

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RA TL 1022/2013 de 11 de diciembre de 2013 (**R.A.R. 1022/2013**); la Resolución Administrativa Regulatoria ATT-DJ-RAR TL LP 845/2018 de 13 de noviembre de 2018 (**R.A.R. 845/2018**); la Resolución Administrativa Regulatoria ATT-DJ-RAR TL LP 202/202 de 16 de abril de 2019 (**R.A.R. 202/2019**); la Resolución Administrativa Regulatoria ATT-DJ-RAR TL LP 209/202 de 24 de abril de 2019 (**R.A.R. 209/2019**); el Informe Técnico Jurídico ATT-DTLTIC-INF TJ LP 691/2019 de 27 de junio de 2019 (**INF-TJ 691/2019**); la demás normativa vigente y aplicable, todo lo que convino ver y se tuvo presente;

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 establecido 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 y las leyes en forma efectiva.

CONSIDERANDO 2.- ANTECEDENTES

Que mediante **R.A.R. 1022/2013** esta Autoridad aprobó el Instructivo para la Homologación de Equipos de Telecomunicaciones de Entidades Certificadoras y Registro de Fabricantes, Distribuidores, Comercializadores, Operadores y Proveedores de Servicios de Telecomunicaciones, conforme al Anexo adjunto a dicha Resolución.

Que por **R.A.R. 845/2018** se aprobaron los Documentos Públicos de la Entidad Certificadora Raíz y establece las Políticas de Certificación generales de la Infraestructura de Clave Pública del Estado Plurinacional de Bolivia.

Que mediante **R.A.R. 202/2019** se establecieron los requisitos legales, económicos y técnicos para la Entidad Certificadora Pública y las Entidades Certificadoras Privadas que quieran brindar servicios de Certificación Digital en el país.

Que mediante **R.A.R. 209/2019** se aprobó el Estándar Técnico para la Emisión de Certificados Digitales.

Que mediante el **INF-TJ 691/2019** se concluyó que en cumplimiento al Decreto Supremo N° 3527 de 11 de abril de 2018 (**D.S. 3527**), esta Autoridad efectuó el análisis correspondiente a la normativa internacional vigente relacionada al desarrollo de software de aplicación para la generación de par de claves para el servicio de certificación digital con el propósito de elaborar un instructivo de homologación de software de aplicación para la generación de par de claves para el servicio de certificación digital, el cual deberá ser aprobado y puesto en vigencia mediante Resolución Administrativa Regulatoria.



I-LP-12534

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

**CONSIDERANDO 3.- MARCO NORMATIVO**

Que la ATT en lo que se refiere a telecomunicaciones, tecnología de información y comunicación y servicio postal, tiene la atribución establecida en el numeral 15 del artículo 14 de la Ley N° 164 de: *"Elaborar, actualizar y modificar manuales, instructivos, circulares y procedimientos a ser aplicados en el sector"*.

Que el Parágrafo I del Artículo Único del Decreto Supremo N° 1793 de 13 de noviembre de 2013 (D.S. 1793) aprobó el Reglamento a la Ley N° 164, para el Desarrollo de Tecnologías de Información y Comunicación, que en Anexo forma parte integrante del presente Decreto Supremo.

Que la Disposición Transitoria Primera del D.S. 1793 estipula lo siguiente:

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, en un plazo no mayor a:

- Ocho (8) meses a partir de la publicación del presente Decreto Supremo, elaborará y aprobará los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las entidades certificadoras;
- Seis (6) meses a partir de la aprobación de los estándares técnicos, deberá implementar la infraestructura y procedimientos internos necesarios para la aplicación de la firma y certificación digital como Certificadora Raíz.

Que el artículo primero del D.S. 3527 modificó el D.S. 1793 en sus artículos 3, 25, 27, 33, 34, 39 y 45 e incorporó el inciso h) y el inciso i) en el Parágrafo III del artículo 3, el inciso l) en el Parágrafo I del artículo 27, inciso k) en el artículo 33, inciso f) en el Parágrafo II del artículo 34, inciso l) en el artículo 38 e inciso q) en el artículo 43.

CONSIDERANDO 4.- ANÁLISIS TÉCNICO Y LEGAL

Que con el objeto de contar con un instructivo que establezca los requisitos necesarios para la homologación de Software de Aplicación para la Generación de Par de Claves para el Servicio de Certificación Digital y su Desarrollador se siguieron estándares y recomendaciones internacionales que establecen los lineamientos y características técnicas de seguridad para el desarrollo de software, conforme lo estipulado en el INF-TJ 691/2019.

Que en virtud a lo establecido en el numeral 15 del artículo 14 de la Ley N° 164, entre las atribuciones de la ATT, se encuentra la de elaborar, actualizar y modificar manuales, instructivos, circulares y procedimientos a ser aplicados en el sector, por lo que corresponde la aprobación del "INSTRUCTIVO PARA LA HOMOLOGACIÓN DE SOFTWARE DE APLICACIÓN PARA LA GENERACIÓN DE PAR DE CLAVES PARA EL SERVICIO DE CERTIFICACION DIGITAL", sea mediante Resolución Administrativa Regulatoria conforme lo señalado en el INF-TJ 691/2019 y su anexo adjunto.

POR TANTO:

El Director Ejecutivo de la ATT, Ingeniero Roque Roy Méndez Soletto, designado mediante Resolución Suprema N° 19249 de 03 de agosto de 2016, en ejercicio de sus atribuciones conferidas por ley y demás normas vigentes a nombre del Estado Plurinacional de Bolivia;



I-LP-12534



RESUELVE:

PRIMERO.- APROBAR el INSTRUCTIVO PARA LA HOMOLOGACIÓN DE SOFTWARE DE APLICACIÓN PARA LA GENERACIÓN DE PAR DE CLAVES PARA EL SERVICIO DE CERTIFICACION DIGITAL, que forma parte integrante e indivisible de la presente Resolución Administrativa Regulatoria.

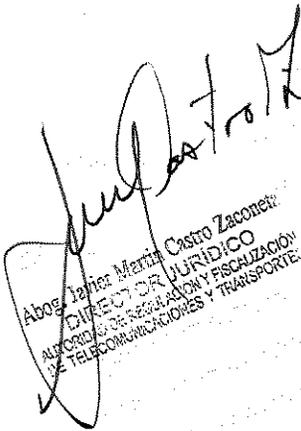
SEGUNDO.- DISPONER que el INSTRUCTIVO PARA LA HOMOLOGACIÓN DE SOFTWARE DE APLICACIÓN PARA LA GENERACIÓN DE PAR DE CLAVES PARA EL SERVICIO DE CERTIFICACION DIGITAL, entrará en vigencia a partir de su publicación.

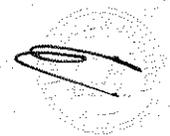
TERCERO.- NOTIFICAR a la Dirección Técnica Sectorial de Telecomunicaciones y TIC y a la Unidad de Homologaciones para efectos de conocimiento y otros actos pertinentes.

CUARTO.- INSTRUIR a la Dirección Técnica Sectorial de Telecomunicaciones y TIC 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, comuníquese y archívese.


Ing. Roque Roy Méndez Soletó
DIRECTOR EJECUTIVO:
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES


Abog. Javier Martín Castro Zaconeri
DIRECTOR JURÍDICO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES



I-LP-12534

**INSTRUCTIVO PARA LA HOMOLOGACIÓN DE SOFTWARE DE APLICACIÓN PARA LA GENERACIÓN DE PAR DE CLAVES PARA EL SERVICIO DE CERTIFICACION DIGITAL****Artículo 1 (Objeto). –**

Establecer el procedimiento para la homologación del software de aplicación o aplicativo para la generación de par de claves para el servicio de certificación digital, cumpliendo con los estándares y formatos de seguridad establecidos en la normativa vigente.

Artículo 2 (Ámbito de aplicación).-

La aplicación del presente instructivo es para toda persona jurídica, pública o privada, nacional o extranjera que desarrolle software de aplicación o aplicativo de generación de par de claves para el servicio de certificación digital, en el marco del Decreto Supremo N° 3527 el cual Modificó al Decreto Supremo N° 1793 aprobando entre otros, la posibilidad de generar el par de claves de certificación digital a través de Software.

Artículo 3 (Definiciones). –

Además de lo establecido en la normativa vigente, se deberán considerar las siguientes definiciones:

Software de aplicación o aplicativo: Conjunto de programas o aplicaciones informáticas que permiten a la computadora realizar determinadas tareas.

Software de aplicación para la generación de par de claves: Es un software criptográfico que genera, almacena y protege claves criptográficas.

FIPS140-2 - Federal Information Processing Standard 140-2 (Estándares Federales de Procesamiento de la Información publicación 140-2): Estándar de requerimientos de seguridad para módulos criptográficos (Security Requirements for Cryptographic Modules se publicó en su primera versión en el 2001 y se tiene una última actualización del 3 de diciembre de 2003.

Artículo 4 (Alcance). –

La Categoría y Subcategoría que se adicionan a la lista de equipos sujetos a homologación detallados en la Resolución Administrativa ATT-DJ-RA TL 1022/2013 del 11 de diciembre de 2013, son:

Categoría	Subcategoría
Software de aplicación o aplicativo de la Infraestructura Nacional de Certificación Digital	Software de aplicación para la generación de par de claves

Artículo 5 (Registro del desarrollador). –

El desarrollador del Software de aplicación para la generación de par de claves deberá estar inscrito en el registro de la ATT. Para el propósito el solicitante deberá presentar la siguiente documentación de carácter legal en original o fotocopia legalizada, exceptuando los casos en que la señale fotocopia simple:



I-LP-12534





Resolución Administrativa Regulatoria

- a) Solicitud escrita dirigida al Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT.
- b) Nombre, dirección, teléfono(s), correo electrónico, fax y casilla postal del solicitante
- c) Documentos que certifiquen la naturaleza del solicitante:
 - 1. Personas Jurídicas: Nacionales o Extranjeras:
 - a) Empresa privada:
 - i. Certificado de la matrícula de inscripción actualizada otorgada por registro de comercio en Bolivia.
 - ii. Fotocopia simple del Documento de Identidad del Representante Legal o del Titular designado.
 - iii. Poder Especial que acredite la personería del representante legal que especifique las facultades de apersonamiento y para realizar este tipo de trámite ante la ATT.
 - iv. Para importadores fotocopia simple del Registro de importador emitido por la Aduana, si corresponde.
 - v. Fotocopia simple del Número de identificación Tributaria NIT. y Certificado de Inscripción al Padrón de Contribuyentes actual.
 - b) Entidades Públicas:
 - i. Norma Jurídica de creación y disposición de nombramiento del Titular.
 - ii. Fotocopia simple del Documento de Identidad del Representante Legal o del Titular designado.
 - iii. Poder Especial que acredite la personería del representante legal que especifique las facultades de apersonamiento y para realizar este tipo de trámites ante la ATT.
 - iv. Fotocopia simple del Número de identificación Tributaria NIT. y Certificado de Inscripción al Padrón de Contribuyentes actual.

Artículo 6 (Homologación del software de aplicación para la generación de par de claves para el servicio de certificación digital).-

- 1. Para homologar un software de aplicación para la generación de par de claves el solicitante deberá presentar la siguiente documentación: Solicitud escrita dirigida al Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT.
- 2. Registro de Desarrollador (Fotocopia Simple).
- 3. La solicitud deberá ser realizada de acuerdo al formulario F.3. (Anexo 1), detallando en lengua castellana las siguientes características técnicas y adjuntando la documentación respaldatoria, considerando lo siguiente:

Describir el ciclo de vida del desarrollo del software, que al menos contenga:

- a) Diseño conceptual (requisitos)
- b) Descripción Técnica del Software de aplicación o aplicativo
 - i) Características funcionales y no funcionales
 - ii) Módulos de Seguridad y Autenticación: Algoritmos e encriptación utilizada para el acceso al software de aplicación.
 - iii) Diagrama Entidad Relación
 - iv) Lenguaje de Programación
 - v) Software Base (Versiones)
 - vi) Motor de Bases de Datos y su versión
 - vii) Protocolo de pruebas.



I-LP-12534



Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 311/2019

- viii) Resultado de las pruebas y ajustes: Documentación sobre todas las pruebas efectuadas durante el desarrollo.
 - ix) Versiones (Revisiones): Documentación de las versiones, revisión de todos los cambios realizados durante el diseño y el desarrollo.
 - x) Programa fuente (última versión)
 - xi) Procedimientos en las Bases de Datos
 - xii) Protocolos de Seguridad
 - xiii) Código o Programa ejecutable
 - xiv) Certificado y/o Informe de Auditoría orientado a garantizar la seguridad del Software de Aplicación elaborado por una empresa tercera autorizada y/o acreditada para realizar este tipo de evaluaciones (Adjuntar documentación de respaldo).
 - xv) MD5 o SHA1 de la versión final del Software de Aplicación
- c) Manual de Uso del Software
 - d) Cualquier documentación adicional, que permita visualizar el diseño, desarrollo, pruebas y puesta en producción del software de aplicación o aplicativo para la generación de claves.
 - e) En caso de que la solicitud sea para una familia de herramientas, se debe remitir documentos que respalden, certifiquen y/o garanticen la homogeneidad de estas herramientas en cuanto a sus características técnicas principales.

Artículo 7 (De la responsabilidad)

- I. El desarrollador del software de aplicación o aplicativo para la generación de claves, es responsable de la correcta generación del par de claves para los propósitos del servicio de Certificación Digital.
- II. Toda entidad Certificadora, debe hacer uso de un software de aplicación o aplicativo registrado en la ATT.

Artículo 8 (Actualizaciones, renovación y/o reevaluación)

En caso de realizar cualquier modificación al código del Software Remitido, deberá remitir el formulario F.3. con todos los cambios efectuados y la siguiente documentación que respalde la modificación del software para que la ATT realice la correspondiente evaluación y aprobación:

- a) Documentación que respalde la versión, revisión de todos los cambios realizados durante el diseño y el desarrollo.
- b) MD5 o SHA1 de la versión final del Software de Aplicación.
- c) Certificado y/o Informe de Auditoría orientado a garantizar la seguridad del Software de Aplicación elaborado por una empresa tercera autorizada y/o acreditada para realizar este tipo de evaluaciones (Adjuntar documentación de respaldo).

Artículo 9 (Transitorio). –

Los desarrolladores que hubieran desarrollado un software de aplicación para la generación de claves y que este se encuentra en operación, tienen un plazo para la regularización de seis (6) meses a partir de la publicación del presente instructivo para registrarse y homologar su software de aplicación o aplicativo desarrollado.



I-LP-12534





ANEXOS

TABLA 1) DATOS GENERALES:

Formulario F-3

PRODUCTO	
DESARROLLADOR	
SISTEMA OPERATIVO Y VERSIÓN EN EL QUE FUE CREADO	
COMPATIBILIDAD DE SISTEMAS OPERATIVOS	
LIBRERÍAS PRINCIPALES UTILIZADAS EN EL DESARROLLO	
VERSIÓN DEL PRODUCTO.	
LENGUAJES UTILIZADOS PARA EL DESARROLLO	
CODIGO(S) DE IDENTIFICACIÓN OTORGADO POR EL O LOS ORGANISMO(S) INTERNACIONAL(ES) QUE CERTIFICA(N) AL EQUIPO	
RESUMEN DEL USO/SERVICIO A APLICAR	

TABLA 2) ESPECIFICACIONES TÉCNICAS PRINCIPALES

Esta tabla es específica para la homologación de Software de generación de par de claves del Servicio de Certificación Digital de la Infraestructura Nacional de Certificación Digital de Bolivia y sus características técnicas principales que deben ser respaldadas por el manual técnico que se adjuntan en la solicitud.

ESPECIFICACIONES TECNICAS	
A) CARACTERISTICAS ESPECIFICAS	
TIPO DE AUTENTICACIÓN Y CONTROL DE ACCESO	
SOPORTE API DEL CLIENTE Y ESTÁNDARES	
TAMAÑO DE LA MEMORIA ROM	
ALGORITMOS CRIPTOGRÁFICOS	
ALGORITMOS DE HASH	
LONGITUD DE CLAVE RSA	
NIVEL DE SEGURIDAD FIPS140-2	
TIPO DE GENERACIÓN DE NÚMEROS ALEATORIOS	
TIEMPO DE RETENCIÓN DE DATOS EN MEMORIA DE TARJETA INTELIGENTE	
REESCRITURA DE CELDA DE MEMORIA DE TARJETA INTELIGENTE	
COMPATIBILIDAD DE SISTEMAS OPERATIVOS	
B) OTRAS CARACTERISTICAS IMPORTANTES	



I-LP-12534