Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019

La Paz, 24 de abril de 2019

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RA TL 32/2015 de 09 de enero de 2015 (**R.A.R. 32/2015**); la Resolución Administrativa Regulatoria ATT-DJ-RAR- TL LP 845/2018 de 13 de noviembre de 2018 (**R.A.R. 845/2018**); el Informe Técnico Jurídico ATT-DTLTIC-INF TJ LP 433/2019 de 12 de abril de 2019 (**INF-TJ 433/2019**); la demás 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.

Lic. Juan Carlos Mancilla Peñafiel
ANALISTA LEGAL
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

CONSIDERANDO 2.- ANTECEDENTES

Que mediante **R.A.R. 32/2015** se estableció 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. 845/2018** se aprobó 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 el **INF-TJ 433/2019** concluyó que como parte de las actividades concernientes y en cumplimiento al **D.S. N° 3527**, la ATT efectuó el análisis correspondiente a la normativa internacional vigente relacionada con la emisión y utilización de certificados digitales a través de dispositivos criptográficos basados en hardware y software recomendando la emisión de la correspondiente Resolución Administrativa Regulatoria que apruebe y ponga en vigencia el Estándar Técnico para la Emisión de Certificados Digitales conforme al Anexo y las características técnicas detalladas en el mencionado Informe.

DIRECTOR JURÍDICO V° B° J.M.O.Z. A.T.T.

CONSIDERANDO 3.- MARCO NORMATIVO

Que el parágrafo 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 comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.H.M.S.O. A.T.T.

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 de 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**) modifico ciertos artículos del REGLAMENTO A LA LEY N° 164 de la siguiente manera:

I. Se modifican los incisos a) y g) del Parágrafo III del artículo 3 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"a) Autenticación: Proceso técnico de verificación por el cual se garantiza la identidad del signatario en un mensaje electrónico de duros o documento digital, que contengan firma digital;

g) Signatario: Es la usuaria o usuario titular de un certificado digital emitido por una entidad certificadora autorizada, que le permite firmar digitalmente."

DIRECTOR JURÍDICO V° B° J.M.C.Z. A.T.T.

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

I-LP-10715

II. Se modifica el artículo 25 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"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."

III. Se modifica el inciso i) del Parágrafo I del artículo 27 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"i) Contemplar las características técnicas y los límites de uso del certificado;"

IV. Se modifican los incisos b), d) y e) del artículo 33 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"b) Haber sido creada durante el periodo de vigencia del certificado digital válido del signatario;

d) Ser creada por medios que permitan al signatario a quien pertenece el certificado digital, mantener el control sobre su uso;

e) Contener información vinculada a su titular y su uso;"

V. Se modifica el incido d) del Parágrafo II del artículo 34 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"d) Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del signatario y que su certificado digital no haya expirado, no haya sido revocado ni su pendido;"

VI. Se modifica el inciso d) del artículo 39 del del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"d) Validar y comprobar cuando corresponda, la identidad y existencia real del solicitante;"

VII Se modifica el artículo 45 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"ARTÍCULO 45.- (GARANTÍA).

I. Las entidades certificadoras deberán obtener una boleta de garantía de cumplimiento de contrato, por el siete por ciento (7%) sobre sus proyecciones para el primer año, que respalde su actividad para prestación de servicios de certificación digital.

II. A partir del segundo año, la entidad certificadora pública deberá mantener vigente una boleta de garantía de cumplimiento de contrato, por el tres y medio por ciento (3,5%) de sus ingresos brutos de la gestión inmediata anterior, que respalde su actividad durante la vigencia de la autorización para prestación de servicios de certificación digital.

DIRECTOR JURÍDICO V° B° J.M.C.Z. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

III. A partir del segundo año, las entidades certificadoras privadas deberán 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, que respalde su actividad durante la vigencia de la autorización para prestación de servicios de certificación digital.

IV. El incumplimiento de este requisito dara lugar a las acciones correspondientes en el marco de las competencias de la ATT".

Que el artículo 3 del Decreto Supremo N° 3527 de 11 de abril de 2018 (**D.S. N° 3527**) incorporo algunos párrafos a diferentes artículos del REGLAMENTO A LA LEY N° 164 de la siguiente manera:

I. Se incorporan el inciso h) y el inciso i) en el Parágrafo III del artículo 3 del REGLAMENTO A LA LEY N° 164, con los siguientes textos:

*h) **Firma Digital Automática**: Firma Digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en éste.*

*i) **Sistema Digital Automática**: El sistema compuesto de equipos y personal pertinente que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos.*

II. Se incorpora el inciso 1) en el Parágrafo I del artículo 27 del REGLAMENTO A LA LEY N° 164 con el siguiente texto:

"*Identificar su nivel de seguridad, en caso que el par de claves sea generado por dispositivo éste tendrá nivel de seguridad alto, en caso que el par de claves sea generado por software éste tendrá nivel de seguridad normal.*"

III. Se incorpora el inciso k) en el artículo 33 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"k) En el caso de la Firma Digital Automática, debe utilizarse en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

IV. Se incorpora el inciso f) en el parágrafo II del artículo 34 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"f) En el caso de la Firma Digital Automática, que al momento de su creación, los datos con los que se creare sean controlados por medios que permitan evitar de forma técnicamente segura y confiable su uso por terceros no autorizados, para otros fines que no se encuentren establecidos en su certificado digital."

V. Se incorpora el inciso 1) en el artículo 38 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

"1) Definir el tiempo de vigencia de los certificados digitales."

VI. Se incorpora el inciso q) en el artículo 43 del REGLAMENTO A LA LEY N° 164, con el siguiente texto:

DIRECTOR JURÍDICO V° B° J.M.C.Z. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

"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."

CONSIDERANDO 4.- ANALISIS TECNICO Y LEGAL

Que en el marco de lo dispuesto por el **D.S. N° 3527** el cual establece que la ATT podrá modificar y adecuar los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las entidades certificadoras y en virtud a lo dispuesto por el **INF-TJ 433/2019** se concluyó que se debe aprobar el Estándar Técnico para la Emisión de Certificados Digitales, por lo que en virtud a lo instruido por el mencionado Decreto Supremo, por lo que corresponde emitir la Resolucion Administrativa Regulatoria que apruebe y ponga en vigencia el Estándar Técnico para la Emisión de Certificados Digitales.

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 **ESTÁNDAR TÉCNICO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES**, así como sus Anexos, el cual forma 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 y Archívese.

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

Abog. Javier Martin Castro Zaconeta
DIRECTOR JURÍDICO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

I-LP-10715

ESTÁNDAR TÉCNICO PARA LA EMISIÓN DE CERTIFICADOS DIGITALES

Capítulo I
Disposiciones Preliminares

Artículo 1 (Objeto)

El presente estándar tiene por objeto definir los lineamientos y características técnicas para la emisión de Certificados Digitales dentro de la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia.

Artículo 2 (Definiciones)

Para efectos del cumplimiento del presente instructivo, además de lo establecido en la normativa vigente, se entiende por:

Solicitante: Persona Natural o Jurídica que solicita se le emita un certificado digital.
Signatario: Es la usuaria o usuario titular de un certificado digital emitido por una Entidad Certificadora Autorizada, que le permite firmar digitalmente.
Firma Digital Automática: Firma Digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en este.
Sistema Informático: El sistema compuesto de equipos y de personal pertinente que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos.

Artículo 3 (Abreviaturas)

Para efectos del cumplimiento del presente Estándar, se entiende por:

ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
CRL: (Certificate Revocation List) Lista de Certificados Revocados.
EC: Entidad Certificadora.
ECA: Entidad Certificadora Autorizada.
INCD: Infraestructura Nacional de Certificación Digital
OID: Identificador de Objeto
PKCS: (Public-Key Cryptography Standards) Estándares de Criptografía de Llave Pública
PKI: (Public Key Infraestructure) Infraestructura de Clave Pública.

Artículo 4 (Estándares, Recomendaciones y Normas Internacionales)

Los siguientes Estándares, Recomendaciones y Normas Internacionales son adoptados para el presente .

a. RFC 3647 - Política de Certificados de Infraestructura de Clave Pública y Marco de Prácticas de Certificación
b. ITU-T X.509 - Marcos para certificados de claves públicas y atributos.
c. ISO 27001 - Sistemas de Gestión de Seguridad de la Información
d. FIPS 140-2 - Requisitos de seguridad para los módulos criptográficos
e. CWA 14365-2 - Guía sobre el uso de firmas electrónicas - Parte 2: Perfil de protección para dispositivos de creación de firmas de software
f. ETSI EN 319 411-2 V2.2.0 - Firmas e Infraestructuras Electrónicas (ESI)

I-LP-10715

Capítulo II
Emisión de certificados digitales

Articulo 5.- (Formato de los certificados)

I. 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), para persona jurídica deben cumplir con la siguiente estructura:

Formato para el Certificado Digital de una Persona Jurídica	
Versión (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 (issuer):	CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón Social de la ECA; C = "Entidad " estándar de acuerdo a ISO3166 {BO}
Periodo de validez (validity)	Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón Social de la empresa o Institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; 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)	Algoritmo: RSA, Longitud: mínimo 2048 bits.

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

Formato para el Certificado Digital de una Persona Natural o Física	
Versión (version):	el valor del campo es 2.

I-LP-10715

DIRECTOR EJECUTIVO V°B° R.R.M.S. A.T.T.

Número de Serie (serialNumber)	Número asignado por la ECA
Algoritmo de firmas (signatureAlgorithm):	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer):	CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón Social de la ECA; C = "Entidad " estándar de acuerdo a ISO3166 {BO}
Periodo de validez (validity)	Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = Nombres y Apellidos de la persona Natura; 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)	Algoritmo: RSA, Longitud: mínimo 2048 bits.

III. El formato para los certificados digitales emitidos para dispositivo criptográfico basado en software (nivel normal de seguridad), para persona jurídica que sean utilizados para interoperabilidad de servicios deben cumplir con la siguiente estructura:

Formato para el Certificado Digital de una Persona Jurídica	
Versión (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 (issuer):	CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón Social de la ECA; C = "Entidad " estándar de acuerdo a ISO3166 {BO}

DIRECTOR JURIDICO V° B° J.M.C.B. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

Periodo de validez (validity)	Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón Social de la empresa o Institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; 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)	Algoritmo: RSA, Longitud: mínimo 2048 bits.

Adicionalmente, los certificados deben cumplir con las extensiones definidas a continuación:

Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier):	Función Hash (SHA1) del atributo subjectPublicKey.
Identificador de la clave del suscriptor (subjectKeyIdentifier):	
Uso de Claves (keyUsage):	digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1, keyAgreement = 0, keyCertSign = 0, cRLSign = 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). Identificador de Objeto= OID del certificado {alfanumérico}
Restricciones Básicas (basicConstraints):	CA = FALSE.

DIRECTOR JURÍDICO V° B° J.M.C.U. A.T.T.

I-LP-10715

DIRECTOR EJECUCIÓN V° B° R.R.M.S. A.T.T.

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

El campo Política de Certificación (certificatePolicies), además de contener la dirección de la Política de Certificación, debe contener el OID del tipo de Certificado, de acuerdo a la estructura de OIDs establecido en el Anexo 3 del presente estándar.

Artículo 6.- (Emisión de certificados digitales)

a) Certificados digitales emitidos por dispositivo criptográfico basado en software. El solicitante deberá generar el par de claves (público y privada) por software, en un dispositivo seguro que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente (ver descripción en Anexo 2), posteriormente debe proporcionar a una Entidad Certificadora Autorizada la Solicitud de Firma de Certificado - CSR en un archivo electrónico que contiene el requerimiento de firma de certificado (CSR- *Certificate Signing Request*) en formato PKCS#10 (ver Anexo 1).

Las ECAs pondrán a disposición de los solicitantes un software para la generación del par de claves (público y privada), garantizando la confidencialidad de la información, de acuerdo a lo establecido en el Artículo 43 del Decreto Supremo 1793; proporcionando al signatario el contenedor PKCS#12 (certificado, claves pública y privada). Este software deberá ser homologado por la ATT.

b) Certificados digitales emitidos por dispositivo criptográfico basado en hardware. El solicitante deberá generar el par de claves (público y privada) en un dispositivo que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente (ver descripción en Anexo 2), posteriormente debe proporcionar a una Entidad Certificadora Autorizada la Solicitud de Firma de Certificado - CSR en un archivo electrónico que contiene el requerimiento de firma de certificado (CSR- *Certificate Signing Request*) en formato PKCS#10 (ver Anexo 1).

Una vez revisada la solicitud por parte de la ECA y concluido el proceso de registro, la ECA debe firmar digitalmente la solicitud de firma de certificado (CSR) y hacer entrega al Signatario de su certificado.

Artículo 8.- (Condiciones de uso)

a) Firma Digital Automática

Los certificados digitales con seguridad Alta o Normal podrán ser usados para realizar Firma Digital Automática, siempre y cuando el firmado se realice en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

Para la realización del firmado digital de forma automática, se debe comprobar que los datos con los que se creare sean controlados por medios que permitan evitar de forma técnicamente segura y confiable su uso por terceros no autorizados, para otros fines que no se encuentren descritos en el certificado digital.

I-LP-10715

b) Certificados digitales emitidos por dispositivo criptográfico basado en software

Los certificados digitales emitidos a través de dispositivos criptográficos basados en software solo podrán ser utilizados por Personas 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.

Capítulo II
Otros Aspectos

Artículo 9- (Incumplimiento)

El incumplimiento a cualquier disposición del presente Estándar, implica una infracción contra las atribuciones de la Autoridad Reguladora de acuerdo al Reglamento de Sanciones vigente.

DIRECTOR JURÍDICO V° B° J.M.C.Z. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

ANEXO 1
ESTÁNDARES CRIPTOGRÁFICOS

La generación de certificados está basada en estándares de criptografía PKCS.

ESTÁNDAR	NOMBRE	DESCRIPCIÓN
PKCS#1	Estándar criptográfico RSA	Define el formato de almacenamiento de clave RSA sin encriptar. Estándar: RFC 3447.
PKCS#7	Estándar sobre la sintaxis del mensaje criptográfico	Usado para firmar y/o cifrar mensajes en PKI. También usado para la diseminación de certificados o colección de certificados públicos. Estándar: RFC 2315.
PKCS#8	Estándar sobre la sintaxis de la información de clave privada	Formato de clave privada cifrada para claves RSA DSA EC. Estándar: RFC 5208.
PKCS#10	Estándar de solicitud de certificación	Formato de solicitud de firma de certificado CSR. Estándar: RFC 2986.
PKCS#11	Interfaz de dispositivo criptográfico ("Cryptographic Token Interface" o cryptoki)	Define un API genérico de acceso a dispositivos criptográficos (token de seguridad / tarjeta inteligente / acceso HSM)
PKCS#12	Estándar de sintaxis de intercambio de información personal	Define el formato de fichero usado para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

DIRECTOR JURIDICO V° B° J.M.C.Z. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.M.S. A.T.T.

ANEXO 2
NIVELES DE SEGURIDAD

FIPS 140-2 define cuatro niveles de seguridad. La validación de FIPS 140-2 especificará el nivel de seguridad que el producto deberá cumplir.

Nivel 1	Usado para cifrado por software, impone requisitos de seguridad muy limitados. Todos los componentes deben ser de *nivel de producción* y los diversos tipos flagrantes de inseguridad deben estar ausentes.
Nivel 2	Requiere autenticación *basada en el cargo del usuario*. (No requiere autenticación individual de los usuarios) También requiere la capacidad para detectar la intrusión física mediante sistemas de bloqueo físico o precintos de seguridad.
Nivel 3	Proporciona resistencia a la intrusión física con fines de desmontaje o modificación, de manera que dificulta al máximo los ataques. Si se detecta la intrusión, el dispositivo debe ser capaz de borrar los parámetros de seguridad críticos. El Nivel 3 también incluye protección criptográfica eficaz y administración de claves, autenticación basada en la identidad y separación física o lógica entre las interfaces a través de las que se accede a los parámetros de seguridad crítica y se sale de ellos.
Nivel 4	Incluye una protección avanzada contra violación y está diseñado para ser utilizado con productos que operan en ambientes desprotegidos físicamente.

DIRECTOR JURÍDICO V° B° J.M.A.Z. A.T.T.

I-LP-10715

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.