

Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

La Paz, 09 de Enero de 2015

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 1211/2014 de 11 de julio de 2014; el Informe Técnico ATT-DS-INF TEC LP 14/2015 de 07 de enero de 2015; el Informe Jurídico ATT-DJ-INF-JUR LP 50/2015 de 09 de enero del 2015; la normativa aplicable vigente y todo lo que se tuvo presente.

CONSIDERANDO 1: (Antecedentes)

La Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 1211/2014 de 11 de julio de 2014, mediante la cual se aprobó los Estándares Técnicos y Otros Lineamientos Establecidos para el Funcionamiento de las Entidades Certificadoras y sus diez (10) Anexos,

El Informe Técnico ATT-DS-INF TEC LP 14/2015 de 07 de enero de 2015, señala como conclusión que en cumplimiento a lo establecido en el Artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013, se ha efectuado complementaciones y modificaciones a los “ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS” y los diez (10) Anexos, aprobados mediante la Resolución Administrativa Regulatoria ATT DJ RA TL LP 1211/2014 de 11 de julio de 2014; y recomienda:

- Dejar sin efecto los “ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS” y diez (10) Anexos, aprobados mediante la Resolución Administrativa Regulatoria ATT DJ RA TL LP 1211/2014 de 11 de julio de 2014.
- Aprobar los nuevos “ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS” y sus diez (10) Anexos, que se encuentran adjunto al Informe.

El Informe Jurídico ATT-DJ-INF-JUR LP 50/2015 de 09 de enero de 2014, recomienda aprobar mediante Resolución Administrativa Regulatoria, los “ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS” y sus diez (10) Anexos, que se encuentran adjunto al Informe Técnico.

CONSIDERANDO 2: (Marco normativo aplicable)

Que el parágrafo II del Artículo 103 de la Constitución Política del Estado, determina 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, General de Telecomunicaciones, Tecnologías de Información y Comunicación de 8 de agosto de 2011, dispone como objetivos asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de



DIRECCIÓN JURÍDICA
VO DO
G.S.P.

**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

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.

Que el Artículo 24 del Reglamento a la Ley N° 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, establece que: *"Los certificados digitales deben ser emitidos por la 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 completar la información necesaria para la verificación de la firma digital"*.

Que en cuanto a las características del certificado digital establecidas en el parágrafo II del Artículo 27 del mencionado Reglamento, señala que la ATT, mediante Resolución Administrativa establecerá el formato y estructura de los certificados digitales tanto para personas naturales como para personas jurídicas.

Que de acuerdo al parágrafo II del Artículo 28 del citado Reglamento, 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 citado Reglamento, en su parágrafo IV del Artículo 32, 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 Artículo 36 del Reglamento antes mencionado, establece los niveles de la Infraestructura Nacional de Certificación Digital, donde existe una entidad Certificadora de nivel Superior encargada de regular y fiscalizar los procesos de certificación.

Que el 1. Primer Nivel del Artículo 37, del mencionado Reglamento dispone que dentro de la estructura jerárquica: *"1. 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, emitirá certificados digitales a las entidades certificadoras públicas y privadas subordinadas"*.

Que el Artículo 38, establece las atribuciones asignadas a la ATT.

CONSIDERANDO 3: (Análisis)

Que conforme al Artículo 14 de la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de 08 de agosto de 2011, la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, tiene la atribución de cumplir y hacer cumplir la presente Ley y sus reglamentos, asegurando la correcta aplicación de sus principios, políticas y objetivos.

Que el Informe Técnico ATT-DS-INF TEC LP 14/2015 y el Informe Jurídico ATT-DJ-INF-JUR LP 30/2015, recomiendan la emisión de la Resolución Administrativa por el que se disponga dejar sin efecto los "ESTÁNDARES TÉCNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS" y los diez (10) Anexos, aprobados mediante la Resolución Administrativa Regulatoria ATT DJ RA TL LP 1211/2014 de 11 de julio de 2014. Asimismo, aprobar los nuevos "ESTÁNDARES TÉCNICOS Y OTROS LINEAMIENTO



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS" y los diez (10) Anexos, adjuntos al Informe Técnico, en conformidad a lo establecido por el inc. j) del Artículo 38 del Reglamento a la Ley N° 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.

CONSIDERANDO 4: (Del ámbito de la competencia)

Que las competencias y atribuciones para la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes están definidas por el Decreto Supremo N° 0071 de 09 de abril de 2009, 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.

Que la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de 08 de agosto de 2011, en su Disposición Transitoria Séptima, dispone: *"La presente Ley entrará en vigencia en la fecha de su publicación, con aplicación progresiva, conforme a la aprobación de sus reglamentos en tanto se aprueben éstos, se aplicarán los reglamentos vigentes de telecomunicaciones y específicos; en tanto se aprueben éstos, se aplicarán los reglamentos vigentes de telecomunicaciones y postal en todo lo que no contravenga a esta Ley".*

Que de conformidad a lo dispuesto por la Disposición Transitoria Novena de la mencionada Ley, la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes cambia de denominación a AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT, asumiendo las atribuciones, competencias, derechos y obligaciones en materia de telecomunicaciones; tecnologías de la información y comunicación; transportes; servicio postal; bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda.

Que mediante Resolución Ministerial N° 006 de 08 de enero de 2014 del Ministerio de Obras Públicas Servicios y Vivienda, se designó a LUIS FELIPE GUZMAN SANJINES, como Director Ejecutivo Interino de la ATT.

POR TANTO:

El Director Ejecutivo Interino de la ATT, en uso de sus atribuciones conferidas por ley y demás normas vigentes.

RESUELVE:

PRIMERO.- Dejar sin efecto los "ESTÁNDARES TÉCNICOS Y OTROS LINEAMIENTOS ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS" y los diez (10) Anexos, aprobados mediante la Resolución Administrativa Regulatoria ATT DJ RA TL LP 32/2014 de 11 de julio de 2014.

SEGUNDO.- APROBAR los nuevos "ESTÁNDARES TÉCNICOS Y OTROS LINEAMIENTOS ESTABLECIDOS PARA EL FUNCIONAMIENTO DE LAS ENTIDADES CERTIFICADORAS" y los diez (10) Anexos, que forman parte integrante de la presente Resolución.



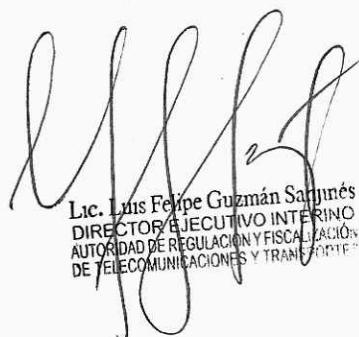


AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

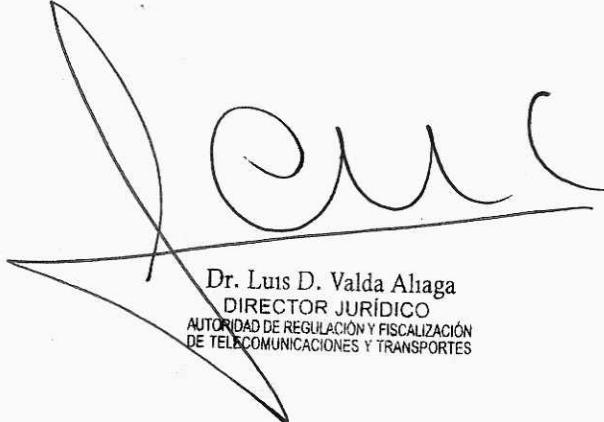
TERCERO.- INSTRUIR a la Unidad de Tecnologías de Información y Comunicación de esta Autoridad, publicar la presente Resolución en un Matutino de circulación nacional, así como en el portal WEB de la Institución.

Regístrate, comuníquese y archívese.



Lic. Luis Felipe Guzmán Sarmiento
DIRECTOR EJECUTIVO INTERINO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Es Conforme;



Dr. Luis D. Valda Aliaga
DIRECTOR JURÍDICO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES



Resolución Administrativa Regulatoria **ATT-DJ-RA TL LP 32/2015**

**ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS
PARA EL FUNCIONAMIENTO DE LAS ENTIDADES
CERTIFICADORAS**

**Capítulo I
Disposiciones Preliminares**

Sección 1.- Objeto, Normativa aplicable, Abreviaturas y Definiciones.

Artículo 1 (Objeto).-

- I. La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes es la encargada de autorizar, regular, fiscalizar, supervisar, controlar y realizar auditorías técnicas a las Entidades Certificadoras.
- II. El presente estándar establece los formatos y procedimientos necesarios para la aplicación de la firma y certificación digital para la Entidad Certificadora Raíz, basado en el Estándar Internacional RFC5280 el cual define el formatos de los certificados X.509 versión 3 y el formato de la Lista de los Certificados Revocados (CRL) X.509 versión 2.
- III. Establece los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras tanto la pública como las privadas.
- IV. Establece los requisitos, condiciones legales, económicas y técnicas para la autorización de la prestación de servicios de Firma y Certificación Digital.

Artículo 2 (Normativa aplicable).-

- I. Los artículos del 78 al 84 de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, Ley N° 164, de 08 de agosto de 2011.
- II. Los artículos del 24 al 56 del Reglamento a la Ley N° 164, de 08 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
- III. La Disposición Transitoria Primera del Decreto Supremo N° 1793 del 13 de noviembre de 2013.

Artículo 3 (Abreviaturas).-

Para efectos del presente estándar entiéndase por:

- **EC:** Entidad Certificadora.
- **ECA:** Entidad Certificadora Autorizada como parte de la PKI Bolivia.
- **ECR:** Entidad Certificadora Raíz.
- **AR:** Agencia de Registro.
- **URI:** Identificador Uniforme de Recursos
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **SHA:** (Secure Hash Algorithm) Algoritmo de Hash Seguro.
- **RFC¹:** (Request For Comments) Requerimiento de Comentarios.



¹ Es un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **HSM²:** (Hardware Security Module) Módulo de Hardware de Seguridad.
- **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
- **ADSIB:** Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- **ATT:** Autoridad de Regulación y Fiscalización de Transportes y Telecomunicaciones.
- **CP:** (Certificate Policy) Política de Certificación.
- **CPS:** (Certification Practice Statement) Declaración de Prácticas de Certificación.
- **TIC:** Tecnologías de Información y Comunicación.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.
- **OID³:** (Object Identifier) Identificador de Objeto.

Artículo 4 (Definiciones).-

I. En lo referido a los campos básicos de los certificados digitales en base al RFC 5280, se deberán tomar las siguientes definiciones y consideraciones:

- a) ***version (Versión):*** Se define la versión del formato de los certificados digitales (el valor del campo es 2 para todos los tipos de certificados, dicho valor corresponde al estándar X.509 v3).
- b) ***serialNumber (Número de serie del Certificado):*** Este campo es un entero, no secuencial asignado por la ECA. Cada certificado emitido por la ECA debe tener un número de serie único hasta de 20 octetos (bytes) de longitud.
- c) ***signatureAlgorithm (Algoritmo de firmas):*** Es el campo que utiliza el certificado para identificar el algoritmo para firmar un documento, debe ser acompañado por su respectiva OID.
- d) ***issuer (Nombre del emisor):*** Este campo identifica la ECA emisora que ha firmado y emitido el certificado.
- e) ***validity (Periodo de validez):*** Este campo indica el periodo de tiempo durante el cual el certificado es válido. Los campos notbefore y notafter deben estar en el formato de fecha y hora YYMMDDHHMMSSZ, formato UTC Time.
- f) ***subject (Nombre suscriptor):*** Este campo identifica al propietario de la clave pública del certificado. La existencia de algunos atributos depende del tipo de certificado (Anexo 1).
- g) ***subjectPublicKey (Información de la clave pública del suscriptor):*** Este campo contiene la clave pública y el identificador del algoritmo con el que se ha codificado la clave.

II. En lo referido a las extensiones de los certificados digitales en base al RFC 5280, se deberán tomar las siguientes definiciones y consideraciones:

- a) ***basicConstraints (Restricciones Básicas):*** Este campo es crítico para todos los tipos de certificados, sirve para determinar si el certificado pertenece a una EC.

² El HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege claves criptográficas.

³ OID es una nomenclatura que permite identificar objetos dentro de la estructura de la PKI Bolivia, existen valores predefinidos de los algoritmos.



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

- b) keyUsage: (Uso de la clave): Esta campo es crítico para todos los tipos de certificados, debe describir los usos permitidos de la clave pública mediante la habilitación o deshabilitación de los siguientes campos:
- digitalSignature: Utilizado para verificar la firma digital en procesos de autenticación de entidades, autenticación de datos y de integridad.
 - nonRepudiation: Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
 - keyEncipherment: Para cifrar claves u otra información de seguridad, por ejemplo, para el transporte de claves.
 - dataEncipherment: Para cifrar datos de usuario, pero no las claves u otra información de seguridad.
 - keyAgreement: indica que se utiliza la clave pública para realizar un acuerdo de claves.
 - keyCertSign: indica que se utiliza la clave pública para verificar las firmas en los certificados de clave pública.
 - cRLSign: indica que se utiliza la clave pública para la verificación de firmas en las listas de revocación de certificados.
 - encipherOnly: Utilizada solo para cifrar los datos durante la realización de un acuerdo de claves.
 - decipherOnly: Utilizada solo para descifrar los datos durante la realización de un acuerdo de claves.

Los valores de los atributos dependen del tipo del certificado (Anexo 1).

- c) cRLDistributionPoint (Puntos de Distribución de la CRL): Este campo debe especificar donde se almacenara la CRL en una dirección en formato URI.
- d) certificatePolicies (Política de Certificación): Esta campo debe especificar donde se almacenara las CP que aplican al certificado emitido en formato URI.
- e) authorityKeyIdentifier (Identificador de la clave de la Autoridad Certificante): Este campo es usado para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de confianza.
- f) subjectKeyIdentifier (Identificador de la Clave del Suscriptor): Este campo proporciona un medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.
- g) authorityInformationAccess (Información de Acceso a la Autoridad Certificante): Este campo debe identificar la dirección en formato URI de acceso al OCSP.
- h) extendedKeyUsage (Uso de claves Extendido).- Este campo debe describir el uso extendido permitido de la clave pública mediante la habilitación o deshabilitación del siguiente campo:
 - clientAuth: Utilizado para la autenticación de SSL/TLS en modo cliente.
 - serverAuth: Utilizado para la autenticación de SSL/TLS en modo Web Server.
 - codeSigning: Utilizado para la firma de código.
 - emailProtection: Protección E-mail (S/MIME).



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

Capítulo II Entidades Certificadoras y Certificados Digitales

Sección 1.- Tipos y Funciones de los Certificados Digitales, Formatos de los Certificados Digitales

Artículo 5 (Tipos y funciones de los Certificados Digitales).-

I. La ECR dispondrá la emisión de los siguientes Certificados:

- a) Certificado de la ECR: Certificado digital auto firmado que identifica a la ECR, como la base de confianza en la ruta de certificación de la Infraestructura de clave pública para Bolivia y tiene una duración máxima de 20 años.
- b) Certificados para las ECA públicas y privadas: Certificado digital que se otorga como parte de la autorización para la prestación de servicios de Certificación Digital a las EC públicas y privadas y tiene una duración máxima de 10 años.

II. Los tipos de certificados digitales que podrán emitir las ECA, de acuerdo a su uso según el Reglamento para el desarrollo de las TIC aprobado por el Decreto Supremo N° 1793 y conforme a estándares internacionales son los siguientes:

- a) Certificado de Persona Natural: Documento digital que pertenece y contiene los datos de una persona natural y tiene una duración máxima de 1 año.
- b) Certificado de Persona Jurídica: Documento digital que pertenece y contiene los datos de una persona jurídica que figura en representación de una entidad pública o privada y tiene una duración máxima de 2 años.
- c) Certificado de Cargo Público: Documento digital que pertenece y contiene los datos de un servidor público del Estado Plurinacional de Bolivia y tiene una duración máxima de 2 años.

III. Tipos de certificados digitales adicionales deberán ser redactados en un formato propuesto de acuerdo al estándar X 509 v3 por las ECA que así lo requieran a la ECR, quien evaluará su incorporación a la PKI Boliviana.

Artículo 6 (Formatos de los Certificados Digitales).-

El formato para los tipos de Certificados Digitales que pueden emitir tanto la ECR como las ECA pública y privadas están basados en el RFC 5280 y están definidos en el Anexo 1 del presente estándar, por motivos de interoperabilidad, aquello que no esté fijado se deberá ajustar al RFC 5280.

Capítulo III Requisitos y Condiciones de Autorización para Entidades Certificadoras y Agencias de Registro

Artículo 7 (Requisitos y Condiciones para Entidades Certificadoras).-

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, en uso de sus atribuciones, otorgará la autorización para la prestación de servicios de Firma y Certificación Digital con vigencia de 5 años para Entidades Certificadoras Públicas y Privadas, según se establecen el art. 47 de Reglamento a la Ley N° 164, de 08 de agosto de 2011, para el Desarrollo de Tecnologías de Información



Línea Gratuita de Protección al Usuario
800-10-6000 8 de 34
www.att.gob.bo

Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

y Comunicación, previo cumplimiento de los siguientes requisitos y condiciones:

Sección 1.- Requisitos Legales y Económicos para la Entidad Certificadora Pública.

Artículo 8 (Requisitos legales).-

Los requisitos legales para la prestación de servicios de Firma y Certificación Digital son los siguientes:

- I. Nota o memorial de solicitud de acreditación con la siguiente información:
 - a) Nombre, dirección, teléfono(s), correo electrónico y si corresponde, fax, casilla postal del solicitante.
- II. Norma jurídica de creación y disposición de nombramiento del Titular como documentos que certifique la naturaleza del solicitante.
- III. Fotocopia legalizada del Documento de Identidad del Titular designado.
- IV. Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributaria).
- V. Declaración Jurada de la persona representante legal de no estar comprendido(a) dentro de las prohibiciones del artículo 39 de la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- VI. Certificado de antecedentes penales judiciales del Representante Legal expedido por la autoridad competente.
- VII. En caso de cambio de autoridades por parte de la Entidad Certificadora Pública, la información del representante deberá ser actualizada en un plazo máximo de 5 días y durante ese periodo no podrá emitir certificados ni llaves.

Artículo 9 (Requisitos económicos).-

Los requisitos económicos para la prestación de servicios de Firma y Certificación Digital son los siguientes:

- I. Estados Financieros.
- II. Balance de apertura o balance general correspondiente al último ejercicio anual presentado al Servicio de Impuestos Nacionales.
- III. Plan de negocio proyectado para un período de cinco (5) años, vinculados a la licencia solicitada que contenga además el programa de inversiones generales a efectuar.
- IV. Boleta de garantía de cumplimiento de contrato, por el siete por ciento (7%) de sus ingresos brutos sobre sus proyecciones para el primer año, que respalte su actividad durante la vigencia de la autorización para la prestación de servicios de certificación digital de acuerdo al artículo 45 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
- V. La EC deberá pagar por adelantado a la ATT el uno por ciento (1%) de sus ingresos brutos de operación del servicio de certificación digital, como tasa de fiscalización y regulación. en base a la proyección de sus ingresos brutos de acuerdo al artículo 38 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793. Presentación de su estructura tarifaria a la ATT para su aprobación y registro de acuerdo al artículo 42 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
- VI.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****Sección 2.- Requisitos Legales y Económicos para Entidades Certificadoras Privadas.****Artículo 10 (Requisitos legales).-**

Los requisitos legales para la prestación de servicios de Firma y Certificación Digital son los siguientes:

- I. Nota o memorial de solicitud de acreditación con la siguiente información:
 - a) Nombre, dirección, teléfono(s), correo electrónico y si corresponde, fax, casilla postal del solicitante.
- II. Documentos que certifiquen la naturaleza del solicitante como empresas privadas, mixtas o con participación estatal mayoritaria: Certificado de matrícula de inscripción actualizada otorgada por registro de comercio y escritura de Constitución Social de la empresa (incluyendo estatutos y escrituras modificatorias posteriores) registrada en el registro de comercio.
- III. Fotocopia legalizada del Documento de Identidad del Representante Legal.
- IV. Poder Especial que acredite la personería del representante legal que especifique las facultades de apersonamiento y para realizar trámites ante la ATT.
- V. Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributaria Nómica y fotocopias o documentos de identidad de todos los miembros de juntas o consejos directivos o socios de personas jurídicas.
- VI. Declaración Jurada de personas naturales o jurídicas, de todos los miembros de juntas o consejos directivos de no estar comprendidos dentro de las prohibiciones del artículo 39 de la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- VII. Certificado de antecedentes penales judiciales del propietario o Representante Legal expedido por la autoridad competente.
- VIII. En caso de cambio del representante legal por parte de la Entidad Certificadora Privada, la información del representante deberá ser actualizada en un plazo máximo de 5 días y durante ese periodo no podrá emitir certificados ni llaves.

Artículo 11 (Requisitos económicos).-

Los requisitos económicos para la prestación de servicios de Firma y Certificación Digital son los siguientes:

- I. Estados Financieros.
- II. Certificado de Solvencia Fiscal otorgado por la Contraloría General del Estado.
- III. Balance de apertura o balance general correspondiente al último ejercicio anual presentado al Servicio de Impuestos Nacionales.
- IV. Plan de negocio proyectado para un período de cinco (5) años, vinculados a la licencia solicitada que contenga además el programa de inversiones generales a efectuar.
- V. Fuentes de financiamiento, o demostrar que cuenta con los recursos necesarios para implementar el proyecto técnico presentado.
- VI. La entidad certificadora deberá rendir una caución por medio de una póliza de seguros expedida por una Entidad de Seguros, debidamente establecida en el Estado Plurinacional de Bolivia. El monto será fijado por la ATT anualmente.
- VII. Boleta de garantía de cumplimiento de contrato, por el siete por ciento (7%) de sus ingresos brutos sobre sus proyecciones para el primer año, que respalte su actividad durante la vigencia de la autorización para la prestación de servicios de certificación digital de acuerdo al artículo 45 del



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.

- VIII. La ECA deberá pagar por adelantado a la ATT el uno por ciento (1%) de sus ingresos brutos de operación del servicio de certificación digital, como tasa de fiscalización y regulación, en base a la proyección de sus ingresos brutos de acuerdo al artículo 38 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
- IX. Presentación de su estructura tarifaria a la ATT para su aprobación y registro de acuerdo al artículo 42 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.

Sección 3.- Requisitos Técnicos para Entidades Certificadoras Pública y Privadas y Agencias de Registro.

Artículo 12 (Requisitos técnicos para las Entidades Certificadoras).-

Los requisitos técnicos que deben presentar para la prestación de servicios de Certificación Digital son los siguientes:

- I. Descripción de servicios prestados incluyendo duración y alcance de los mismos.
- II. Políticas de Certificación (CP) debe ser presentado a la ATT para su aprobación considerando mínimamente:
 - a. El RFC 3647 o el contenido mínimo del Anexo 4.
 - b. Un Plan de Cese de Actividades de la ECA de acuerdo al artículo 51 del Reglamento para el Desarrollo de las TIC, Decreto Supremo N° 1793.
 - c. Se debe considerar la protección de datos personales garantizando mínimamente las consideraciones del artículo 56 del Reglamento para el Desarrollo de las TIC, Decreto Supremo N° 1793.
- III. Declaración de Prácticas de Certificación (CPS) (De acuerdo al RFC 3647 o el contenido mínimo del Anexo 5) debe ser presentado a la ATT para su aprobación.
- IV. Infraestructura tecnológica: describir detalladamente la plataforma tecnológica incluyendo un detalle pormenorizado de hardware, software, dispositivos de comunicación y seguridad con los que cuenta, sus características y funcionalidad.
- V. Planes y procedimientos para recuperación ante desastres de la ECA (Certificación ISO 22301 o el contenido mínimo del Anexo 6).
- VI. Planes y procedimientos de seguridad y evaluación de riesgos de la EC (Certificación ISO 27001 o el contenido mínimo de los Anexos 7 y 8).
- VII. Procedimiento y 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 (Certificación ISO 30300 o el contenido mínimo del Anexo 9).
- VIII. La Entidad Certificadora deberá contar un sistema de información permanente y actualizada de acceso libre vía web con la siguiente información:
 - a. Procedimientos de certificación digital.
 - b. Condiciones de validación, renovación, baja, suspensión, tarifas y usos del certificado digital.
 - c. Certificados Digitales suspendidos y revocados con los siguientes datos:
 - Número único de serie.
 - Fecha de emisión.
 - Vigencia y restricciones aplicables.



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

- d. Procedimientos de reclamos.
- e. Tarifas y servicios aprobados por la ATT.
- f. Domicilio legal, teléfonos y correo electrónico de contacto.
- IX. Modelo de Contrato tipo con suscriptores (Anexo 2).
- X. Términos y condiciones de servicio con los suscriptores (Anexo 3).
- XI. Contrato de servicios de tercerización (Si corresponde).

Artículo 13 (Requisitos para Agencias de Registro y Servicios terciarizados).-

Las Entidades Certificadoras Autorizadas deberán establecer los requisitos y condiciones que deben cumplir las Agencias de Registro, basándose en lo establecido en los requisitos legales, económicos y técnicos del presente estándar según corresponda a una Agencia de Registro de una ECA Pública o una Agencia de Registro de una ECA Privada.

Los servicios terciarizados deberán cumplir las mismas condiciones de funcionamiento que la ECA que la contrata, asegurando la integridad para la conservación de la información contenida en mensajes electrónicos de datos o documentos digitales. (De acuerdo al artículo 32 del Reglamento para el Desarrollo de las TIC aprobado por el D.S. N° 1793).

Artículo 14 (Renovación de la Autorización).-

La ECA deberá solicitar la renovación de su autorización de servicios de Firma y Certificación Digital, mínimamente seis meses antes de que su contrato finalice con la ATT y deberá cumplir los requisitos y condiciones establecidos en el presente estándar.

La ECA debe manejar el periodo transitorio durante el cual contará con dos certificados (el nuevo y el anterior) y deberá cuidar las fechas de los certificados que emitirá.

La ECA que no vaya a renovar su autorización, deberá brindar soporte a sus servicios hasta que expire el tiempo de validez del último certificado emitido, una vez que haya finalizado su autorización no podrá emitir más certificados.

Sección 4.- Requisitos Mínimos para la Obtención de un Certificado Digital.

Se debe acreditar la identidad del titular del certificado, por lo que la solicitud es personal y de manera presencial, de acuerdo al propósito del certificado pueden existir más requisitos. Se debe informar al signatario respecto a los niveles de seguridad que se tienen en el Anexo 10 del presente estándar.

Artículo 15 (Vigencia y requisitos mínimos para personas naturales).-

- I. Un certificado digital para personas naturales tendrá una vigencia máxima de 1 año.
- II. Fotocopia simple de carnet de identidad o carnet de extranjero del solicitante.
- III. Fotocopia de la última factura de pago de luz, agua o teléfono que permita verificar la dirección actual del solicitante.
- IV. La documentación debe ser validada por la Entidad de Certificación / Agencia de Registro con la presentación de la documentación original por parte del solicitante.
- V. Dispositivo que permita firmar un documento al signatario, donde sean almacenados y custodiados el certificado digital y su clave privada (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2. (inciso g art. 33 del D.S. 1793).



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

Artículo 16 (Vigencia y requisitos mínimos para personas Jurídicas).-

- I. Un certificado digital para personas jurídicas tendrá una vigencia máxima de 2 años.
- II. Fotocopia simple del 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.
- III. Fotocopia simple de carnet de identidad o carnet de extranjero del representante legal de la empresa u organización solicitante.
- IV. Fotocopia del nombramiento o certificado laboral del solicitante firmado por el Representante Legal de la empresa u organización solicitante.
- V. Autorización original de la persona jurídica solicitante firmada por el Representante Legal.
- VI. La documentación debe ser validada por la Entidad de Certificación / Agencia de Registro con la presentación de la documentación original por parte del solicitante.
- VII. En función al tipo de información que utiliza una organización las claves pública y privada podrán ser emitidas de acuerdo a los criterios de seguridad del Anexo 10 y de acuerdo a las siguiente recomendaciones:
 - a) Dispositivo que permita firmar un documento al signatario, donde sean almacenados y custodiados el certificado digital y su clave privada (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2. (inciso g art. 33 del D.S. 1793).
 - b) Software donde sea almacenado el certificado digital que permita firmar uno o varios documentos y que cumpla con sistemas de seguridad reconocidos internacionalmente, garantizando la confiabilidad del mismo. (inciso g art. 33 del D.S. 1793).

Artículo 17 (Vigencia y requisitos mínimos para Cargos Públicos).-

- I. Un certificado digital para cargos públicos tendrá una vigencia máxima de 2 años.
- II. Fotocopia simple de carnet de identidad o carnet de extranjero.
- III. Fotocopia del memorándum de designación firmado por el Representante de la Entidad.
- IV. Autorización del servidor público firmada por el Representante de la Entidad.
- V. La documentación debe ser validada por la Entidad de Certificación / Agencia de Registro con la presentación de la documentación original por parte del solicitante.
- VI. Dispositivo que permita firmar un documento al signatario, donde sean almacenados y custodiados el certificado digital y su clave privada (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2. (inciso g art. 33 del D.S. 1793).

Capítulo IV Otros Aspectos

Artículo 18 (Incumplimiento).-

El incumplimiento a cualquier disposición del mismo implica una infracción contra las atribuciones de la Autoridad Reguladora, de acuerdo a los alcances del inciso c) del parágrafo I del Reglamento de Sanciones vigente.

Artículo 19 (Modificaciones al reglamento).-

El presente estándar está sujeto a modificaciones de acuerdo al artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo N° 1793.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 1: FORMATO DE LOS CERTIFICADOS DIGITALES Y DE LA LISTA DE CERTIFICADOS REVOCADOS.****I. FORMATO DE LOS CERTIFICADOS DIGITALES.**

El formato de los Tipos de Certificados Digitales debe seguir los lineamientos del Estándar ITU X.509 “Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks” en todos los aspectos relativos al formato, codificación, contenidos e interpretación. Se adhiere en consiguiente al RFC 5280.

1. Formato para el Certificado Digital de la Entidad Certificadora Raíz.

i. El formato para el Certificado Digital de la ECR tendrá los siguientes atributos y contenidos:

- Versión (version): el valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECR, valor hasta de 20 octetos.
- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA)
- Nombre del Emisor (issuer): CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
- Periodo de validez (validity): Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
- Información de la clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 4096 bits.

ii. Las extensiones del Certificado Digital de la ECR serán las siguientes:

- Identificador de la clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey.
- Uso de Claves (keyUsage): digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
- Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
- Restricciones Básicas (basicConstraints): CA = TRUE, pathLenConstraint = “1”.
- Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).

**2. Formato para el Certificado Digital de una ECA.**

i. El formato para el Certificado Digital de una ECA tendrá los siguientes atributos y contenidos:

- 
- 
- 
- Versión (version): el valor del campo es 2.
 - Número de Serie (serialNumber): Número asignado por la ECR.
 - Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
 - Nombre del Emisor (issuer): CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
 - Periodo de validez (validity): Fecha de emisión del Certificado, Fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time).
 - Nombre suscriptor (subject): CN = “Entidad Certificadora” y el nombre de la ECA; O = Razón social de la ECA; C = BO de acuerdo a ISO3166.

**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

g) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 4096 bits.

ii. Las extensiones del Certificado Digital de una ECA serán las siguientes:

- a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier): Identificador de la clave pública de la ECR.
- b) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función HASH (SHA1) del atributo subjectPublicKey.
- c) Uso de Claves (keyUsage): digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
- d) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
- e) Restricciones Básicas (basicConstraints): CA = TRUE, pathLenConstraint = "0".
- f) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).
- g) Información de Acceso de la ECA (authorityInformationAccess): URI: (.crt).

3. Formato para el Certificado Digital de una Persona Natural o Física.

i. El formato para el Certificado Digital de una Persona Natural o Física tendrá los siguientes atributos y contenidos:

- a) Versión (version): El valor del campo es 2.
- b) Número de Serie (serialNumber): Número asignado por la ECA.
- c) Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
- d) Nombre del Emisor (issuer): CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón social de la ECA; C = BO de acuerdo a ISO3166.
- e) Período de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time).
- f) Nombre suscriptor (subject): CN = Nombre completo de la persona natural; Country (C) = BO de acuerdo a ISO3166; serialNumber: Tipo, nro. de documento y el lugar de emisión.
- g) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

ii. Las extensiones del Certificado Digital de una Persona Natural o Física serán las siguientes:

- a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier): Valor de la Extensión subjectKeyIdentifier del certificado de la ECA emisora.
- b) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey.
- c) Uso de Claves (keyUsage): digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1, keyAgreement = 0, keyCertSign = 0, cRLSign = 0, encipherOnly = 0, decipherOnly = 0.
- d) Uso de Claves Extendido (Extended Key Usage): clientAuth, EmailProtection, codeSigning.
- e) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
- f) Restricciones Básicas (basicConstraints): CA = FALSE.
- g) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).
- h) Información de Acceso de la ECA (authorityInformationAccess): URI: (.crt).
- h) Nombre Alternativo del Suscriptor (subjectAlternativeName): E = Correo electrónico del suscriptor.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****4. Formato para el Certificado Digital de una Persona Jurídica.**

i. El formato para el Certificado Digital de una Persona Jurídica tendrá los siguientes atributos y contenidos:

- 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 = BO de acuerdo a ISO3166.
- 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 Organizativa a la que depende; Country (C) = BO de acuerdo a ISO3166; serialNumber = Tipo, numero documento de identidad y el lugar de emisión.
- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

ii. Las extensiones del Certificado Digital de una Persona Jurídica serán las siguientes:

- 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, 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).
- Restricciones Básicas (basicConstraints): CA = FALSE.
- 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

** La persona jurídica podrá tener varias representaciones legales de acuerdo a las atribuciones asignadas.

5. Formato para el Certificado Digital de Cargo Público.

i. El formato para el Certificado Digital de Cargo Público tendrá los siguientes atributos y contenidos:

- 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 = BO de acuerdo a ISO3166.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

- e) Período de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time).
 - h) Nombre suscriptor (subject): CN = Nombres y Apellidos del servidor público; O = Nombre de la institución pública a la que pertenece; OU = Unidad Organizativa de la que depende el funcionario público; title = Cargo del servidor público Country (C) = BO de acuerdo a ISO3166; serialNumber= Tipo, numero documento de identidad y el lugar de emisión.
 - f) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 2048 bits.
- ii. Las extensiones del Certificado Digital de Cargo Público serán las siguientes:
- a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier): Valor de la Extensión subjectKeyIdentifier del certificado de la ECA emisora.
 - b) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey.
 - c) Uso de Claves (keyUsage): digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 0, cRLSign = 0, encipherOnly = 0, decipherOnly = 0.
 - j) Uso de Claves Extendido (Extended Key Usage): clientAuth, EmailProtection, codeSigning.
 - i) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
 - d) Restricciones Básicas (basicConstraints): CA = FALSE.
 - i) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).
 - e) Información de Acceso de la ECA (authorityInformationAccess): URI: (.crt).
 - f) Nombre Alternativo del Suscriptor (subjectAlternativeName): E = Correo electrónico del suscriptor.

II. FORMATOS DE LAS LISTAS DE CERTIFICADOS DIGITALES REVOCADOS.

El formato de las Listas de Certificados Revocados debe seguir los lineamientos del Estándar ITU X.509 "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks" en todos los aspectos relativos al formato, codificación, contenidos e interpretación. Se adhiere en consiguiente al RFC 5280.

- i. El formato de las Listas de Certificados Revocados tendrá los siguientes contenidos y atributos mínimos:

- a) Versión (version): el valor del campo es 1 (corresponde a la versión 2 del estándar).
- b) Algoritmo de firma (signatureAlgorithm): Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Autorizada para firmar la Lista de Certificados Revocados.
- c) Nombre del Emisor (Issuer): CN = Nombre de la Entidad Certificadora Autorizada, O = Razón Social de la Entidad Certificadora Autorizada, C = BO de acuerdo al estándar ISO 3166
- d) Día y Hora de Vigencia (This Update): Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time).

Próxima actualización (Next Update): Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time).

Certificados Revocados (Revoked Certificates): contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas.

- ii. Las extensiones de la Lista de Certificados Revocados serán, como mínimo, las siguientes:



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

- a) Identificador de la Clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo SubjectPublicKey (clave pública correspondiente a la clave privada usada para firmar la Lista de Certificados Revocados).
- b) Número de Lista de Certificados Revocados (CRL Number): número entero de secuencia incremental para una CRL y una Entidad Certificadora Autorizada determinadas.
- c) Extensiones de un elemento de la Lista de Certificados Revocados.
- d) Código de motivo (Reason code): indica la razón de revocación de un elemento de la CRL
- e) Para los formatos y contenidos de todos los campos y extensiones no indicados expresamente en la presente sección, deberá seguirse los lineamientos del RFC 5280.
- f) En la extensión conocida como código de razón (o reasonCode) que identifica el motivo de la pérdida de vigencia del certificado, se habilitan como opciones las siguientes:
 - keyCompromise (1) – Compromiso de clave, utilizada para la revocación de un certificado de usuario final, indicando que se sabe o sospecha que la clave privada del suscriptor ha sido comprometida.
 - cACompromise (2) – Compromiso de clave de la entidad certificadora, utilizada para indicar que se sabe o sospecha que la clave privada de la entidad certificadora que lo emitió ha sido comprometida.
 - affiliationChanged (3) – Cambio de afiliación, indica que el nombre del suscriptor u otra información contenida en el certificado ha sufrido modificaciones
 - superseded (4) – sustituido, utilizado para indicar que el certificado revocado ha sido sustituido por otro certificado digital.
 - cessationOfOperation (5) – cesación de la operación, utilizado para indicar que el certificado ya no es necesario para el propósito para el cual fuera emitido
 - certificateHold (6) – retención de certificado, utilizado para reflejar el estado de suspensión de un certificado.
 - privilegeWithdrawn (9) – retiro de privilegio, indicando que se ha revocado el certificado en razón de que ha cesado la titularidad de un privilegio por parte que su suscriptor.
 - aACompromise (10) – compromiso de la Autoridad de Atributo, indicando que se sabe o sospecha que uno o varios aspectos de la Autoridad de Atributo han sido comprometidos.

III. OCSP “On line Certificate Status Protocol”

La adhesión en cuanto a definiciones, implementación y formatos, a los RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” y 6960 “X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol - OCSP”.

i. El requerimiento de inclusión de los siguientes datos en las consultas OCSP:

- a) Versión (version).
- b) Requerimiento de servicio (service request).
- c) Identificador del certificado bajo consulta (target certificate identifier).
- d) Extensiones que puedan incluirse en forma opcional (optionals extensions) para su procesamiento por quien responde.

Cuando se recibe una consulta OCSP, quien responde debe considerar al menos los siguientes aspectos:

- a) Que el formato de la consulta sea el apropiado.



Resolución Administrativa Regulatoria **ATT-DJ-RA TL LP 32/2015**

- b) Que quien responde sea una entidad autorizada para responder la consulta.
- c) Que la consulta contenga la información que necesita quien responde.
- d) Si estas condiciones son verificadas, se devuelve una respuesta. De lo contrario, si alguna de estas condiciones no se cumpliera, se deberá emitir un mensaje de error.

- ii. Cuando se emite una respuesta OCSP, se sugiere requerir que se consideren los siguientes datos:
 - a) Versión.
 - b) Identificador de la Entidad Certificante Autorizada o de la entidad habilitada que emite la respuesta.
 - c) Fecha y hora correspondiente a la generación de la respuesta.
 - d) Respuesta sobre al estado del certificado.
 - e) Extensiones opcionales.
 - f) Identificador de objeto (OID) del algoritmo de firma.
 - g) Firma de la respuesta.

- iii. Una respuesta a una consulta OCSP debería contener:
 - a) Identificador del certificado.
 - b) Valor correspondiente al estado del certificado, pudiendo este ser de acuerdo al RFC 5280.
 - c) Válido (good), respuesta positiva a la consulta lo que implica que no existe un certificado digital revocado con el número de serie contenido en la consulta.
 - d) Revocado (revoked), es decir certificado revocado.
 - e) Desconocido (unknown), es decir sin reconocer el número de serie del certificado.
 - f) Período de validez de la respuesta.
 - g) Extensiones opcionales.

Las respuestas OCSP deben estar firmadas digitalmente por la Entidad Certificadora Autorizada correspondiente o por una entidad habilitada a tal efecto en el marco de la Infraestructura de Clave Pública de Bolivia.

El certificado utilizado para la verificación de una respuesta OCSP debe contener en el campo “extendedKeyUsage” con el valor “id-kp_OCSPSigning”, cuyo OID es 1.3.6.1.5.5.7.3.9.

Dicho certificado deberá ser emitido dentro de la Infraestructura de Claves Públicas de Bolivia, con una ruta de certificación que finalice en el certificado de la Entidad Certificadora Raíz.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 2: MODELO DE CONTRATO TIPO DE LAS ENTIDADES CERTIFICADORAS CON SUS SIGNATARIOS.****MODELO DE CONTRATO DE ADHESIÓN PARA LA PROVISIÓN DE SERVICIOS DE FIRMA Y CERTIFICACION DIGITAL**

Conste por el tenor del presente Documento Privado, que los suscriptores acuerdan celebrar un Contrato para la PROVISIÓN DE SERVICIOS DE FIRMA Y CERTIFICACION DIGITAL, que con el reconocimiento de firmas y rubricas surtirá los mismos efectos de documento público, sujeto a las siguientes cláusulas:

PRIMERA (PARTES CONTRATANTES).- Intervienen en la suscripción del presente Contrato:

1.1.- EMPRESA/ECA/AGENCIA DE REGISTRO representada (o) legalmente por.....por el Sr.(a) en virtud al Poder Especial N°/..... de fecha de.....del otorgado mediante Notaría de Fe Pública N°que para efectos de éste Contrato se denominará

(LLENAR EN CASO DE PERSONA NATURAL)

1.2.- El/la Señor/ra/ita . , C.I. N° , que en lo sucesivo se denominará SIGNATARIO (A), cuyos datos personales se detallan en el Anexo de Solicitud de Provisión de Servicios, mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

(LLENAR EN CASO DE PERSONA JURIDICA)

1.3.- La Empresa legalmente representada (o) por el Sr. (a)....., en virtud al Poder Especial/..... de fechade.....del....., otorgado ante la Notaría de Fe Pública N° a cargo del Dr.(a)con C.I. con Matricula N°.....con NIT N°con Domicilio legalque en lo sucesivo se denominará, cuyos datos se detallan en el Anexo de Solicitud de Provisión de Servicios mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

SEGUNDA (ANTECEDENTES).- Descripción del (los) servicio (s) a prestar, usos del certificado y limitaciones.

TERCERA (OBJETO DEL CONTRATO)- Describir el objeto del Contrato del servicio y la no transferibilidad de las claves y el certificado digital.

CUARTA (TÉRMINOS Y CONDICIONES).- Establecer que el servicio a contratar se someterá a sus términos y condiciones, señalando que deben formar parte integrante, indivisible, e inseparable del presente Contrato para todos los efectos legales (debiendo realizar un breve resumen).

QUINTA (PLAZO DEL CONTRATO. VIGENCIA Y PRORROGA).- Establecer plazo, vigencia y prórroga y/o renovación del Contrato de acuerdo a la normativa establecida por el ente regulador.

SEXTA (PLAZOS PARA LA ENTREGA. HABILITACIÓN, SUSPENSION, REVOCACION Y VIGENCIA DEL SERVICIO).- Establecer y describir los plazos, costos y requisitos señalado en los términos y condiciones del servicio a contratar.

SÉPTIMA (TITULARIDAD).- Describir la titularidad del uso del servicio a contratar.

OCTAVA (ESTRUCTURA TARIFARIA).- Establecer estructura tarifaria según lo señalado en los términos y condiciones del servicio a contratar.

NOVENA (FACTURACIÓN Y COBRANZA).- Establece los plazos señalados en los términos y condiciones.

DÉCIMA (DERECHOS Y OBLIGACIONES).- Describir derechos y obligaciones según señala en los términos y condiciones.

- (DE LA USUARIA Y/O USUARIO)

- (DE LA ECA O AGENCIA DE REGISTRO)

DÉCIMA SEGUNDA (EXENCIOS DE RESPONSABILIDAD).- Descripción para ECA/ AGENCIA



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

DE REGISTRO, en consideración a los marcos legales aplicables, sobre el servicio, la responsabilidad civil y penal u otro que se considere pertinente. Causales y condiciones bajo las cuales deba efectuarse la Revocatoria.

DÉCIMA TERCERA (ATENCIÓN DE RECLAMOS).- Describir los procedimiento y sus plazos de acuerdo a la normativa regulatoria aplicable.

DÉCIMA CUARTA (SERVICIOS DE INFORMACIÓN Y ASISTENCIA).- Establecer, y detallar los horarios días de atención, teléfono(s) y dirección del mismo.

DÉCIMA QUINTA (DECLARACIÓN EXPRESA).- Relativo a la voluntad de las partes y considerando que no media presión para la firma del presente Contrato.

DÉCIMA SEXTA (INVIOLABILIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE LA USUARIA O USUARIO).- Establecer la manera de proteger la información proporcionada por la usuaria o usuario a la ECA.

DÉCIMA SÉPTIMA (RESOLUCIÓN Y RESCISIÓN DEL CONTRATO).- Describe, establece las formas y atribuciones de la disolución del Contrato.

DÉCIMA OCTAVA (INTEGRIDAD DEL CONTRATO).- Establece una breve descripción de los documentos que forman parte del presente Contrato, como formularios, documentos requeridos por la Entidad Certificadora / Agencia de Registro, los términos y condiciones del servicio ofrecido, entre otros, los mismos que deberán ser entregados al momento de la suscripción del contrato.

DÉCIMA NOVENA (CLÁUSULA DE INTERPRETACIÓN).- En caso de duda sobre la interpretación del presente Contrato, se aplicará lo más favorable al usuario o usuaria.

VIGÉSIMA (ACEPTACIÓN).- Describir la conformidad de la usuaria o usuario y la aceptación por parte de la Entidad Certificadora / Agencia de Registro, debiendo entregarse copia del presente Contrato al usuario o usuaria en el momento de la suscripción del contrato.





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

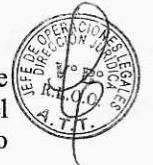
Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

ANEXO 3: CONTENIDO MÍNIMO DE LOS TÉRMINOS Y CONDICIONES DE LAS ENTIDADES CERTIFICADORAS.

TÉRMINOS Y CONDICIONES PARA LA PROVISIÓN DE SERVICIOS DE FIRMA Y CERTIFICADO DIGITAL

Con carácter previo a la celebración de los términos y condiciones entre la Entidad Certificadora / Agencia de Registro y el signatario, para la provisión de servicios de firma digital y certificados digitales deberá tenerse en cuenta la normativa que regula esta materia, prevista tanto en la Ley N° 164/2011 como en el Decreto Supremo N° 1793 y normas complementarias.

1. DESCRIPCIÓN DEL SERVICIO Y ASPECTOS ASOCIADOS: La ECA / Agencia de Registro deberá detallar de manera exhaustiva la descripción de los objetivos y servicios a brindar.
2. MODALIDADES DE PRESTACIÓN DEL SERVICIO: Describir por nombre de modalidad los servicios involucrados en el contrato.
3. REQUISITOS TÉCNICOS NECESARIOS PARA ACCEDER AL SERVICIO: La ECA / Agencia de Registro proveedora de servicios debe establecer cuáles son los requisitos mínimos necesarios para acceder al servicio. Asimismo, debe informar a los usuarios de las variables técnicas que pueden afectar la prestación del servicio y las limitaciones de éste.
4. HABILITACIÓN Y PLAZO PARA LA PROVISIÓN DEL SERVICIO: La Entidad Certificante / Agencia de Registro debe establecer plazos para la habilitación del servicio.
5. TARIFAS: En este caso la Entidad Certificadora deberán establecer las tarifas considerando criterios sustentados y orientados en costos del servicio de certificación digital, previa presentación y aprobación por parte de la ATT según lo establecido por el artículo 42 del Reglamento para el Desarrollo de las TIC aprobado mediante D.S. 1793 y publicadas en medios de comunicación escrita y en su página web.
6. OBTENCION, SUSPENSION, REVOCACION, VIGENCIA Y CONSERVACION DEL CERTIFICADO DIGITAL: Para la elaboración de este punto la ECA de servicios deberá listar y regirse a lo establecido por los artículos 28, 29, 30, 31, y 32 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793.
7. DERECHOS Y OBLIGACIONES DEL TITULAR DEL CERTIFICADO DIGITAL: Para la elaboración de este punto la ECA de servicios deberá listar y regirse a lo establecido por el artículo 54 y artículo 55 de la ley N° 164, y los artículos 52, 53, 54 y 55 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793.
8. DERECHOS Y OBLIGACIONES DE LA ECA O AGENCIA DE REGISTRO: Para la elaboración de este punto la Entidad Certificante / Agencia de Registro deberá listar y regirse a lo establecido por el artículo 58 y artículo 59 de la ley N° 164, y los artículos 43 al 46 y 56 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793
9. DERECHOS Y OBLIGACIONES DE LA ECA, AGENCIA DE REGISTRO Y ANTE TERCEROS QUE CONFIAN: Para la elaboración de este punto el operador o proveedor de servicios deberá listar y regirse a lo establecido en el artículo 44 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793.

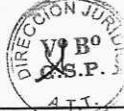


**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

10. ATENCIÓN DE CONSULTAS, RECLAMACIONES Y EMERGENCIAS Y/O SERVICIOS DE INFORMACIÓN Y ASISTENCIA: Para la elaboración de este punto la ECA de servicios debe regirse a lo establecido en el Reglamento de la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial aprobado por D.S. 27172. El contratante tiene derecho a recibir por parte de la Entidad Certificadora / Agencia de Registro, a través de la Oficina de Atención del Consumidor ODECO, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación del servicio.

13. MEDIDAS PARA SALVAGUARDAR LA INVOLABILIDAD DE LAS TELECOMUNICACIONES Y PROTECCIÓN DE LA INFORMACIÓN: Para la elaboración de este punto la Entidad Certificante / Agencia de Registro de servicios debe regirse a lo establecido por el artículo 56 de la ley N° 164 que establece la inviolabilidad y secreto de las comunicaciones.

14. CAMBIO O MODIFICACIONES EN LA LEY O REGLAMENTOS DE TELECOMUNICACIONES: Los términos y condiciones deben estar enmarcados en la Ley 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.



Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

ANEXO 4: CONTENIDO MÍNIMO DE LAS POLÍTICAS DE CERTIFICACIÓN PARA UNA ECA.

POLÍTICAS DE CERTIFICACIÓN

1. Introducción
 - 1.1. Descripción general.
Descripción del servicio, descripción y propósito del certificado, descripción de la ECA.
 - 1.2. Identificación y nombre del documento.
Identificación de la Política de Certificación, nombre, versión fecha de elaboración, fecha de actualización, sitio web de consulta.
 - 1.3. Participantes de la PKI Bolivia.
Descripción breve de la jerarquía nacional de la PKI Bolivia y de cada uno de sus componentes.
 - 1.4. Uso de los certificados.
Descripción de los siguientes usos de acuerdo al D.S. 1793, Reglamento para el Desarrollo de las TIC: Función del certificado digital, Características del certificado digital, Usos Permitidos de los Certificados, Restricciones en el Uso de los Certificados.
 - 1.5. Administración de la Política de Certificación.
Responsabilidad de la administración de la Política de Certificación.
 - 1.6. Definiciones y abreviaturas.
2. Responsabilidad del repositorio (CRL) y su publicación.
3. Identificación y Autenticación.
Formato del Nombre Distinguido, validación de la identidad inicial, identificación y autenticación para solicitudes de revocación.
4. Requerimientos Operativos del Ciclo de Vida de los Certificados.
Solicitud del certificado, procesamiento de solicitud del certificado, emisión del certificado, aceptación del certificado, generación del par de claves y uso del certificado, renovación del certificado, reemisión de claves del certificado, suspensión y reemisión del certificado, servicios de estado de certificados, fin de la suscripción, depósito de las claves y recuperación.
5. Controles operacionales o de gestión.
Controles de seguridad física, controles procedimentales, controles de seguridad del personal, controles para registros de auditoría, archivo de registros, cambio de clave, cambio de claves del certificado, procedimientos para recuperación de desastres, procedimientos para concluir las operaciones de la ECA.
6. Controles de Seguridad Técnica.
Instalación y generación del par de claves, protección criptográfica de la clave privada, controles, otros aspectos de la gestión del par de claves.
Datos de activación, controles de seguridad informática, controles de seguridad sobre el ciclo de vida de los sistemas, seguridad de la red, sincronización horaria.
7. Perfiles de Certificado, CRL y OCSP.
Perfil de certificado del tipo de certificado, perfil de la CRL de las ECRB y de la ECA y perfil del OCSP si corresponde.
Administración Documental.
Procedimiento para cambio de especificaciones, procedimientos de Publicación y Notificación.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 5: CONTENIDO MÍNIMO DEL DOCUMENTO DE DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN DE LAS ENTIDADES CERTIFICADORAS.****DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN**

1. Introducción.
 - 1.1 Presentación.
 - 1.2 Identificación y nombre del documento.
 - 1.3 Participantes de la PKI Bolivia, Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, Entidad de Certificación, Agencia de Registro, Signatarios, terceros aceptantes.
 - 1.4 Uso de los certificados.

Usos típicos, usos prohibidos, fiabilidad de la firma digital a lo largo del tiempo.
 - 1.5 Administración de la Declaración de Prácticas, procedimiento de aprobación.
 - 1.6 Definiciones y abreviaturas.
2. Publicación de información y del repositorio CRL de certificados.
 - Repositorio CRL.
 - Publicación.
 - Frecuencia de actualización.
 - Controles de acceso al repositorio CRL de certificados.
3. Identificación y Autenticación de los titulares de los certificados.
 - I.1. Registro de nombres.

Tipos de nombres, significado de los nombres, interpretación de formatos de nombres, unicidad de nombres resolución de conflictos relativos a nombres.
 - I.2. Validación de la identidad inicial.

Métodos de prueba de posesión de la clave privada, autenticación de la identidad de una organización, autenticación de la identidad de un individuo.
 - I.3. Identificación y autenticación de las solicitudes de renovación de clave.

Identificación y autenticación de las solicitudes de renovación rutinarias, de las solicitudes de renovación clave.
4. Ciclo de Vida de los Certificados.

Solicitud de Certificado, tramitación de solicitud de certificado, emisión de certificado, aceptación del Certificado, uso del Certificado y del par de claves, renovación del certificado, cambio de clave del Certificado, modificación del Certificado, suspensión y revocación del Certificado, servicio de estado de los Certificados, finalización de la Suscripción, recuperación de la clave.
5. Controles de seguridad física, gestión y de operaciones.
 - VI.1. Controles de seguridad física.

Ubicación y construcción, acceso físico, alimentación eléctrica y aire acondicionado, exposición al agua, protección y prevención de incendios, sistema de almacenamiento, eliminación de residuos, copia de seguridad.
 - VI.2. Controles de procedimientos.

Roles de confianza, número de personas requerida por tarea, identificación y autenticación para cada rol.
 - VI.3. Controles de Seguridad de personal.

Requerimientos de antecedentes, calificación, experiencia y acreditación, procedimientos de





Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

comprobación de antecedentes, formación y frecuencia de actualización de la formación. Frecuencia y secuencia de rotación de tareas, sanciones por acciones no autorizadas, requerimientos de contratación de personal, controles periódicos de cumplimiento, finalización de los contratos.

VI.4. Procedimientos de control de seguridad.

Tipos de eventos registrados, frecuencia de procesado de logs, periodo de retención para los logs de auditoría, protección de los logs de auditoría, procedimientos de copia de seguridad de los logs de auditoría, sistema de recogida de información de auditoría, notificación al sujeto causa del evento, análisis de vulnerabilidades.

VI.5. Archivo de informaciones y registros.

Tipo de informaciones y eventos registrados, periodo de retención para el archivo, sistema de recogida de información para auditoría, procedimientos para obtener y verificar información archivada.

VI.6. Cambio de clave de la ECA.

VI.7. Recuperación de la clave de la ECA.

VI.8. Cese de actividades de la ECA.

6. Controles de Seguridad Técnica.

6.1. Generación e instalación del par de claves.

Generación del par de claves, entrega de la clave privada y pública a la ECA, entrega de la clave pública y privada a los signatarios, tamaño de las claves, parámetros de generación de la clave pública, comprobación de la calidad de los parámetros, hardware y software de generación de claves, fines del uso de la clave.

6.2. Protección de la clave privada.

Estándares para los módulos criptográficos, control multi-persona de la clave privada, custodia de la clave privada, copia de seguridad de la clave privada, archivo de la clave privada, introducción de la clave privada al módulo criptográfico, método de activación de la clave privada, método de destrucción de la clave privada, clasificación de los módulos criptográficos.

6.3. Otros aspectos de la gestión del par de claves.

6.4. Datos de activación.

6.5. Controles de seguridad informática.

6.6. Controles de seguridad del ciclo de vida.

6.7. Controles de seguridad de la red.

6.8. Controles de los módulos criptográficos.

7. Perfil de certificados y de Listas de certificados revocados.

7.1 Perfil del Certificado de la ECA Raíz,

7.2 Perfil del Certificado de las ECA.

7.3 Perfil de la CRL de la Entidad Certificadora Raíz.

7.4 Perfil del OCSP si corresponde.

8. Auditoría de conformidad.

8.1 Frecuencia de los controles de conformidad para cada entidad.

8.2 Relación entre el auditor y la entidad auditada.

8.3 Comunicación de resultados.

9. Requisitos comerciales y legales.

9.1 Tarifas.

9.2 Política de confidencialidad.





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

- 9.3 Protección de datos personales.
- 9.4 Obligaciones de los participantes de la PKI.
- 9.5 Modificaciones al presente documento.
- 9.6 Resolución de conflictos.
- 9.7 Legislación aplicable.
- 9.8 Conformidad con la Ley aplicable.



LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 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 Bení, entre 4º y 5º anillo, calle 3,
Gardenia Condominio Club Torre Sur Planta Baja Of. 2
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio s/n esq. O'Connor - Piso 1
Telf.: 4-6644136 - 4-6666484
Fax.: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-60007 de 34
www.att.gob.bo

**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 6: CONTENIDO MÍNIMO DE LOS PLANES Y PROCEDIMIENTOS PARA RECUPERACIÓN ANTE DESASTRES DE LA ECA.****PLANES Y PROCEDIMIENTOS PARA RECUPERACIÓN ANTE DESASTRES****Principios:**

La ECA debe mantener controles que permitan una seguridad razonable de continuidad de las operaciones en caso de un desastre. Estos controles incluyen, como mínimo:

- a) el desarrollo y prueba de un plan de continuidad de negocio de la ECA que incluye un proceso de recuperación de desastres para los componentes críticos del sistema de la ECA;
- b) el almacenamiento de materiales criptográficos necesarios (es decir, dispositivos de activación y de materiales criptográficos seguros) estén en una ubicación alternativa;
- c) el almacenamiento de copias de seguridad de los sistemas, los datos y la información de configuración están en una ubicación alternativa, y
- d) existe la disponibilidad de un sitio alternativo, equipamiento y conectividad para permitir la recuperación.

La ECA mantiene controles para proporcionar una seguridad razonable de que las posibles interrupciones a los suscriptores y a las partes que confían se reduzcan al mínimo, como resultado de la interrupción o la degradación de los servicios de la ECA.

Controles:

1. La ECA tiene una gestión de procesos para desarrollar y mantener sus planes de continuidad del negocio. La EC tiene una estrategia de planificación para la continuidad del negocio basado en una evaluación adecuada del riesgo.
2. La ECA tiene un plan de continuidad del negocio para mantener o restablecer las operaciones de la ECA de manera oportuna después de la interrupción de, o el fracaso de los procesos de la ECA críticos. El plan de continuidad del negocio de la ECA se refiere a lo siguiente:
 - a. las condiciones para la activación de los planes;
 - b. los procedimientos de emergencia;
 - c. procedimientos alternativos;
 - d. los procedimientos de reanudación;
 - e. un programa de mantenimiento para el plan;
 - f. los requisitos de educación y sensibilización;
 - g. las responsabilidades de los individuos;
 - h. el objetivo de tiempo de recuperación (RTO), y;
 - i. las inspecciones periódicas de los planes de contingencia.
3. Los planes de continuidad del negocio de la ECA incluyen los procesos de recuperación de desastres para todos los componentes críticos de un sistema de la ECA, incluyendo el hardware, el software y las claves, en el caso de fallo de uno o más de estos componentes. En concreto:
 - a. los dispositivos criptográficos utilizados para el almacenamiento de las claves privadas de la ECA se almacenan de forma segura en un lugar fuera del sitio para la recuperación de la ECA en el caso de un desastre en las instalaciones de la ECA primaria, y;
 - b. las acciones clave secretas necesarias o componentes clave, necesarios para utilizar y gestionar los dispositivos criptográficos de recuperación de desastres, se almacenan de forma



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

segura en una ubicación fuera del sitio.

4. Se toman regularmente copias de seguridad de la información empresarial esencial. Los requisitos de seguridad de estas copias son consistentes con los controles de la información respaldada.
5. La ECA identifica y organiza un sitio alternativo donde las operaciones de PKI básicas se pueden restaurar en caso de un desastre en el sitio principal de la ECA. Los equipos de repliegue y los medios de copia de seguridad están situados a una distancia segura para evitar daños por desastre en el sitio principal.
6. Los planes de continuidad del negocio de la ECA incluyen los procedimientos para asegurar su facilidad en la medida de lo posible durante el período de tiempo después de un desastre y antes de restaurar un entorno seguro ya sea en el original o en un sitio remoto.
7. Los planes de continuidad del negocio de la ECA hacen frente a los procedimientos de recuperación aplicados si los recursos de computación, software y / o los datos están dañados o son sospechosos de estar dañado.
8. Los planes de continuidad del negocio son probados con regularidad para asegurarse de que están al día y son efectivos.
9. Los planes de continuidad de negocios definen un tiempo de interrupción del sistema aceptable, el tiempo de recuperación, y el tiempo medio entre fallos, como se describe en el CP y / o CPS.
10. Los planes de continuidad de negocios son mantenidos por las revisiones periódicas y las actualizaciones para asegurar su eficacia constante.
11. La ECA mantiene procedimientos para la terminación, la notificación de las entidades afectadas, y para transferir los registros de la ECA archivados correspondientes a un custodio, como se describe en el CP y / o CPS.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 7: CONTENIDO MÍNIMO PARA LAS PLANES Y PROCEDIMIENTOS DE SEGURIDAD Y EVALUACION DE RIESGOS DE LA ECA.****CONSIDERACIONES DE SEGURIDAD DE LA ECA****Controles:**

1. Un documento de política de seguridad de la información, que incluye seguridad física, de personal, controles técnicos y de procedimiento, está aprobado por la administración, publicada y comunicada a todos los empleados.
2. La política de seguridad de la información incluye lo siguiente:
 - a. una definición de la seguridad de la información, sus objetivos generales y ámbito de aplicación, la importancia de la seguridad como un mecanismo que permite el intercambio de información;
 - b. una declaración de intenciones de gestión, el apoyo a los objetivos y principios de la seguridad de la información;
 - c. una explicación de las políticas de seguridad, los principios, las normas y los requisitos a cumplir de particular importancia para la organización;
 - d. una definición de las responsabilidades generales y específicas para la gestión de seguridad de la información, incluidos los incidentes de seguridad de información, y
 - e. las referencias a la documentación, que apoya la política.
3. Hay un proceso de revisión definido para el mantenimiento de la política de seguridad de la información, incluyendo las responsabilidades y las fechas de revisión.

Infraestructura de la Seguridad de la Información

1. La alta dirección y/o un comité de seguridad de la información de alto nivel tienen la responsabilidad de asegurarse de que haya una clara dirección y gestión de apoyo para gestionar los riesgos de manera efectiva.
2. Un grupo de administración y/o un comité de seguridad debe existir para coordinar la aplicación de controles de seguridad de la información y la gestión del riesgo.
3. Las responsabilidades para la protección de los activos individuales, y para llevar a cabo procesos específicos de seguridad están claramente definidos.
4. Se tiene una administración de procesos de autorización para facilitar nuevos procesos de información y es seguido.

**Seguridad de Acceso de Terceros**

1. Existen procedimientos y se aplican para controlar el acceso físico y lógico a las instalaciones de la EC y los sistemas por parte de terceros.
2. Si existe necesidad de la entidad emisora para permitir el acceso de terceros a las instalaciones y los sistemas de la EC, se realiza una evaluación de riesgos para determinar las implicaciones de seguridad y los requisitos de control específicos.
3. Los preparativos en cuanto al acceso de terceros a las instalaciones y los sistemas de la EC se basan en un contrato formal que contenga los requisitos de seguridad necesarios.

**Subcontratación**

1. Si la EC externaliza la gestión y control de todos o algunos de sus sistemas de información, redes y / o entornos de escritorio, los requisitos de seguridad de la EC se abordan en un contrato acordado entre las partes.

Si la EC elige delegar una parte de las funciones de la EC a otra parte, la EC mantiene la responsabilidad en la realización de las funciones externalizadas y la definición y mantenimiento de un estado de la CPS.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 8: CONTENIDO MÍNIMO PARA LOS PLANES Y PROCEDIMIENTOS DE SEGURIDAD Y EVALUACION DE RIESGOS DE LA ECA.****CONSIDERACIONES PARA LA ADMINISTRACIÓN DE OPERACIONES DE LA ECA****Principios:**

La EC mantiene controles para proporcionar una seguridad razonable de que:

- se garantiza el funcionamiento correcto y seguro de las instalaciones de procesamiento de información de la EC;
- el riesgo de fallo de los sistemas de la EC se reduce al mínimo;
- la integridad de los sistemas de la EC y la información está protegido contra virus y software malicioso;
- el daño de los incidentes de seguridad y fallos de funcionamiento se reduce al mínimo mediante el uso de la notificaciones de incidentes y procedimientos de respuesta, y;
- los medios están bien manejados para protegerlos de daños, robo y acceso no autorizado.

Controles:**Procedimientos operacionales y responsabilidades**

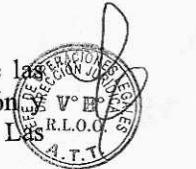
- Los procedimientos operativos de la EC están documentados y mantenidos para cada área funcional.
- La gestión formal de las responsabilidades y procedimientos existen para controlar los cambios de equipamiento de la EC, de software y procedimientos operativos.
- Los deberes y áreas de responsabilidad están segregadas en orden para reducir oportunidades no autorizadas de modificaciones o mal uso de la información y los servicios.
- Los ambientes de pruebas de desarrollo y los ambientes operacionales están separadas.
- Se prioriza el uso externo de los ambientes de gestión de servicios, riesgos y controles de confianza identificados, además del contratante, e incorporado en el contrato.

Planificación y Aceptación del Sistema

- Las demandas de capacidad son monitoreadas y se realizan proyecciones de las necesidades futuras de capacidad, para asegurar que la capacidad de procesamiento y almacenamiento adecuados estén disponibles.
- Los criterios de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones se establecen y se realizan pruebas adecuadas del sistema antes de la aceptación.
- Protección contra virus y software malicioso
- Se implementan controles de detección y prevención para proteger los sistemas contra virus y software malicioso. Existen programas de sensibilización de los empleados.

**Reporte de Incidentes y Respuesta**

- Existe un procedimiento formal de notificación de incidentes de seguridad que establece las acciones a tomar en la recepción de un informe de incidente. Esto incluye una definición documentación de las responsabilidades asignadas y procedimientos de escalamiento. Las incidencias se reportan a la ECR como una cuestión de urgencia.
- Los usuarios están obligados a observar y reportar las deficiencias observadas o sospechadas de seguridad en los sistemas de la EC, o amenazas a los sistemas o servicios a medida que se detecten.
- Existen procedimientos y son seguidos para informar de fallos de hardware y software.
- Existen procedimientos y se siguen para evaluar que la acción correctiva se toma para los incidentes reportados.





Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015

5. Existe un proceso formal de gestión de problemas que permite a los tipos, volúmenes y los impactos de incidentes y fallos de funcionamiento ser documentados, cuantificados y controlados.

Manejo del Papel y la Seguridad

1. Los procedimientos para la gestión de los medios informáticos extraíbles requieren lo siguiente:
 - a. Si ya no es necesario, el contenido previo de cualquier medio reutilizable que se va a eliminar de la organización, se borra o se destruye el medio informático;
 - b. Se requiere autorización para todos los medios removidos de la organización y se mantiene un registro para mantener una pista de auditoría, y
 - c. Todos los medios informáticos se guardan en un ambiente seguro, de acuerdo con las especificaciones de los fabricantes.
2. Los equipos que contienen medios de almacenamiento (por ejemplo, discos duros, fijos) se los revisa para determinar si contienen datos sensibles antes de su eliminación o reutilización. Los dispositivos de almacenamiento que contienen información sensible están físicamente destruidos o sobrescritos de forma segura antes de su eliminación o reutilización.
3. Existen procedimientos para el manejo y almacenamiento de la información y se siguen con el fin de proteger dicha información contra su divulgación o uso no autorizado.
4. La documentación del sistema está protegida del acceso no autorizado.



**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015****ANEXO 9: CONTENIDOS MÍNIMOS DE LOS PROCEDIMIENTOS Y LAS CONDICIONES QUE DEBERÁN CUMPLIR LAS ENTIDADES CERTIFICADORAS PARA LA CONSERVACIÓN DE LOS DOCUMENTOS FÍSICOS Y DIGITALIZADOS.****PROCEDIMIENTOS Y CONDICIONES PARA LA CONSERVACIÓN DE DOCUMENTOS DE LA EC**

Según el artículo 32 parágrafo IV del Reglamento para el Desarrollo de las TIC aprobado por D.S. N° 1793 del 13 de noviembre de 2013 y estándares internacionales.

1. Para la conservación y mantenimiento de archivos físicos y digitales mínimamente se establece:
 - a) Una vez terminado el proceso de registro y emisión del certificado y las claves del usuario, se procederá a la foliación de la documentación presentada y el almacenamiento de las claves y el certificado en forma segura.
 - b) Cada documento presentado después de foliado, deberá ser escaneado, con el fin de tener un archivo magnético ordenado por número de certificado en carpetas distribuidas por años.
 - c) Se mantendrá un archivo físico, ordenados en carpetas que deben estar rotuladas en el lomo con escritura clara a computadora en la que especificará el número y tipo de certificado.
 - d) Se mantendrá un archivo físico, ordenados en medios de almacenamiento de la información rotulados con escritura clara a computadora en la que especificará el número y tipo de certificado
 - e) Después de terminada cada auditoría externa realizada por la ATT, se procederá a empastar la documentación física.
 - f) La documentación debe estar archivada hasta 5 años después de la revocación del certificado o el cambio de claves del signatario.
2. Para la conservación y mantenimiento de archivos físicos y magnéticos de archivos se establecen las siguientes directrices:
 - a) Toda la documentación generada en los registros de signatarios deberán conservarse de manera ordenada y cronológica, separando mes, año y tipo de documento.
 - b) La documentación digital y los archivos digitales deben conservarse de manera ordenada y cronológica, separando mes, año y tipo de documento.
3. Destrucción de los documentos
 - a) La Política de Certificación especifica el medio a través del cual se realiza la destrucción de claves y del certificado del signatario.
 - b) La CP o CPS especifican los requisitos para la destrucción de todas las copias y fragmentos de las claves públicas y privadas y el certificado del signatario al final del ciclo de vida del par de claves.
 - c) Si es necesario, la CP especifica los requisitos para el uso y manejo de hardware criptográfico y los procesos de autenticación de abonado (y las acciones posteriores) en el que el hardware criptográfico está en otras ubicaciones físicas (es decir, un HSM conectado a un ordenador central o servidor remoto).
 - d) La destrucción de la documentación física y digital de una EC debe ser supervisada por la ATT.

ANEXO 10: NIVELES DE SEGURIDAD.

De acuerdo al DS 1793 la generación de la firma digital debe estar en control del signatario es por este motivo que la ECA y la AR deben informar al usuario lo siguiente:

"Los datos de creación de firma digital pueden definirse como: "aquellos datos únicos, tales como



33 de 34

**Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015**

códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital”, siendo estos los que el signatario debe mantener bajo su control”.

Los niveles de seguridad están clasificados en:

Nivel de seguridad alto:

Dispositivo que cuente con la certificación del NIST FIPS 140-2 nivel 3 o superior, aconsejado para la generación de claves y almacenamiento de la clave privada de las Entidades Certificadoras Autorizadas.

Nivel de seguridad medio:

Dispositivo que cuente con la certificación del NIST FIPS 140-2 nivel 2, aconsejado para la generación de claves (pública y privada), almacenamiento de la clave privada y almacenamiento del certificado digital será recomendado para:

- aquellos usuarios (futuros signatarios) que tengan responsabilidad de acreditación de identidad y otras condiciones de los signatarios en las Agencias de Registro.
- aquellos usuarios (futuros signatarios) que requieran mayor seguridad de acuerdo al tipo de documento a rubricar (tipo de información, rol del signatario, requerimiento de una aplicación, etc.).

Nivel de seguridad normal:

Por software, puede ser recomendado para la generación de claves y almacenamiento de la clave privada y resguardo del certificado digital, para el resto de los usos y signatarios.

NOTA: De optarse por esta modalidad, la ECA debe realizar las correspondientes previsiones de recursos para mesa de ayuda y/o información del estilo tutorial para los usuarios.

