Resolución Administrativa Regulatoria **ATT-DJ-RAR-TL LP 186/2018**

La Paz, 16 de Marzo de 2018

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RA TL 1022/2013 de 11 de diciembre de 2013 **(RAR 1022/2013)**; la Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015 de 9 de enero de 2015 (**RAR 32/2015**), Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 1538/2015 de 27 de noviembre de 2015 (**RAR 1538/2015**); el Informe Técnico ATT-DTLTIC-INF TEC LP 29/2018 de 10 de enero de 2018 **(INFORME TÉCNICO)**; el Informe Juridico ATT-DJ-INF JUR LP 322/2018 de 15 de marzo de 2018 **(INFORME JURÍDICO)**; la demás normativa vigente y aplicable, todo lo que convino ver, se tuvo presente;

Mariene Ruth Ramos Agreda
TÉCNICO LEGAL II
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

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 Nº 0071 de 09 de abril de 2009, concordante con lo establecido en la Disposición Transitoria Novena de la Ley Nº 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación **(Ley Nº 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 RAR 1022/2013 se aprobó el Instructivo para la Homologación de Equipos de Telecomunicaciones, Acreditación de Entidades Certificadoras y Registro de Fabricantes, Distribuidores, Comercializadores, Operadores y Proveedores de Servicios de Telecomunicaciones.

Que mediante RAR 32/2015 se dejó sin efecto la Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 1211/2014 de 11 de julio de 2014 y se aprobó los Estándares técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras.

Que los artículos 15, 16 y 17 de la Sección 4 del Capítulo 2 de la RAR 32/2015 determinan los requisitos mínimos para la Obtención de un Certificado Digital, entre ellos se requiere un dispositivo que permita firmar un documento al signatario, donde sean almacenados y custodiados el certificado digital y su clave privada (Token HSM o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2.

Que mediante RAR 1538/2015 se modificó el Anexo 1, en sus numerales i de los puntos 3 (Formato para el Certificado Digital de una Persona Natural o Física), 4 (Formato para el Certificado Digital de una Persona Jurídica), 5 (Formato para el Certificado Digital de Cargo Público) y el inciso c) del numeral ii del punto 5 (extensiones del Certificado Digital de Cargo Público) de los Estándares Técnicos y Otros

I-LP-5175

Lineamientos Establecidos para el Funcionamiento de las Entidades Certificadoras, aprobado mediante RAR 32/2015, respecto a la estructura del formato de los tres tipos de Certificados Digitales.

Que mediante el INFORME TÉCNICO se concluyó que se debe incluir una nueva categoría y subcategoría de dispositivos de hardware de seguridad de certificación y firma digital (Token, HSM o tarjetas inteligentes - smart cards-) para homologación, los cuales deben cumplir con los estándares de formatos y seguridad establecidos en la normativa vigente del sector para los tipos de certificados digitales aprobados, por lo que recomendó emitir la Resolucion Administrativa Regulatoria, que apruebe el Instructivo para la Homologación de dispositivos de Hardware de seguridad de Certificación y Firma Digital.

Que mediante el INFORME JURÍDICO se concluyó que en el marco de lo dispuesto en el inciso j) del artículo 38 del Reglamento a la Ley Nº 164, de 08 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013(**Reglamento para el Desarrollo de Tecnologías de Información y Comunicación**), a efectos de incluir una nueva categoría y subcategoría de dispositivos de hardware de seguridad de certificación y firma digital (Token, HSM o tarjetas inteligentes - smart cards) en la lista de equipos sujetos de homologación, debe emitirse la Resolucion Administrativa Regulatoria que apruebe el Instructivo para la Homologación de dispositivos de Hardware de seguridad de Certificación y Firma Digital.

CONSIDERANDO 3.- MARCO NORMATIVO

Que el numeral 9 de la Ley N° 164, establece: *"Homologar equipos de telecomunicaciones y tecnologías de información y comunicación en todo el país."*

Que el artículo 14 del Reglamento a la Ley de Telecomunicaciones aprobado mediante D.S. 1391 de 24 de octubre de 2012 (**Reglamento a la Ley N° 164**), establece: *" I. Se entiende por homologación, al procedimiento realizado por la ATT de verificación de la compatibilidad de funcionamiento y operación de equipos o terminales con una red de telecomunicaciones, de acuerdo a los estándares nacionales elaborados por la ATT y aprobados por el Ministerio de Obras Públicas, Servicios y Vivienda, así como a los estándares internacionales, principalmente para: a) Proteger de interferencias perjudiciales a los servicios de telecomunicaciones de operadores o proveedores autorizados, garantizando la utilización apropiada del espectro radioeléctrico; b) Verificar que los equipos o terminales tengan las características técnicas adecuadas para el tipo de servicio autorizado. II. La ATT, emitirá instructivos técnicos para homologación los cuales serán actualizados periódicamente. III. Cuando así se requiera, la ATT podrá contratar a terceras personas para las pruebas técnicas de homologación, las mismas que serán denominadas Entidades Verificadoras y su contratación podrá ser para casos específicos o por plazo determinado de acuerdo a la normativa vigente aplicable. IV. No podrán ser designadas Entidades Verificadoras las personas naturales o jurídicas que sean titulares de autorizaciones para proveer servicios de telecomunicaciones y tecnologías de información y comunicación o que tengan relación directa con proveedores o comercializadores de equipos u operadores y proveedores de servicios. V. Para la solicitud de homologación de equipos de telecomunicaciones incluidos aquellos que utilizan*

I-LP-5175

frecuencias radioeléctricas de uso libre, los fabricantes, proveedores o comercializadores deberán previamente estar inscritos en el registro de la ATT."

Que el artículo 15 del Reglamento a la Ley N° 164, en cuanto al procedimiento para la homologación de equipos dispone: *"I. A solicitud de los interesados, sean fabricantes, operadores de servicios, proveedores o comercializadores de equipos destinados a redes de telecomunicaciones, la ATT procederá a la homologación de los mismos, mediante Resolución Administrativa en el plazo máximo de treinta (30) días, siempre y cuando se cumplan los requisitos establecidos en los instructivos técnicos de homologación. II. Para los equipos que requieran pruebas de laboratorio con el fin de su homologación, la ATT podrá solicitar al interesado un prototipo por cada tipo de equipo a ser homologado, el mismo que será entregado a la ATT hasta la finalización de las pruebas. III. La ATT publicará en su página web de manera permanente los equipos que hayan sido homologados y por tanto estarán autorizados para su uso y comercialización en el territorio nacional."*

Que el artículo 24 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, 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 artículo 33 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, en cuanto a las características de la firma digital dispone que debe cumplir mínimamente las siguientes condiciones: *" [...] c) Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable; d) Ser creada por medios que el firmante pueda mantener bajo su exclusivo control y la firma sea controlada por la persona a quien pertenece. [...] g) Que el método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual fue generado un registro de creación de la firma;[..] i) Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del signatario; [...]"*

Que el inciso j) del artículo 38 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, que dispone: *"Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones".*

CONSIDERANDO 4.- ANÁLISIS TÉCNICO Y LEGAL

Que en el marco de lo dispuesto en el inciso j) del artículo 38 del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación la ATT tiene la atribución de aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones.

Que en virtud a lo expuesto mediante el INFORME TÉCNICO y el INFORME JURÍDICO, se concluyó que se debe incluir una nueva categoría y subcategoría de dispositivos de hardware de seguridad de certificación y firma digital (Token, HSM o tarjetas inteligentes - smart cards-) en la lista de equipos

I-LP-5175

sujetos a homologación, por lo que corresponde emitir Resolución Administrativa Regulatoria que apruebe el Instructivo para la Homologación de dispositivos de Hardware de seguridad de Certificación y Firma Digital.

POR TANTO:

El Director Ejecutivo de la ATT, Ingeniero Roque Roy Méndez Soleto, 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;

RESUELVE:

PRIMERO.- APROBAR el **INSTRUCTIVO PARA LA HOMOLOGACIÓN DE DISPOSITIVOS DE HARDWARE DE SEGURIDAD DE CERTIFICACIÓN Y FIRMA DIGITAL** y su Anexo, mismos que forman parte integrante e indivisible de la presente Resolución Administrativa Regulatoria.

SEGUNDO.- 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, comuníquese y archívese.

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

Cecilia Rios Moeller
DIRECTORA JURÍDICA
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

DIRECCIÓN JURÍDICA V° B° J.C.T.

DIRECCIÓN JURÍDICA V° B° M.V.R.A. A.T.T.

I-LP-5175

Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 186/2018

INSTRUCTIVO PARA LA HOMOLOGACIÓN DE DISPOSITIVOS DE HARDWARE DE SEGURIDAD PARA FIRMA DIGITAL

Artículo 1 (Objeto).-

Adicionar a la lista de equipos sujetos a homologación los dispositivos de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-) los cuales deben cumplir con los estándares y formatos de seguridad establecidos en la normativa vigente.

Artículo 2 (Objetivos).-

a) Dar cumplimiento a los estándares establecidos para el uso de la firma digital y los certificados digitales disponibles al público.

b) Garantizar el cumplimiento de los aspectos de seguridad establecidos por la ATT en la funcionalidad de los dispositivos de hardware de seguridad, indistintamente del proveedor del servicio.

Articulo 3 (Ámbito de aplicación).-

Están sometidas a la aplicación del presente instructivo toda aquella persona natural o jurídica, pública o privada, nacional o extranjera que fabrique, importe, distribuya, comercialice y/o opere con dispositivos de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-).

Artículo 4 (Definiciones).-

Se deberán considerar las siguientes definiciones:

HSM - Hardware Security Module (Dispositivo de Hardware de Seguridad): Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas.

Token: Es un dispositivo electrónico USB que permiten almacenar contraseñas y certificados y llevan la identidad digital del signatario propietario.

Smart-Card (Tarjetas inteligentes de contacto): Permiten almacenar contraseñas y certificados y llevan la identidad digital del signatario propietario.

FIPS140-2 - Federal Information Processing Standard 140-2 (Estándares Federales de Procesamiento de la Información publicación 140-2): Es un estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. Su título original es Security Requirements for Cryptographic Modules (requerimientos de seguridad para módulos criptográficos), que salió a la luz en 2001 y la última actualización es del 3 de diciembre de 2003.

Artículo 5 (Alcance).-

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

I-LP-5175

Categoría	Subcategoría
Dispositivos de Hardware de Seguridad	HSM (Hardware Security Module) Token Smart-Cards

Artículo 6 (Organismos internacionales reconocidos).-

Se complementa el artículo 24 de la RAR ATT-DJ-RA TL 1022/2013 del 11 de diciembre de 2013 con los siguientes organismos:

- National Institute of Standards and Technology (NIST) de los Estados Unidos.
- Canadian Security Establishment (CSE).
- Internet Engineering Task Force (IETF).

Artículo 7 (Registro de fabricantes, distribuidores, importadores, comercializadores y proveedores de servicios de certificación digital).-

Los fabricantes, distribuidores, importadores, comercializadores y proveedores de servicios de certificación digital que comercialicen u operen dispositivos de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-) deberán estar inscritos en el registro de la ATT, los requisitos y procedimientos para el registro están especificados en la RAR ATT-DJ-RA TL 1022/2013 del 11 de diciembre de 2013.

Artículo 8 (Homologación de dispositivos de hardware de seguridad - HSM, Token, tarjetas inteligentes -smart cards-).-

I. Para homologar un dispositivo de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-) por cada tipo de equipo, marca y modelo el solicitante deberá presentar toda la documentación señalada en la RAR ATT-DJ-RA TL 1022/2013 del 11 de diciembre de 2013 excepto los reportes de pruebas de laboratorio.

II. Se adiciona el Formulario F-2 en el Anexo, mismo que detalla las características mínimas que deben cumplir los dispositivos de hardware de seguridad para firma digital.

III. El procedimiento de homologación está especificado en la RAR ATT-DJ-RA TL 1022/2013 del 11 de diciembre de 2013.

Artículo 9 (Plazo de regularización).-

Los fabricantes, distribuidores, importadores, comercializadores y proveedores de servicios de certificación digital tienen un plazo de regularización de 6 meses a partir de la publicación del presente instructivo para registrarse y homologar los dispositivos de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-).

I-LP-5175

Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 186/2018

ANEXO
Formulario F-2

TABLA 1) DATOS GENERALES:

PRODUCTO	
FABRICANTE	
MARCA	
MODELO	
NOMBRE(S) DEL O LOS ORGANISMO(S) INTERNACIONAL(ES) QUE CERTIFICA(N) AL EQUIPO	
CODIGO(S) DE IDENTIFICACION 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 los dispositivos de hardware de seguridad (HSM, Token, tarjetas inteligentes -smart cards-) y sus características técnicas principales que deben ser respaldadas por los manuales técnicos que se adjuntan en la solicitud.

A) ESPECIFICACIONES FISICAS	
Dimensiones	
Peso	
Cantidad y tipo de interfaces	
B) ESPECIFICACIONES TECNICAS	
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	
C) OTRAS CARACTERISTICAS IMPORTANTES	

I-LP-5175