Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 845/2018

La Paz, 13 de Noviembre de 2018

Abog. Nicola Fernanda Peña Barriga
ANALISTA LEGAL
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

VISTOS:

El Informe Técnico ATT-DTLTIC-INF TEC LP 648/2018 de 07 de septiembre de 2018 **(INF. - TEC. 648/2018)**; el Informe Jurídico ATT-DJ-INF-JUR LP 839/2018 de 13 de noviembre de 2018 **(INF. - JUR. 839/2018)**; y todo lo que ver convino y se tuvo presente;

CONSIDERANDO 1. ÁMBITO DE COMPETENCIA.-

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

CONSIDERANDO 2. ANTECEDENTES.-

Que por **INF. – TEC. 648/2018** la Unidad de Tecnologías de Información dependiente de la Dirección Técnica Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación - DTLTIC, concluyó que en cumplimiento de lo establecido por el Decreto Supremo N° 3527 de 11 de abril de 2018 **(D.S. N° 3527)** que modificó el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante el Decreto Supremo N° 1793 de 13 de noviembre de 2013 **(REGLAMENTO TIC)**, el cual determinó que la ATT modificará y adecuara los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las entidades certificadoras, por lo que existe la necesidad de dejar sin efecto la Resolución Administrativa Regulatoria ATT-DJ-RA TL 31/2015 de 09 de enero de 2015 **(R.A.R. 31/2015)** y emitir un nuevo acto administrativo, considerando las modificaciones e inclusiones realizadas en el referido D.S. N° 3527.

Que el **INF. – JUR. 839/2018** concluyó que la propuesta de aprobación de los documentos públicos de la Entidad Certificadora Raíz en el marco de la modificación al REGLAMENTO TIC realizada mediante el D.S. N° 3527, se encuentra conforme a lo establecido en la normativa del sector y toda vez que no contraviene ninguna normativa legal vigente, recomendó aprobar dichos documentos a través de Resolución Administrativa Regulatoria correspondiente y dejar sin efecto la Resolución Administrativa ATT-DJ-RA TL LP 31/2015 de 09 de enero de 2015.

CONSIDERANDO 3. MARCO NORMATIVO.-

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 el artículo 81 de la LEY N° 164, determina que la ATT es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras de acuerdo a lo establecido en la citada Ley y su Reglamentación.

I-LP-15466

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

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

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

TARIJA: Calle Alejandro del Carpio N° 720 esq. O´Connor
Piso 1
Telf.: 4-644136

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

Que el artículo 83 de dicha Ley, establece que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB, prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la citada Ley y velará por la autenticidad, integridad y no repudio entre las partes.

Que el artículo 1 del REGLAMENTO TIC 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 24 del REGLAMENTO TIC 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 el parágrafo II del artículo 27 de dicho Reglamento, dispone que la ATT mediante Resolución Administrativa establecerá el formato y estructura de los certificados digitales tanto para personas natrales como para personas jurídicas.

Que el parágrafo II del artículo 28 del REGLAMENTO TIC, determina 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 parágrafo IV del artículo 32 del referido Reglamento, establece que la ATT mediante Resolución Administrativa determinara 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 numeral 1 el artículo 37 del REGLAMENTO TIC, establece dentro de la organización de la Infraestructura Nacional de Certificación Digital, el siguiente nivel: *"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 artículo 38 de dicho Reglamento, determina las funciones de la ATT respecto a la certificación digital, como Entidad Certificadora Raíz para el cumplimiento de las atribuciones establecidas en la LEY N° 164.

Que el inciso j) del referido artículo, establece que la ATT tiene entre sus funciones: *"aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones"*.

Que el D.S. N° 3527 modificó varios artículos del REGLAMENTO TIC e incorporó varios incisos a los articulados de dicho Reglamento, respecto a las definiciones de autenticación y signatario, se incorporaron definiciones de firma digital automática y de sistema informático.

Que la Disposición Transitoria Primera del D.S. N° 3527 establece que la ATT tendrá un plazo de noventa (90) días para modificar y adecuar los estándares técnicos u otros lineamientos establecido para el funcionamiento de las entidades certificadoras.

I-LP-15466

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

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

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

TARIJA: Calle Alejandro del Carpio N° 720 esq. O´Connor Piso 1 Telf.: 4-644136

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

CONSIDERANDO 4. ANÁLISIS.-

Que la Unidad de Tecnologías de Información dependiente de la DTLTIC a través del **INF - TEC 648/2018**, propuso dejar sin efecto la R.A.R. 31/2015 que aprobó en anexo los documentos públicos de la Entidad Certificadora Raíz – ECR, y dando cumplimiento a lo establecido en el D.S. N° 3527 que modificó el REGLAMENTO TIC, el cual establece que la ATT modificará y adecuará los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras; y emitir una nueva Resolución Administrativa Regulatoria que en anexo apruebe los siguientes documentos públicos de la Entidad Certificadora Raíz conforme a las modificaciones realizadas por el D.S. N° 3527:

- ***Política de Certificación (ECR - PC)***, contiene las directivas generales de la ATT para la emisión de certificados digitales a las Entidades Certificadoras Autorizadas por parte de la ECR, el ámbito de aplicación y los lineamientos para su funcionamiento considerando las modificaciones al REGLAMENTO TIC.

- ***Declaración de Prácticas de Certificación (ECR-DPC)***, describe los pasos para la emisión de certificados digitales para entidades certificadoras autorizadas.

- ***Lineamientos para terceros aceptantes (ECR-LT)***, describe los pasos necesarios que debe seguir un tercero aceptante para validar la firma digital, eliminando el certificado de cargo público en el marco de la modificación al REGLAMENTO TIC.

- ***Procedimiento para la Autorización de las Entidades Certificadoras (ECR-PAEC)***, describe los pasos a seguir para la autorización de entidades certificadoras.

Que en este sentido, toda vez que dicha propuesta se encuentra conforme a lo establecido en el D.S. N° 3527 que modificó el REGLAMENTO TIC y en el marco de la normativa vigente del Sector, se deberá dar curso a la solicitud de la DTLTIC y emitir la correspondiente Resolución Administrativa Regulatoria.

POR TANTO:

El Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, Ing. 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.- DEJAR SIN EFECTO la Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 31/2015 de 09 de enero de 2015, mediante la cual se aprobó los Documentos Públicos de la Entidad Certificadora Raíz en el marco del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante el Decreto Supremo N° 1793 de 13 de noviembre de 2013 .

SEGUNDO.- APROBAR los Documentos Públicos de la Entidad Certificadora Raíz – ECR en cumplimiento de lo establecido por el Decreto Supremo N° 3527 de 11 de abril de 2018 que modificó el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, que forman parte del anexo indivisible de la presente Resolución, los cuales son:

I-LP-15466

1. *Política de Certificación (ECR - PC).*
2. *Declaración de Prácticas de Certificación (ECR-DPC).*
3. *Lineamientos para terceros aceptantes (ECR-LT).*
4. *Procedimiento para la Autorización de las Entidades Certificadoras (ECR-PAEC).*

TERCERO.- INSTRUIR a la Dirección Técnica Sectorial de Telecomunicaciones y TIC que proceda a la publicación de la presente Resolución Administrativa Regulatoria en un medio de comunicación escrito de circulación nacional, así como en la página web de la ATT (www.att.gob.bo).

Regístrese y archívese.

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

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

DIRECCIÓN TEC. SECTORIAL DE TEL. Y TIC V°B° A.T.T.

DIRECCIÓN JURÍDICA V°B° J.C.M. A.T.T.

DIRECCIÓN JURÍDICA V°B° N.F.P.B. A.T.T.

I-LP-15466

ANEXOS

I-LP-15466

ENTIDAD CERTIFICADORA RAÍZ ESTADO PLURINACIONAL DE BOLIVIA

AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT

POLÍTICA DE CERTIFICACIÓN DE LA ENTIDAD CERTIFICADORA RAÍZ DE LA INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN DIGITAL INCD

Datos del documento	
Título del documento	Política de Certificación de la Entidad Certificadora Raíz
Identificador documental	ECR-PC
Criticidad:	Alta
Fecha	13 de noviembre de 2018
Autor	ATT
Versión	2.0
Comentario	
Publicación	Público

I-LP-15466

Noviembre 2018

CONTENIDO

I-LP-15466

I-LP-15466

LA PAZ: Calle 13 de Calacoto Nº 8260 entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-4581184 4-4581185

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

TARIJA: Calle Alejandro del Carpio Nº 720 esq. O´Connor Piso 1 Telf.: 4-644136

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

1. INTRODUCCIÓN

1.1. DESCRIPCION GENERAL

La presente política de emisión de certificados digitales para entidades certificadoras se encuadra en las prescripciones de la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones y Tecnologías de Información y Comunicación, en el Reglamento para el Desarrollo de las TIC aprobado mediante el Decreto Supremo N° 1793 del 13 de noviembre de 2013, en las modificaciones al Decreto Supremo N° 1793 aprobadas mediante Decreto Supremo N° 3257 de 11 de abril de 2018 y en los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente del Estado Plurinacional de Bolivia.

La implementación técnica de la infraestructura de firma digital de clave pública se basa en el uso de estándares técnicos internacionales. En este sentido, además de la normativa citada se ha tenido en cuenta para la elaboración de esta Política de Certificación, el RFC 3647 producido por IETF[1] y la especificación ITU-T [2]X.509. La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT del Estado Plurinacional de Bolivia, es la entidad encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras dentro de la Jerarquía Nacional de Certificación Digital. En consiguiente, administra la Entidad Certificadora Raíz - ECR, constituyéndose en la entidad certificadora de nivel superior que emite certificados digitales a las entidades certificadoras públicas y privadas subordinadas, que hayan cumplido con los requisitos exigidos para la prestación de servicios de firma y certificación digital en la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia (INCDB).

Las entidades certificadoras que requieran un certificado de la ECR deben ajustarse a los procedimientos determinados por la ATT en la Resolución Administrativa Regulatoria vigente que apruebe los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras", mediante los cuales son autorizadas pasando a ser denominadas "Entidades Certificadoras Autorizadas", en adelante ECA.

El certificado de la ECR permitirá la verificación de los certificados de las ECA subordinadas, generando una cadena de confianza.

La ATT en su calidad de ECR asesora y orienta en la asistencia necesaria a fin de facilitar el cumplimiento de lo establecido en la presente Política y en la Declaración de Prácticas de Certificación, como así también en el cumplimiento de la normativa marco de la INCDB.

La presente Política de Certificación contiene las directivas generales de la ATT para la emisión de certificados digitales a las ECA por parte de la ECR, el ámbito de aplicación y los lineamientos para su funcionamiento.

Este documento se complementa con la Declaración de Práctica de Certificación y los procedimientos específicos desarrollados para su implementación en el ámbito institucional del Estado Plurinacional de Bolivia.

I-LP-15466

[1] Internet EngineeringTaskForce (IETF) (en español Grupo de Trabajo de Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, es mundialmente conocido por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

[2] Sector de Normalización de las Telecomunicaciones de la UIT (Unión Internacional de Telecomunicaciones).

Las ECA emiten certificados digitales a las personas naturales, las personas jurídicas públicas o privadas. Luego las firmas basadas en certificados digitales emitidos por las Entidades Certificadoras Autorizadas constituyen las firmas digitales con la validez jurídica y probatoria establecida en el artículo 78 de la Ley N°164.

1.1.1. OBLIGACIONES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS

En particular, de acuerdo al artículo 43 del Decreto Supremo N° 1793 y sus modificaciones aprobadas mediante Decreto Supremo N" 3257 de 11 de abril de 2018, las ECA están obligadas a:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT en su calidad de ECR;
b) Desarrollar y actualizar los procedimientos vinculados a los servicios de certificación digital, en función de las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT en su calidad de ECR;
c) Informar a los usuarios de las condiciones acordadas para la emisión, validación, renovación, baja, suspensión, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web entre otros medios;
d) Mantener el control, reserva y cuidado de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Cualquier anomalía que pueda comprometer su confidencialidad deberá ser comunicada inmediatamente a la ATT en su calidad de ECR;
e) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
f) Mantener un sistema de información de acceso libre, permanente y actualizado donde se publiquen los procedimientos de certificación digital, así como los certificados digitales emitidos consignando, su número único de serie, su fecha de emisión, vigencia y restricciones aplicables, así como el detalle de los certificados digitales suspendidos y revocados;
g) Las entidades certificadoras que derivan de la certificadora raíz (ATT) deberán mantener un sistema de información con las mismas características mencionadas en el punto anterior, ubicado en territorio y bajo legislación del Estado Plurinacional de Bolivia;
h) Revocar el certificado digital al producirse alguna de las causales establecidas en el presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la revocatoria deben ser estipuladas en los contratos de los titulares;
i) Mantener la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso;
j) Mantener la información relativa a los certificados digitales emitidos, por un período mínimo de cinco (5) años posteriores al periodo de su validez o vigencia;
k) Facilitar información y prestar la colaboración debida al personal autorizado por la ATT, en el ejercicio de sus funciones, para efectos de control, seguimiento, supervisión y fiscalización del servicio de certificación digital, demostrando que los controles técnicos que emplea son adecuados y efectivos cuando así sea requerido;
l) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
m) Notificar a la ATT en su calidad de ECR cualquier cambio en la personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos o correo electrónico;
n) Verificar toda la información proporcionada por el solicitante del servicio, bajo su exclusiva responsabilidad;
o) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;

I-LP-15466

p) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidos que administra.
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.

1.1.2. RESPONSABILIDADES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS (ECA):

- Las ECA serán responsables ante terceros, por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios.
- Las ECA se liberarán de responsabilidades si se demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.
- Las ECA deberán responder por posibles perjuicios que se causen al signatario o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

1.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Título del documento: "Política de Certificación de la Entidad Certificadora Raíz del Estado Plurinacional de Bolivia"
Versión: 2.0
Fecha de emisión del documento: 09/01/2015
Fecha de la última actualización: 13/11/2018
Sitio Web de Publicación: www.ecrb.att.gob.bo
Para solicitar información o aclaraciones respecto a la presente política se podrá dirigir a:
UNIDAD DE REGULACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN ADMINISTRADORA DE LA ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA - ATT
Calle 13 de Calacoto entre Av. Costanera y Av. Los Sauces # 8260.
Teléfono: (+591)2772266
Fax: (+591)2772299
Dirección de correo electrónico: ecrb@att.gob.bo

1.3. PARTICIPANTES DE LA INFRAESTRUCTURA DE CERTIFICACIÓN DIGITAL DE BOLIVIA

La INCD de Bolivia es el conjunto de normas, estándares tecnológicos, procedimientos, equipos, redes, bases de datos, programas informáticos y dispositivos de cifrado, preparados para la generación, almacenamiento y publicación del estado, la vigencia y validez de los certificados digitales reconocidos por las entidades certificadoras, de acuerdo a los establecido en el inciso e del parágrafo III del artículo 3 del Decreto Supremo N° 1793 del 13 de noviembre de 2013 y su modificación aprobada mediante Decreto Supremo N° 3527 de 11 de abril de 2018.
Los participantes de la Infraestructura antes mencionada son:

- ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte, es el organismo que asume las atribuciones, competencias derechos y obligaciones en materia de comunicaciones, tecnologías de la información y comunicación; transporte; servicio postal en el

I-LP-15466

ámbito del Ministerio de Obras Públicas, Servicios y Vivienda, y cuyas funciones específicas se encuentran en el artículo 38 del Decreto Supremo N° 1793 y su modificación aprobada mediante Decreto Supremo N° 3527 de 11 de abril de 2018, siendo las siguientes:

a) Autorizar la operación de entidades de certificación;
b) Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad;
c) Definir los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación;
d) Evaluar las actividades desarrolladas por las entidades de certificación de acuerdo a los estándares definidos en los reglamentos técnicos;
e) Revocar o suspender la autorización para operar como entidad de certificación;
f) Requerir en cualquier momento a las entidades de certificación información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren;
g) Verificar la calidad de prestación del servicio público de certificación y firma digital;
h) Imponer sanciones a las entidades de certificación por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio;
i) Ordenar la revocación o suspensión de certificados digitales cuando la entidad de certificación los hubiere emitido sin el cumplimiento de las formalidades legales;
j) Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones;
k) Emitir certificados digitales en relación con las firmas digitales de las entidades de certificación.
l) Definir el tiempo de vigencia de los certificados digitales.

- ECR: Entidad Certificadora Raíz de ATT, constituyendo el primer nivel dentro de la Jerarquía Nacional de Certificación Digital emite certificados a las Entidades Certificadoras Autorizadas – ECA-, sus funciones se establecen en el artículo 39 del Decreto Supremo N° 1793 y su modificación aprobada mediante Decreto Supremo N° 3527 de 11 de abril de 2018.

- ECA: Entidades Certificadoras Autorizadas, de segundo nivel subordinadas a la ECR, que cumplieron los requisitos exigidos para la autorización de prestación del servicio, emiten certificados a los signatarios finales, sus funciones se establecen en el artículo 39 del Decreto Supremo N° 1793 y su modificación aprobada mediante Decreto Supremo N° 3527 de 11 de abril de 2018, siendo las siguientes:

a) Emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales;
b) Facilitar servicios de generación de firmas digitales;
c) Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario;
d) Validar y comprobar cuando corresponda, la identidad y existencia real del solicitante;
e) Reconocer y validar los certificados digitales emitidos en el exterior;
f) Otras funciones relacionadas con la prestación de servicios de certificación Digital.

1-LP-15466

- AR: Agencia/Autoridad de Registro, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además, es quién se encarga de solicitar la aprobación o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital. Constituyen el tercer nivel de la Jerarquía. Sus funciones se establecen en el artículo 40 del Decreto Supremo N° 1793 y su modificación aprobada mediante Decreto Supremo N° 3527 de 11 de abril de 2018, siendo las siguientes:

  a) La recepción de las solicitudes de emisión de certificados;
  b) Comprobar la identidad y autenticación de los datos de los titulares de certificados;
  c) Comprobar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la entidad certificadora;
  d) La remisión de las solicitudes aprobadas a la entidad certificadora con la que se encuentre operativamente vinculada;
  e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la entidad certificadora con la que se vinculen;
  f) La identificación y autenticación de los solicitantes de revocación de certificados;
  g) El archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la entidad certificadora;
  h) El cumplimiento de las normas y recaudos establecidos para la protección de los datos personales;
  i) El cumplimiento de las disposiciones que establezca la política de certificación y el manual de procedimiento de la entidad certificadora con la que se encuentre vinculada.

- Signatario: titular del certificado digital emitido por una ECA autorizada, que le permite firmar digitalmente. Para la presente Política, los signatarios serán las ECA, titulares de los certificados emitidos por la ECR. Las Entidades Certificadoras cumplen los procedimientos de autorización y a los lineamientos establecidos en este documento para integrar la INCDB.

- Repositorio de la ECR: sistema único que almacena los certificados y las CRL que emite la ECR y que sirve para distribuirlos a los signatarios.

- Terceros aceptantes: es la persona natural o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez, para el momento de la firma, del certificado digital correspondiente y validar la cadena de confianza.

1.4. USO DE LOS CERTIFICADOS

La ECR emite certificados digitales para las ECA que serán a su vez utilizados en la emisión y firma de los certificados de sus respectivos signatarios y la firma se sus listas de certificados revocados (CRL), de acuerdo a las correspondientes Políticas de Certificación y en cumplimiento de la normativa vigente.

La función del certificado de la ECR es identificar a la ATT como la entidad que firma los certificados digitales de las ECA. De esta manera, permite identificar a las entidades certificadoras que se encuentran autorizadas a funcionar en la INCD del Estado Plurinacional de Bolivia, completando la cadena de

I-LP-15466

confianza de cualquier certificado digital emitido en dicho país. El certificado de la ECR es auto-firmado y vincula su clave pública con los datos de ATT en su calidad de ECR, permitiendo la verificación de la validez de la firma digital de su Lista de Certificados Revocados (CRL) y de los certificados de las ECA y de todos los certificados emitidos por ellas.

La ECR almacena su clave privada en dispositivos criptográficos seguros HSM[3].

El uso de los certificados emitidos por la ECR se encuentra expresado en la presente política, prohibiéndose para cualquier otro fin.

La Entidad Certificadora Raíz es el punto de inicio de la confianza de INCD, su certificado es utilizado para dar validez a las ECA mediante la emisión a su nombre de un certificado digital.

Cada una de las Entidades que fueron autorizadas para brindar servicios de certificación digital utilizarán dicho certificado para firmar los certificados digitales que emitan a sus signatarios, construyéndose a través de este encadenamiento la confianza de la INCD, basada técnicamente en la aplicación de estándares reconocidos internacionales.

La verificación de una firma digital se realiza validando que se ha utilizado un certificado emitido por una ECA perteneciente a la INCDB y al mismo tiempo se debe controlar que se ha realizado durante el periodo de vigencia de ese certificado y que no se encuentre revocado. La verificación de la validez del certificado se realiza mediante la consulta de su estado a la Lista de Certificados Revocados (CRL) en la fecha para el momento de la firma. Asimismo, se debe corroborar que la CRL se encuentra firmada por la ECR para garantizar su integridad y origen.

1.5. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

La Política de Certificación es administrada por la ATT en su calidad de ECR y se han desarrollado procedimientos para efectuar cualquier modificación o actualización.

Esta política se encuentra disponible en su sitio web en forma permanente y en sus versiones anteriores como la vigente, así como en otros medios de difusión pública que la ATT en su calidad de ECR considere oportunos.

Los cambios realizados al presente documento se comunicarán a las ECA de manera anticipada.

Los procedimientos asociados directamente a lo establecido por esta política se encuentran descriptos en la Declaración de Prácticas de Certificación.

1.6. DEFINICIONES Y ABREVIATURAS

ITU-T: (*International Telecommunication Union*) Unión Internacional de Telecomunicaciones. Sector de Normalización de las Telecomunicaciones.
IETF: (*Internet Engineering Task Force*) Grupo de Trabajo de Ingeniería de Internet

I-LP-15466

[3] El HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege claves y llaves criptográficas.

RFC: (*Requestfor Comments*) Publicación del IETF que describe aspectos del funcionamiento de internet. Cada publicación es identificada con un número y un título, y antes de su versión final es sometido a un proceso que asegura calidad y coherencia.
INCD: Infraestructura Nacional de Certificación Digital
EC: Entidad de Certificación o Entidad Certificadora
ECR: Entidad Certificadora Raíz
ECA: Entidad Certificadora Autorizada
ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes
AR: Agencia de Registro
CRL: (*Certification Revocation List*) Lista de Certificados Revocados
OID: (*Object Identifier*) Identificador de Objeto
PC: Política de Certificación
DPC: Declaración de Prácticas de Certificación.
DN: (*Distinguished name*) Nombre distintivo
CSR :(*Certificate Signing Request)* Requerimiento de firma de certificado
HSM: (*Hardware Security Module*) Dispositivo criptográfico basado en hardware
NIST: *(National Institue of Standards and Tecnhnology*) Instituto Nacional de Estándares y Tecnología.
FIPS: (*Federal Information Proccessing Standards*) Estándares Federales de Procesamiento de la Información.
Certificado digital: Es un documento digital firmado digitalmente por una entidad certificadora autorizada o por la ECR que vincula unos datos de verificación de firma a un signatario. Debe responder a formatos y estándar reconocidos internacionalmente y fijados en los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente.

2. RESPONSABILIDAD DEL REPOSITORIO Y SU PUBLICACIÓN

Es responsabilidad de la ATT en su calidad de ECR la seguridad técnica, operativa y de gestión de las actividades de la ECR, así como de la publicación permanente y actualizada de su Política de Certificación, su certificado digital, su Declaración de Prácticas de Certificación, la lista de certificados revocados -CRL, y toda documentación que considere de relevancia para el cumplimiento de su misión.

La ECR publica en su sitio web las Políticas de las ECA, los actos por las que fueron autorizadas, sus certificados digitales, sus datos de contacto y toda otra información relativa a dichas entidades que considere relevante.

Asimismo, y de acuerdo a la normativa vigente, publica:
- Los procedimientos de certificación digital.
- Los procedimientos de reclamos.
- Los términos y condiciones de servicios para la provisión de servicios de firma y certificación digital.

La CRL será actualizada y publicada cuando se produzca la revocación o emisión de un certificado, o bien a los 6 meses de la última emisión de CRL.

I-LP-15466

Los controles generales de seguridad sobre el repositorio de la ECR se realizan de manera de asegurar la confidencialidad, la disponibilidad e integridad de la información, las redes y los sistemas asociados.

El repositorio se encuentra disponible para consulta del público las veinticuatro (24) horas, los siete (7) días de la semana y su mantenimiento se realiza de acuerdo a un calendario programado.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

La identificación de las Entidades Certificadoras es realizada por la ATT en su calidad de ECR durante el proceso que autoriza su funcionamiento, luego de realizar las revisiones de la documentación y de la infraestructura tecnológica de acuerdo a la reglamentación vigente, verificando su estricto cumplimento.

La ATT en su calidad de ECR, mediante la firma de un contrato con la ECA, otorgará la autorización para la prestación de servicios de certificación digital, con una vigencia de cinco (5) años, renovables por periodos similares, a personas jurídicas de derecho público o privado que así lo soliciten.

Dicho certificado que es firmado por la ECR, vincula la Política de Certificación, los datos de la ECA y su clave pública. Para confirmar estos datos, previo a la emisión del certificado, la ECA verifica que la información contenida en la solicitud del certificado sea correcta.

Los certificados emitidos por la ECR tienen un nombre distintivo (DN) único en el campo *Subject* que es elegido por la ECA para su identificación en la INCD del Estado Plurinacional de Bolivia. Este nombre debe ser único y de fácil comprensión, de acuerdo a la siguiente definición: CN (CommonName) = Denominación de la Entidad Certificadora Autorizada; O (Organization) = Razón Social de la Entidad Certificadora Autorizada; C = BO (estándar de acuerdo a ISO3166).

La información remitida por las ECA para su identificación se considera confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida en causa judicial por juez competente o se trate de información pública.

Los procedimientos llevados a cabo por la ECR para la gestión del ciclo de vida de sus certificados se registran y refrendan de manera documentada por la ATT en su calidad de ECR.

4. REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADO POR PARTE DE UNA ECA

La solicitud del certificado por parte de una Entidad Certificadora se realiza una vez que es autorizada a funcionar por la ATT en su calidad de ECR, luego de notificada del acto administrativo y de la firma del contrato correspondiente y previo al inicio de sus operaciones.

La ECA genera su par de claves en un dispositivo seguro de creación de firma que cumple con el estándar FIPS 140-2 nivel 3, para la PC presentada, completa la solicitud de emisión del correspondiente en un archivo electrónico que contiene el requerimiento de firma de certificado (CSR- *Certificate Signing Request*) en formato PKCS#10, en presencia del personal de la ECR que la ATT en su calidad de ECR designe en las instalaciones de la ECA. La ECA demuestra que se encuentra en poder de la clave privada correspondiente a la clave pública contenida en el CSR, mediante la firma de dicho archivo utilizando esa clave privada.

I-LP-15466

Luego, la ECA presenta la solicitud de emisión de certificado a la ATT en su calidad de ECR acompañando nota firmada por su responsable o máxima autoridad, apoderado o representante según sea el caso.

Cumplidas las tareas precedentes, el personal de la ATT designado al efecto procederá a verificar la autenticidad del requerimiento de firma de certificado (CSR).

4.2. EMISIÓN DEL CERTIFICADO A UNA ECA

La emisión del certificado de la ECA que haya realizado la correspondiente solicitud se realiza en dependencias físicas de la ECR, en recintos específicos, con los niveles de seguridad adecuados, con personal de la ATT y en presencia de integrantes de la ECA solicitante designadas al efecto por la máxima autoridad, representante o apoderado de dicha entidad.

La validez del certificado que emite la ECR a la ECA es de diez (10) años contados desde la fecha de su emisión hasta la fecha de expiración, siempre que no sea revocado.

La autorización que la ATT en su calidad de ECR aprueba para funcionar como ECA es de cinco (5) años, razón por la cual, si la ECA no renovara su autorización de funcionamiento en los periodos establecidos, la ATT en su calidad de ECR podrá revocar su certificado, teniendo en cuenta lo establecido en el punto 4.7 Renovación de un certificado. El certificado revocado lo invalida para emitir certificados digitales nuevos y su CRL.

El certificado emitido por la ECR contiene un número único de serie que identifica al certificado, responde al formato establecido por los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, estándares internacionales y contiene la información necesaria para la verificación de la ATT en su calidad de ECR y la identificación de la presente política.

4.3. ACEPTACIÓN DEL CERTIFICADO

La aceptación del certificado que fue solicitado y generado de acuerdo a los párrafos precedentes por parte de la ECR está dada cuando se formalice su recepción por la autoridad de máximo nivel jerárquico, del representante autorizado, apoderado de la ECA o a quien sea designado para el acto. Luego dicho certificado debe ser instalado por la ECA en el equipo destinado a la generación de sus propios certificados para la política que se solicitó ese certificado.

La ATT en su calidad de ECR luego de entregado y con la constancia de la recepción del citado certificado, publicará en su sitio web el certificado de manera permanente durante todo su periodo de validez y en un medio de comunicación nacional oficial de Bolivia por un (1) día. En el momento de la publicación se considera que la ECA se encuentra en plenas condiciones de operación.

4.4. USO DE LOS CERTIFICADOS Y DEL PAR DE CLAVES

El certificado emitido por la ECR para las ECA se utilizará para la firma digital de los certificados que las ECA emitan y de sus correspondientes CRL. Las claves correspondientes a dichos certificados deben ser utilizadas durante su periodo de vigencia y mientras no se encuentren revocadas. Para las ECA luego de su aceptación a la ECR, no se permitirán otros usos para el certificado y sus claves que los previstos en esta Política de Certificación.

I-LP-15466

4.5. REVOCACIÓN DEL CERTIFICADO DE UNA ECA

La solicitud de revocación del certificado de una ECA deberá ser realizada en todos los casos por una de las siguientes personas: la autoridad con máximo nivel jerárquico de la ECA, las personas que cuenten con formal y debida autorización por parte de la ECA para efectuar dicha solicitud, la ATT en su calidad de ECR o una autoridad judicial competente conforme a Ley. La presentación debe realizarse por escrito con nota dirigida a la ATT en su calidad de ECR e incluir toda la información necesaria para cumplir con el proceso, que permita validar la identidad de quien se presenta y su autorización para solicitar la revocación y la identificación del certificado a revocar así como los motivos que originan la solicitud.

La revocación de un certificado de ECA se realiza a partir de la recepción de la solicitud de revocación y termina cuando el número de serie de ese certificado es incluido en una nueva CRL y ésta se publica.

Asimismo, la ATT en su calidad de ECR podrá revocar la autorización para la prestación de servicios de certificación digital otorgada a favor de la ECA, por las siguientes causales, de acuerdo al artículo 50 del Decreto Supremo N° 1793 y su modificación aprobada mediante Decreto Supremo N° 3257 de 11 de abril de 2018:

a) Cuando la ECA transfiera, ceda, arriende o realice cualquier acto de disposición de su autorización para prestación de servicios de certificación digital, sin contar con la autorización expresa de la ATT en su calidad de ECR;
b) Por petición expresa de la ECA;
c) Por quiebra legalmente declarada de la ECA;
d) Cuando la ECA no haya iniciado la provisión de servicios a los solicitantes durante los doce (12) meses posteriores al otorgamiento de la autorización para prestación de servicios de certificación digital;
e) Cuando la entidad certificadora preste un servicio distinto o modifique el objeto para el cual obtuvo la autorización, sin permiso de la ATT en su calidad de ECR;
f) Cuando la ECA, luego de haber recibido una notificación de la ATT en su calidad de ECR, sobre el incumplimiento de disposiciones contractuales, legales, técnicas y reglamentarias, no las corrija o subsane en los plazos que señale el contrato o la normativa aplicable;
g) En caso que la ECA incumpla el pago del derecho por la prestación de servicios de certificación digital;
h) Por incurrir en cualquier otra causal establecida en su contrato.

Recibida la solicitud o ante decisión fundada, la ATT en su calidad de ECR validará los datos contenidos en la nota de solicitud de revocación o de los datos incluidos en la decisión y si procede, realizará la revocación del certificado en un plazo no mayor a veinticuatro (24) horas, registrando toda la actividad. La documentación generada se guardará por 5 años.

La revocación del certificado digital no exime a la ECA del cumplimiento de las obligaciones contraídas durante la vigencia de su certificado.

El trámite de solicitud de revocación tendrá un plazo máximo entre su inicio y la actualización de la CRL de veinticuatro (24) horas. Se indicarán asimismo los motivos por los que se realiza tal solicitud.

I-LP-15466

En caso de revocatoria de una autorización de una ECA, la misma deberá comunicar inmediatamente a los titulares de certificados digitales esta situación para el traspaso de los certificados digitales a otra ECA, cumpliéndose lo indicado en el punto 5.8 de esta política.

4.6. SUSPENSIÓN Y REEMISIÓN DE LAS CLAVES DE UN CERTIFICADO DE ECA

No se contempla el estado de suspensión para un certificado emitido a una ECA.

4.7. RENOVACIÓN DE UN CERTIFICADO DE ECA

La renovación de un certificado de una ECA se realiza con el fin de que esta entidad pueda continuar operando luego de expirado su periodo de vigencia.

Adicionalmente al fin de la vigencia del certificado, las causas de renovación pueden darse ante la modificación de la información contenida en el Certificado o cuando se realicen cambios que lo ameriten en la política asociada al certificado.

La renovación de un certificado de ECA implica en todos los casos el cambio de claves, y el procedimiento a seguir es idéntico al descrito para la emisión, realizándose una nueva ceremonia de emisión de certificado.

La solicitud de renovación de un certificado de ECA, deberá realizarse con los siguientes plazos de anticipación:

- Cuando la ECA emita certificados de persona natural o jurídica, tres (3) años y seis (6) meses, antes de la fecha de finalización de vigencia de su certificado. Si la ECA emitiera los tipos de certificados previstos, se tomará el plazo mayor de anticipación.

Esta previsión se realiza porque una entidad certificadora no puede emitir un certificado con una fecha de finalización de vigencia que supere a la fecha de finalización de vigencia de certificado de la misma ECA. Por lo tanto, una ECA cuyo certificado tiene una vigencia de cinco (5) años, pasado los dos años, por ejemplo, no podrá emitir un certificado digital a una persona natural que tiene una vigencia de 3 años, porque la fecha de finalización de la vigencia del certificado de la persona natural sería posterior al de la fecha de finalización de vigencia del certificado de la ECA que se lo emite.

La clave privada asociada al certificado que se renovará debe conservarse para firmar las CRL hasta la fecha de expiración del último certificado emitido por la ECA con ese certificado. En ese momento, solicitará a la ECR la revocación de su certificado de ECA y destruirá la clave privada.

Se aclara que en el caso en que el certificado de la ECA efectivamente fuera a expirar en un plazo menor al de vigencia de los certificados que emite, de continuar con sus servicios, deberá solicitar un nuevo certificado a la ECR con la debida antelación. Esta previsión debe realizarse teniendo en cuenta los plazos previstos para la tramitación vinculada a la renovación de un certificado por parte de la ECR.

4.8. SERVICIO DE ESTADO DE LOS CERTIFICADOS.

La ECR pone a disposición pública el acceso a la Lista de Certificados Revocados (CRL) para la verificación del estado de los certificados digitales que emite a las ECA. La autoría y validez de las CRL

I-LP-15466

también deben verificarse mediante la validación de la firma incluyendo la verificación del respectivo periodo de vigencia.

4.9. REEMISIÓN DE LAS CLAVES DE UN CERTIFICADO.

La reemisión de un certificado no está contemplada en la normativa de la INCD y no se permite para las ECA ni en ningún otro caso. La nueva emisión de un certificado no se prevé, la solicitud deberá realizarse por un nuevo certificado de acuerdo al punto 4.2.

4.10. FIN DE SUSCRIPCIÓN

Se considera suscriptor o signatario al titular de un certificado digital durante el periodo de validez del mismo. La finalización de esa condición para una ECA se da por la finalización del periodo de vigencia del certificado digital o por su revocación y cuando la ECA no haya renovado su certificado digital.
Las consecuencias del fin de la suscripción de una ECA como signatario son las que corresponden a las consecuencias por la expiración o revocación de su certificado.
Una ECA que ha finalizado su condición de suscriptor no podrá emitir certificados ni firmar CRL digitalmente.

4.11. ALMACENAMIENTO Y RECUPERACIÓN DE LAS CLAVES

En el caso de la ECR, el almacenamiento y resguardo de las claves se realiza en un dispositivo seguro que cuenta con la certificación de NIST FIPS 140-2 nivel 3 con nivel de seguridad ALTA de acuerdo a los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, garantizando su confidencialidad, integridad y disponibilidad. Asimismo, la ATT en su calidad de ECR mantiene un respaldo de las claves de la ECR a fin de continuar con las operaciones y de acuerdo a su Política de Recuperación ante Desastres.

4.12. EMISIÓN, PUBLICACIÓN Y FRECUENCIA DE LA CRL

La CRL de la ECR es emitida cada vez que se revoca un certificado, por razones operativas o a los seis (6) meses de la última emisión de CRL y será publicada por la ATT en su calidad de ECR inmediatamente después de su emisión.

Las ECA deberán verificar la autenticidad de la validez de la CRL mediante la verificación de la firma de la CRL y su periodo de validez.

La ATT en su calidad de ECR garantiza el acceso a la CRL de la ECR de manera permanente, gratuita y actualizada de acuerdo a la presente política.

5. CONTROLES OPERACIONALES O DE GESTIÓN

5.1. CONTROLES DE SEGURIDAD FÍSICA

La ATT en su calidad de ECR ha desarrollado controles adecuados para los espacios en los que se realiza las actividades de certificación de la ECR.

I-LP-15466

La infraestructura tecnológica de la ECR se encuentra en una ubicación física señalizada identificando los perímetros de acuerdo a los distintos niveles de seguridad requeridos, con los correspondientes controles de acceso a los recintos. Toda entrada y salida del personal es registrada con la respectiva autorización cuando corresponda, así como la indicación del motivo, la fecha y la hora de ocurrencia, extremando los controles para evitar el acceso a personas no autorizadas.

La ECR adopta las medidas de protección física y ambiental para garantizar la seguridad de las personas, los equipos informáticos y de comunicaciones, los documentos, las claves criptográficas y la información en general relativos a los procesos de certificación digital de la ECR.

El personal que circule por las instalaciones de la ECR y en donde residen sus equipos deberá estar perfectamente identificado. Los recintos que alojen los equipos informáticos y de certificación digital cuentan con protección contra incendios e inundaciones, la ventilación adecuada, una provisión de energía asegurada y controles de humedad y temperatura, tanto en los sitios de producción como en los de contingencia.

La documentación relativa a los procesos de certificación es resguardada con los controles adecuados para la protección contra incendios, inundaciones y humedad y de accesos de terceros no autorizados ajenos a la ECR.

Los medios de almacenamiento de la información crítica cuentan con adecuada protección contra daños accidentales y a fin de impedir, detectar y prevenir su uso no autorizado o la divulgación de información que se ha clasificado como confidencial.

La eliminación de medios de almacenamientos utilizados en procesos críticos, se realiza mediante procedimientos que aseguran la eliminación completa de la información contenida en ellos.

Asimismo, se han desarrollado procedimientos para el tratamiento de los elementos descartados en los procesos críticos de la ECR con el objeto de prevenir el acceso, el uso o la divulgación de información no autorizada.

5.2. CONTROLES PROCEDIMENTALES

La ATT en su calidad de ECR ha desarrollado estrictos controles procedimentales para la protección y el resguardo de las claves criptográficas y de los equipos afectados a los procesos de certificación, de la información y documentos de la ECR, así como los controles sobre las aplicaciones y sistemas operativos.

Los controles se aplican en forma proporcional a la criticidad de la información y los recursos utilizados para gestionarla, sobre la base de las evaluaciones de riesgos realizadas.

Los procedimientos son realizados por el personal designado específicamente por la ATT de acuerdo a sus conocimientos y aptitudes y en cumplimiento de sus roles y funciones, con las siguientes pautas:

- Las actividades y procedimientos tienen asignadas responsabilidades para su cumplimiento.
- Los roles asignados para cumplir funciones críticas tienen al menos una persona como alternativa además del titular.

I-LP-15466

- Los roles asignados para el cumplimiento de las funciones críticas de la ECR se han evaluado a fin de que se realice la correcta separación de funciones.

5.3. CONTROLES DE SEGURIDAD DEL PERSONAL

El personal de la ATT que realiza tareas en los procesos de certificación digital se ha designado de acuerdo a sus conocimientos y aptitudes y en cumplimiento de sus roles y funciones formalmente.

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos a fin de que el personal reciba la adecuada instrucción desde su ingreso y de manera planificada, sobre los procedimientos operativos y de seguridad. Todo el personal es informado sobre la existencia de documentos confidenciales y las medidas necesarias para su protección, y este compromiso es documentado con el objeto de impedir el uso no autorizado de la información, evitar fallas previsibles y promover la protección de la información, los sistemas, los equipos y las comunicaciones.

El personal que desarrolla las tareas relacionadas con los procesos de certificación digital conoce los riesgos de seguridad respecto a la protección de la información, los procedimientos a cumplir en cada caso, los mecanismos de alarma y las acciones a seguir en caso de incidentes de seguridad, a fin de prevenir su ocurrencia y mitigar los efectos, si es que ocurren.

Los procedimientos de ingreso para el personal que realiza funciones vinculadas a la ECR contienen pautas para el análisis de antecedentes laborales, experiencia y responsabilidad, de acuerdo al rol a cumplir.

Cuando los procedimientos cambien o se actualicen, el personal es instruido y capacitado para su correcta implementación e intervención de los involucrados.

Todo el personal recibe sus credenciales para autenticación, así como sus dispositivos criptográficos de acuerdo al caso, para asegurar el adecuado control de acceso.

El personal que incumpla o transgreda la presente política será sancionado proporcionalmente a la falta cometida.

5.4. CONTROLES PARA EL REGISTRO DE AUDITORÍA

La ATT en su calidad de ECR mantiene registros de auditoría de los eventos vinculados a su actividad, con el fin de supervisar las tareas operativas y de seguridad que se llevan a cabo en todos los procesos de gestión del ciclo de vida de los certificados digitales y de sus servicios de publicación, dejando de este modo evidencia de las acciones realizadas u ocurridas.

Se realizan registros de eventos para su control, a fin de brindar seguridad sobre las siguientes actividades:

- La operación de la ECR, en su infraestructura tecnológica
- La gestión del ciclo de vida de las claves y de los certificados.
- El registro de eventos respecto de la información de los titulares de certificados,
- El registro de eventos de seguridad críticos.
- La operación de su servicio de publicación y la gestión de su repositorio.

I-LP-15466

Los controles implementados se realizan también con la finalidad de brindar seguridad razonable, respecto de la confidencialidad, integridad y disponibilidad de los registros de auditoría en producción y los almacenados.

Los eventos que por configuración resultaran en alertas son atendidos de manera inmediata de acuerdo a la política de gestión de incidentes.

Los registros de auditoría son accedidos sólo por personal de seguridad autorizado, por razones operativas o de seguridad.

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos para supervisar el ciclo de vida de los equipos y sus vulnerabilidades conocidas, a fin de no incurrir en el uso de equipos obsoletos o sin soporte y prevenir amenazas que aprovechen las vulnerabilidades existentes.

Los equipos informáticos y de comunicaciones se encuentran inventariados, con el registro de sus fechas de adquisición, proveedor, propietario, número de inventario y sistemas informáticos asociados. Este inventario se encuentra actualizado y es periódicamente controlado.

5.5. ARCHIVO DE REGISTROS

Los registros de los eventos sujetos a auditoría se archivan de manera completa, y confidencial, son resguardados de manera segura y pueden ser revisados de forma automática o por el personal, de acuerdo a las pautas establecidas y planificadas.

La ATT en su calidad de ECR almacena los registros de la operación de la ECR y de su gestión administrativa y aquellos registros relativos al ciclo de vida de las claves y los certificados.

Las actividades de la ECR en sus procesos de certificación digital y su propia gestión interna se registran de manera de completa y resguardan en forma segura preservándose su integridad, su confidencialidad y disponibilidad.

Los registros relacionados al ciclo de vida de las claves y los certificados se mantienen por diez (10) años asegurándose durante ese periodo su acceso para consulta y revisión.

5.6. CAMBIO DE CLAVES DEL CERTIFICADO

Para la ECR y para las ECA, el cambio de clave implica la emisión de un nuevo certificado, por lo se deberá remitir en el punto dedicado a la emisión de un nuevo certificado para la ECA.

5.7. PROCEDIMIENTO DE RECUPERACIÓN ANTE DESASTRES

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos en base a su Política interna de evaluación de riesgos, que considera escenarios de riesgo vinculados a la imposibilidad de seguir operando en el sitio principal de la ECR, por la ocurrencia de uno o varios de los siguientes eventos, sin perjuicio de otros que pudieran determinarse a futuro:

- Fallas graves del equipamiento y de los dispositivos criptográficos utilizados para el almacenamiento y la gestión de las claves privadas de la ECR que impidan su funcionamiento normal y que no puedan ser remediados con los elementos disponibles en el sitio principal.

I-LP-15466

- Fallas graves o interrupción en la alimentación eléctrica que superen el respaldo del sistema de emergencia del sitio principal.
- Fallas graves o interrupción en la conectividad que impidan la operatoria de la ECR, incluyendo la publicación de la información relativa a los certificados digitales que emite, las correspondientes políticas de certificación y la lista de Certificados Revocados, siempre que dichas fallas que excedan la capacidad de respuesta de los respaldos inmediatos disponibles en el sitio principal.
- Imposibilidad de acceso a las instalaciones de la ECR por parte del personal que lleva a cabo las operaciones de certificación digital o participa en las ceremonias de emisión o revocación de certificados digitales y listas de revocación, siempre que no sea posible su reemplazo.

La ATT en su calidad de ECR evaluará y actualizará una vez al año su política de recuperación ante desastres documentada y aprobada formalmente, que como mínimo establece:

- Las condiciones y procedimientos para la activación del plan para operar en el sitio alternativo y los procedimientos de emergencias.
- Las condiciones y procedimientos de reanudación en el sitio principal, una vez que ha cesado la contingencia.
- Un programa de mantenimiento del plan.
- Los requisitos de educación y sensibilización para el personal involucrado.
- Las responsabilidades de los actores involucrados.
- El tiempo estimado de recuperación que se considera aceptable para los procesos que se llevan a cabo en la ECR.
- Un programa de inspecciones y pruebas periódicas del plan de continuidad.
- El listado completo de personal involucrado en las actividades de contingencia, incluyendo titulares y suplentes, y sus datos de contacto actualizados, de manera de permitir su convocatoria inmediata ante la activación del plan.

Se prevé la realización de pruebas periódicas y simulacros de operaciones, que tendrán lugar con una periodicidad no inferior a una vez al año o cada vez que se registre un cambio significativo en el equipamiento o en los procesos afectados a las actividades de certificación de la ECR.

Las pruebas de contingencia serán debidamente documentadas y revisadas para posibilitar un proceso de mejora continua.

5.8. PROCEDIMIENTO DE TRANSFERENCIA DE LAS OPERACIONES DE LA ECA

No se contempla la transferencia de la ECR a otra Entidad.
La ECA que transfiera la autorización para prestación de servicios de certificación digital a otra comunicará a la ATT en su calidad de ECR, con al menos tres (3) meses de anticipación sobre el destino que dará a los certificados digitales emitidos.

I-LP-15466

5.9. PROCEDIMIENTO PARA CONCLUIR LAS OPERACIONES DE LA ECA.

La ECA posee un Plan de cese que ha sido presentado en su proceso de autorización y de acuerdo al artículo 51 del Reglamento para el Desarrollo de las TIC, Decreto Supremo N° 1793, y a los estándares técnicos normativos establecidos.
El plan de cese refiere a la finalización de las operaciones de una ECA deberá prever como mínimo lo siguiente:

- Una notificación a la ATT en su calidad de ECR con al menos noventa (90) días de anticipación, que indique los motivos, el estado de situación general de la ECA que contenga además los datos relativos a los certificados emitidos y las instalaciones de su infraestructura tecnológica;
- Comunicación del cese de la ECA de un día (1) con la publicación en un medio de comunicación escrito oficial del Estado y;
- Notificación a todos los suscriptores de su política con un plazo de sesenta (60) días antes de la finalización.

La ECA que finalice sus operaciones revocará todos los certificados emitidos que se encuentren vigentes a esa fecha y procederá a la destrucción de sus claves mediante procedimientos seguros que impidan su reconstrucción o uso con participación de personal de la ATT presente.

La documentación relativa a la emisión de certificados y validación de identidad de los suscriptores de sus certificados deberá ser transferida a la ATT en su calidad de ECR de acuerdo a los procedimientos establecidos por esa Autoridad, así como toda documentación relativa a su administración que considere relevante.

En caso de finalización de operaciones de la ECR, la ATT en su calidad de ECR deberá notificar a todas las ECA con una antelación de (90) días de anticipación y publicar tal situación con la publicación en un medio de comunicación escrito oficial del Estado por tres (3) días. La ATT en su calidad de ECR deberá resguardar de acuerdo a los procedimientos administrativos del Estado, toda la información y los documentos relativos a su gestión y a las de las Entidades Certificadoras que hubieran sido autorizadas hasta la fecha finalización de las operaciones.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. INSTALACIÓN Y GENERACIÓN DEL PAR DE CLAVES

La ATT en su calidad de ECR genera las claves de la ECR en su propia infraestructura tecnológica, con todas las medidas de seguridad. En particular, la ECR genera y almacena sus claves en un dispositivo criptográfico basado en hardware (HSM) que cuenta con la certificación de NIST FIPS 140-2 nivel 3 considerada de ALTA SEGURIDAD según los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente.

La longitud de las claves utilizadas por la ECR para la emisión y revocación de certificados y emisión de la Lista de Certificados Revocados (CRL) es de 4096 bits, generada con el algoritmo RSA.

I-LP-15466

Las ECA generan sus claves de acuerdo a lo establecido en el Manual de Ceremonias de generación de claves aprobado por la ATT en su calidad de ECR y en presencia de personal de la ATT que cumple funciones en la ECR, una vez que ya fuera autorizada formalmente.

La ECA es responsable por la generación y custodia de sus claves de acuerdo a la normativa vigente, debe crear sus claves y almacenarlas en un dispositivo seguro (HSM) que cumpla con la certificación de NIST de acuerdo a FIPS 140-2 nivel 3, con todos los controles de seguridad de sus instalaciones.

6.2. PROTECCIÓN CRIPTOGRÁFICA DE LA CLAVE PRIVADA

La debida protección de las claves de la ECR es responsabilidad de la ATT en su calidad de ECR y se resguardan a través de procedimientos y sistemas desarrollados a tal fin, incluyendo la asignación de responsabilidades para su administración, en particular, su custodia, activación segura y su destrucción, en caso de que fueran comprometidas o al término de su vida útil.

6.3. DATOS DE ACTIVACIÓN

El método de activación de la clave utilizada por la ECR se basa en el esquema de control compartido de autenticación "M de N" con M mayor a 2. Los datos necesarios para la activación se consideran confidenciales y no se exponen a terceros en ninguna circunstancia. Los responsables de su custodia mantienen un acuerdo de confidencialidad a fin de evitar su divulgación, tanto de las claves como de los procedimientos y otra información de similar tenor.

6.4. CONTROLES DE SEGURIDAD INFORMÁTICA

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos para la protección de los equipos informáticos y de comunicación y contempla procedimientos para la seguridad de la información, los sistemas y aplicaciones, para los que ha desarrollado un Plan de Seguridad que incluye una política al efecto.

Acorde a la política de seguridad establecida, la ATT en su calidad de ECR garantiza:

- La administración sobre la identificación y autenticación para el acceso a la infraestructura tecnológica de la ECR, del personal involucrado en las funciones críticas de certificación y publicación.
- La administración del personal con los controles necesarios para una adecuada separación de funciones.
- El registro de los eventos que pueden ser analizados a fin de minimizar riesgos de seguridad y prevenir amenazas conocidas.
- El resguardo de la integridad, confidencialidad y disponibilidad de los datos críticos.
- Una gestión de incidentes planificada, a fin de mitigar los efectos de los eventos no previstos que pueden amenazar la operación de la ECR.

1-LP-15466

6.5. CONTROLES DE SEGURIDAD SOBRE EL CICLO DE VIDA DE LOS SISTEMAS:

Los controles de seguridad sobre el ciclo de vida de los sistemas se basan en el cumplimiento de los procedimientos establecidos por el personal de acuerdo a la política de seguridad y en las características de seguridad determinadas para los equipos involucrados en la generación y almacenamiento de las claves, así como en las configuraciones de seguridad de los sistemas y en los equipos de gestión de la información.

6.6. SEGURIDAD DE LA RED

La operación de los servicios de certificación de la ECR se realiza fuera de línea, asegurando su protección de accesos no autorizados.
La seguridad de los servicios de publicación se basa en los controles sobre la infraestructura y su equipamiento, los controles de acceso a los servicios y equipos, así como en aquellos aplicables a los medios de almacenamiento y los sistemas informáticos asociados.

6.7. SINCRONIZACIÓN HORARIA

Los equipos y sistemas de la ECR asociados a la gestión del ciclo de vida de los certificados, así como su servicio de publicación y de repositorio toman una fuente de hora confiable, a fin de que las operaciones puedan realizarse tomando una marca de tiempo confiable. De este modo, los registros de eventos y auditorías reflejan el tiempo de manera ajustada y precisa -4 UTC Hora Boliviana.

7. PERFILES DE CERTIFICADOS Y CRL.

7.1. PERFIL DE CERTIFICADO DE LA ECR.

El siguiente perfil de certificado se corresponde con la Versión 3 del estándar X.509.

Campos y atributos	Contenido
Versión	el valor del campo es 2.
Número de Serie (serialNumber)	Número asignado por la ECR, valor hasta de 20 octetos
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre Distintivo del Emisor (Issuer DN)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166
Validez (desde, hasta) Validfrom/Valid to	[20 años] Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time).
Nombre distintivo del suscriptor (Subject DN)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
Clave Pública del suscriptor (SubjectPublic Key)	Algoritmo: RSA, Longitud: 4096 bits.
Extensiones	
Identificador de la clave del suscriptor (Suject Key Identifier)	Función Hash (SHA1) del atributo subjectPublicKey

I-LP-15466

Uso de claves (keyUsage)	digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
Políticas de Certificación (CertificatePolicies)	URI: (Archivo en formato de texto).
Restricciones Básicas (basicContraints)	CA = TRUE, pathLenConstriant = "1".
Punto de distribución de la Lista de certificados Revocados (CRL DistributionPoints)	URI: (.crl).

7.2. PERFIL DE CERTIFICADO DE ECA

El siguiente perfil de certificado se corresponde con la Versión 3 del estándar X.509.

Campos y Atributos	**Contenido**
Versión	el valor del campo es 2.
Número de Serie (serialNumber)	Número asignado por la ECR, valor hasta de 20 octetos.
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre Distintivo del Emisor (Issuer DN)	CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
Validez (desde, hasta) Validfrom/Valid to	[10 años] Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time
Nombre distintivo del suscriptor (Subject DN)	CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón Social de la Entidad Certificadora Autorizada;C = BO de acuerdo a ISO3166.
Clave Pública del suscriptor (SubjectPublic Key)	Algoritmo: RSA, Longitud: 4096 bits
Extensiones	
Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier)	Identificador de la clave pública de la ECR
Identificador de la clave del suscriptor (Suject Key Identifier)	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.
Políticas de Certificación (CertificatePolicies)	URI: (archivo en formato de texto).
Restricciones Básicas (basicContraints)	CA = TRUE, pathLenConstriant = "0".
Punto de distribución de la Lista de Certificados Revocados (cRLDistributionPoints)	URI:(.crl)
Información de Acceso a la ECA (authorityInformationAccess	URI: (.crt).

I-LP-15456

7.3. PERFIL DE LA CRL

El siguiente perfil de certificado se corresponde con la Versión 2 del estándar X.509.

Campos y atributos	Contenido
Versión	el valor del campo es 1 (corresponde a versión 2)
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre del Emisor (Issuer DN)	CN = Nombre de la Entidad Certificadora Autorizada; O = Razón Social de la Entidad Certificadora Autorizada; C = BO de acuerdo a ISO3166.
Día y hora de Vigencia (ThisUpdate)	Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
Próxima actualización (Nextupdate)	Día y hora de la próxima actualización de la CRL [seis (6) meses y cada vez que se emite o revoca un certificado] • Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
Certificados revocados (RevokedCertificate)	Contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas
Extensiones	
Identificador de la Clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo SujectPublicKey (clave pública correspondiente a la clave privada usada para firmar la Lista de Certificados Revocados).
Número de Lista de Certificados Revocados (CRL Number)	Número entero de secuencia incremental para una CRL y una Entidad Certificadora Autorizada determinadas.

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.

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

I-LP-15466

- 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.

8. ADMINISTRACIÓN DOCUMENTAL

8.1. PROCEDIMIENTO DE CAMBIO DE ESPECIFICACIONES

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos para la administración de los cambios a la presente Política de Certificación de la ECR.

8.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

La ATT en su calidad de ECR publica en su portal Web las modificaciones que pudiera sufrir la presente Política de Certificación indicando en cada caso, el texto de reemplazo y la versión completa de la nueva política, con su correspondiente identificación.

La ATT en su calidad de ECR procede de igual forma ante cambios sufridos en los términos y condiciones de gestión del ciclo de vida de los certificados de las ECA, notificándolos en todos los casos y realizando una publicación en un medio de comunicación a nivel nacional por un día.

Los cambios que se realicen a la presente política deberán ser aprobados por la ATT en su calidad de ECR, e informados a las ECA dependientes, así como su actualización.

I-LP-15466

ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA

AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES

Y TRANSPORTES – ATT

DECLARACIÓN DE PRÁCTICAS DE LA AUTORIDAD CERTIFICADORA RAÍZ DE LA INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN DIGITAL INCD

	Datos del documento
Título del documento	Declaración de Prácticas de Certificación de la Entidad Certificadora Raíz
Identificador documental	ECR-DPC
Criticidad:	Alta
Fecha	13 de noviembre de 2018
Autor	ATT
Versión	2.0
Comentario	
Publicación	Público

Noviembre 2018

1-LP-15466

CONTENIDO

I-LP-15466

I-LP-15466

I-LP-15466

1. INTRODUCCIÓN

1.1. PRESENTACIÓN

La presente Declaración de Prácticas para la emisión de certificados digitales para entidades certificadoras autorizadas es normativa complementaria a la Política de Certificación de la Entidad Certificadora Raíz-ECR, y se desarrolla en base al marco normativo vigente y para su elaboración se han tenido el RFC 3647 producido por IETF[4] y la especificación ITU-T[5] X.509.

Las entidades que requieran un certificado de la ECR deben ajustarse a los procedimientos determinados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte – ATT en la Resolución Administrativa Regulatoria vigente, la presente Declaración de Prácticas y los procedimientos dictados, aprobados y comunicados por la ATT en su rol de autoridad encargada de autorizar, regular, fiscalizar, supervisar y controlar a las Entidades Certificadoras Autorizadas en adelante ECA.

Cumplidos los procedimientos correspondientes a la autorización, la ATT en su calidad de ECR emitirá los certificados para el funcionamiento de las ECA, funcionando como máximo nivel dentro de la jerarquía de la Nacional de Certificación Digital.

El certificado de la ECR permitirá la verificación de los certificados de las ECA subordinadas para conformar la correspondiente cadena de confianza de la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia, en adelante INCDB.

La ATT en su calidad de ECR asesora y orienta con la asistencia necesaria a fin de facilitar el cumplimiento de lo establecido en la Política de Certificación de la ECR y en la presente Declaración de Prácticas de Certificación, como así también en el cumplimiento de la normativa marco de la - INCDB.

La presente Declaración de Prácticas de Certificación contiene las actividades que realiza la ATT para la operación general de la ECR, la gestión del ciclo de vida de los certificados y de su Lista de Certificados Revocados - CRL.

Este documento es complementario a la Política de Certificación y contiene los procedimientos que se han desarrollado para el cumplimiento de las tareas establecidas para la gestión de la ECR.

1.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Título del documento: "Declaración de Prácticas de Certificación de la Entidad Certificadora Raíz del Estado Plurinacional de Bolivia"

Versión: 2.0

Fecha de emisión del documento: 07/09/2018.

Fecha de la última actualización: 13/11/2018.

I-LP-15466

[4] Internet EngineeringTaskForce (IETF) (en español Grupo de Trabajo de Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, es mundialmente conocido por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

[5] Sector de Normalización de las Telecomunicaciones de la UIT (Unión Internacional de Telecomunicaciones).

LA PAZ: Calle 13 de Calacoto Nº 8260 entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-4581184 4-4581185

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

TARIJA: Calle Alejandro del Carpio Nº 720 esq. O´Connor Piso 1 Telf.: 4-644136

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

Sitio Web de Publicación: www.ecrb.att.gob.bo

Para solicitar información o aclaraciones respecto a la presente política se podrá dirigir a:

UNIDAD DE REGULACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN ADMINISTRADORA DE LA ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA – ATT.

Calle 13 de Calacoto entre Av. Costanera y Av. Los Sauces # 8260.

Teléfono: (+591)2772266.

Fax: (+591)2772299.

Dirección de correo electrónico: ecrb@att.gob.bo

1.3. PARTICIPANTES DE LA INFRAESTRUCTURA DE CERTIFICACIÓN DIGITAL DE BOLIVIA

La INCD del Estado Plurinacional de Bolivia es el conjunto de normas, estándares tecnológicos, procedimientos, equipos, redes, bases de datos y programas informáticos y dispositivos de cifrado, preparados para la generación, almacenamiento y publicación del estado, la vigencia y validez de los certificados digitales reconocidos por las ECA, de acuerdo a los establecido en el artículo 3 del D.S. 1793 del 13 de noviembre de 2013.

Los participantes de la Infraestructura antes mencionada son:

- ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte, es el organismo que asume las atribuciones, competencias, derechos y obligaciones en materia de comunicaciones, tecnologías de la información y comunicación; transporte; servicio postal en el ámbito del Ministerio de Obras Públicas, Servicios y Vivienda, y cuyas funciones específicas se encuentran en el artículo 16 dela Ley N° 164 y el artículo 36 del Decreto Supremo N° 1793.

- ECR: Entidad Certificadora Raíz de ATT, constituyendo el primer nivel dentro de la Jerarquía Nacional de Certificación Digital emite certificados a las ECA, sus funciones se establecen en el artículo 38 del Decreto Supremo N° 1793.

- ECA: Entidades Certificadoras Autorizadas, de segundo nivel subordinadas a la ECR, que cumplieron los requisitos exigidos para la autorización de prestación del servicio, emiten certificados a los signatarios finales, sus funciones se establecen en el artículo 39 del Decreto Supremo N° 1793 antes mencionado.

- AR: Agencia/Autoridad de Registro, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además, es quién se encarga de solicitar la aprobación o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para

I-LP-15466

solicitar el certificado digital. Constituyen el tercer nivel de la Jerarquía. Sus funciones se establecen en el artículo 40 del Decreto Supremo N° 1793 antes mencionado.

- Signatario: titular del certificado emitido por una EC. Para la Política de Certificación de la ECR, los signatarios serán las ECA.
- Repositorio de la ECR: sistema único que almacena los certificados y las CRL que emite la ECR y que sirve para consulta y distribución a los signatarios.
- Terceros aceptantes: es la persona natural o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente y para validar la cadena de confianza.

1.4. USO DE LOS CERTIFICADOS

La ECR emite certificados digitales para las ECA que serán a su vez utilizados en la emisión y firma de los certificados de sus respectivos signatarios y la firma de sus listas de certificados revocados (CRL), de acuerdo a las correspondientes Políticas de Certificación y en cumplimiento de la normativa vigente.

La función del certificado de la ECR es identificar a la ATT como la entidad raíz que firma los certificados digitales de las ECA. De esta manera, permite identificar a las entidades certificadoras que se encuentran autorizadas a funcionar en la INCD del Estado Plurinacional de Bolivia, completando la cadena de confianza de cualquier certificado digital emitido en dicho país.

El certificado de la ECR es auto-emitido, auto-firmado y vincula su clave pública con los datos de la ATT en su calidad de ECR, permitiendo la verificación de la validez de la firma digital de los certificados de las ECA y de todos los certificados emitidos por ellas.

La ECR almacena su clave privada en dispositivos criptográficos seguros HSM[6].

El uso de los certificados emitidos por la ECR se encuentre expresado en su Política de Certificación, prohibiéndose su empleo para cualquier otro fin.

La ECR es el punto de inicio de la confianza de la INCD, su certificado es utilizado para dar validez a las ECA mediante la emisión a su nombre de un certificado digital. Como fuera expresado más arriba, cada una de las entidades que fueron autorizadas para brindar servicios de certificación digital utilizará dicho certificado para firmar los certificados digitales que emita a sus signatarios, construyéndose a través de este encadenamiento la confianza de la INCD, basada técnicamente en la aplicación de estándares reconocidos internacionales.

La verificación de una firma digital se realiza validando que se ha utilizado un certificado emitido por una ECA perteneciente a la INCDB y al mismo tiempo se debe controlar que se ha realizado durante el periodo de vigencia de ese certificado y que no se encuentre revocado. La verificación de la validez del certificado se realiza mediante la consulta de su estado a la CRL en la fecha de la firma. Asimismo, se debe corroborar que la CRL se encuentra firmada por la ECR para garantizar su integridad y origen.

I-LP-15466

[6] El HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege claves y llaves criptográficas.

1.5. ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

La Declaración de Prácticas de Certificación es administrada por la ATT en su calidad de ECR y se han desarrollado procedimientos para efectuar cualquier modificación o actualización.

Esta Declaración se encuentra disponible en su sitio web en forma permanente en sus versiones anteriores como la vigente, todas ellas claramente identificadas.

1.6. PROCEDIMIENTO DE APROBACIÓN.

Este documento se actualizará cada vez que la ATT en su calidad de ECR considere que debe realizarse una mejora o corrección, con un sistema de versionado que permita identificar cada documento, el motivo que originó la modificación, el responsable de la misma y la fecha. El documento será publicado de manera completa en cada oportunidad.

Los cambios realizados al presente documento se comunicarán a las ECA de manera anticipada.

1.7. DEFINICIONES Y ABREVIATURAS

INCD: Infraestructura Nacional de Certificación Digital

EC: Entidad de Certificación o Entidad Certificadora

ECR: Entidad Certificadora Raíz

ECA: Entidad Certificadora Autorizada

ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes

AR: Agencia de Registro

CRL: (*CertificationRevocationList*) Lista de Certificados Revocados

OID: (*ObjectIdentifier*) Identificador de Objeto

PC: Política de Certificación

DPC: Declaración de Prácticas de Certificación.

DN: (*Distinguishedname*) Nombre distintivo

CSR :(*CertificateSigningRequest)* Requerimiento de firma de certificado

HSM:.(*Hardware Security Module*) Dispositivo criptográfico basado en hardware

NIST: *(NationalInstitue of Standards and Tecnhnology*) Instituto Nacional de Estándares y Tecnología.

FIPS: (*Federal Information Proccessing Standards*) Estándares Federales de Procesamiento de la Información.

PKCS#10: Los formatos PKCS son formatos estándares de criptografía de clave pública, en particular, el número #10, describe el formato del mensaje con el que se solicita la emisión de un certificado. Contiene generalmente los datos de la identidad del solicitante y su clave pública.

I-LP-15466

2. PUBLICACIÓN DE LA INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.

2.1. REPOSITORIO

El repositorio de la ECR contiene las Políticas de las ECA, los actos o resoluciones por las que éstas fueron autorizadas, sus certificados digitales, sus datos de contacto y toda otra información relativa a dichas entidades que considere relevante aprobada por la ATT en su calidad de ECR.

Asimismo, y de acuerdo a la normativa vigente, publica:

- Los procedimientos de certificación digital
- Los procedimientos de reclamos
- Los términos y condiciones de servicios para la provisión de servicios de firma y certificación digital.
- La normativa aplicable y demás reglamentación que se dicte en materia de certificación digital.

El repositorio es responsabilidad de la ATT en su calidad de ECR, en cuanto a su seguridad, administración y operación, de acuerdo a sus políticas y procedimientos internos.

2.2. PUBLICACIÓN

Es responsabilidad de ATT en su calidad de ECR, la publicación permanente y actualizada en su repositorio en el sitio web institucional, de su Política de Certificación, su certificado digital, su Declaración de Prácticas de Certificación, su CRL, y toda documentación que considere de relevancia para el cumplimiento de su misión y que asista a los participantes en el uso de los certificados.

Las publicaciones de la ECR se encuentran en el sitio web:

URL: www.ecrb.att.gob.bo

2.3. FRECUENCIA DE PUBLICACIÓN

La CRL será actualizada y publicada cuando se produzca la revocación o emisión de un certificado, o bien a los 6 meses de la última emisión de CRL.

Los procedimientos se publicarán en sus versiones vigentes y actualizadas cada vez que surjan modificaciones.

Toda la documentación deberá estar actualizada y con la identificación correspondiente y accesible de manera permanente para los usuarios en el sitio web institucional.

2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS

Los controles generales de seguridad sobre el repositorio de la ECR se realizan de manera de asegurar la confidencialidad, la disponibilidad e integridad de la información y los sistemas asociados.

El repositorio se encuentra disponible para consulta del público las veinticuatro (24) horas, los siete (7) días de la semana y su mantenimiento se realiza de acuerdo a un calendario programado.

1-LP-15466

2.5. DIVULGACIÓN DE INFORMACIÓN

Los documentos y la información obtenida por la ECR de los solicitantes de autorización para constituirse en una ECA recibidos por la ATT en su calidad de ECR, se mantendrán con carácter de confidencial por razones de seguridad y no serán divulgados, excepto aquellos de carácter público como su denominación, razón social o comercial y su carácter de solicitante.

La ECR mantiene con carácter confidencial la información suministrada por los titulares de certificados digitales, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso.

En estos casos, el solicitante debe enviar una nota que permita validar la identida de quien la presenta, su autoridad o calidad para solicitar la información y la identificación precisa y detallada de la información solicitada, así como los motivos que la originan.

3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1. REGISTROS DE NOMBRES

La identificación de las Entidades Certificadoras es realizada por la ATT en su calidad de ECR durante el proceso que autoriza su funcionamiento, luego de realizar las revisiones de la documentación y de la infraestructura tecnológica de acuerdo a la reglamentación vigente, verificando su estricto cumplimento.

La ATT en su calidad de ECR, mediante la firma de un contrato con la ECA, otorgará la autorización para la prestación de servicios de certificación digital, con una vigencia de cinco (5) años, renovables por periodos similares, a personas jurídicas de derecho público o privado que así lo soliciten.

El certificado emitido vincula la Política de Certificación, los datos de la ECA y su clave pública. Para confirmar estos datos, previo a la emisión del certificado, la ECA verifica que la información contenida en la solicitud del certificado sea correcta.

Los certificados emitidos por la ECR tienen un nombre distintivo (DN) único en el campo *Subject* que es elegido por la ECA para su identificación en la INCD de Bolivia. Este nombre debe ser único y de fácil comprensión, de acuerdo a la siguiente definición: CN (CommonName) = Denominación de la Entidad Certificadora Autorizada; O (Organization) = Razón Social de la Entidad Certificadora Autorizada; C = BO (estándar de acuerdo a ISO3166).

3.2. VALIDACIÓN DE LA IDENTIDAD INICIAL

La información remitida por las ECA para su identificación se considera confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida en causa judicial por un juez competente o se trate de información pública.

Durante el proceso de autorización de Entidades Certificadoras y en particular, en el análisis de los requisitos legales, se realiza el procedimiento de validación de identidad del solicitante. Una vez autorizada, la ECA se encuentra en condiciones de solicitar su certificado, siendo titular de la correspondiente licencia.

Los procedimientos llevados a cabo por la ECR para la gestión del ciclo de vida de sus certificados se registran y refrendan de manera documentada por la ATT en su calidad de ECR.

I-LP-15466

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN.

Para solicitar una renovación, una ECA deberá enviar una nota con la debida anticipación enumerando lo motivos por los que se solicita el trámite, el estado de operación de la ECA, los informes de Auditoría si

correspondiera y la firma de una autoridad habilitada para la solicitud. La ATT en su calidad de ECR deberá realizar la constatación respecto de la Autoridad que realiza la solicitud a fin de corroborar que el firmante tiene la facultad de realizar tal requerimiento y que es quien dice ser.

Luego del análisis correspondiente, la ATT en su calidad de ECR indicará a la ECR que debe proceder a la emisión de un nuevo certificado para la ECA. En estos casos siempre corresponderá la emisión de uno nuevo, con una nueva clave pública, y a partir de la generación de un nuevo par de claves criptográficas.

4. CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD Y TRAMITACIÓN DEL CERTIFICADO POR PARTE DE UNA ECA

La solicitud del certificado por parte de una ECA se realiza una vez que ha cumplido todos los requisitos establecidos y es autorizada a funcionar por la ATT en su calidad de ECR, luego de notificada del acto administrativo y de la firma del contrato correspondiente y previo al inicio de sus operaciones.

La ECA genera su par de claves en un dispositivo seguro de creación de firma, para la PC presentada, completa la solicitud de emisión correspondiente en un archivo electrónico que contiene el requerimiento de firma de certificado (CSR- *Certificate Signing Request*) en formato PKCS#10, en presencia del personal de la ECR que la ATT en su calidad de ECR designe en las instalaciones de la ECA. La ECA demuestra que se encuentra en poder de la clave privada correspondiente a la clave pública contenida en el CSR, mediante la firma de dicho archivo utilizando esa clave privada.

La ECA presenta la solicitud de emisión de certificado a la ATT en su calidad de ECR acompañando nota firmada por su responsable o máxima autoridad, apoderado o representante según sea el caso.

Presentada la solicitud de emisión, la ECR la procesa y procede a darle trámite, siempre que se haya cumplido con las condiciones antes mencionadas en los tiempos y formas establecidos por la ATT en su calidad de ECR, procediendo a notificar a la ECA, si éstas condiciones no fueran satisfechas.

En caso de cumplir todas las condiciones establecidas, la ECR procederá a la emisión del correspondiente certificado. Caso contrario, la solicitud es rechazada y se procede a notificar a la ECA, de los incumplimientos en los que hubiera incurrido, concediéndole un plazo para su rectificación o denegando definitivamente la solicitud.

4.2. EMISIÓN DEL CERTIFICADO

Cumplidas las tareas precedentes, el personal de la ATT designado al efecto procederá a verificar la autenticidad del requerimiento de firma de certificado (CSR).

La emisión del certificado de la ECA que haya realizado la correspondiente solicitud se realiza en dependencias definidas por la ECR, en recintos específicos, con los niveles de seguridad adecuados, con personal de la ATT y en presencia de personal de la ECA solicitante designadas al efecto por la máxima autoridad, representante o apoderado de dicha entidad.

La validez del certificado que emite la ECR a la ECA es de diez (10) años contados desde la fecha de su emisión hasta la fecha de expiración, siempre que no sea revocado.

La autorización que proporciona la ATT en su calidad de ECR para funcionar como ECA es de cinco (5) años, razón por la cual, si la ECA no renovara su autorización de funcionamiento en los periodos establecidos, ATT en su calidad de ECR podrá revocar su certificado, teniendo en cuento lo establecido

I-LP-15466

en el punto "4.6 Renovación de un certificado". El certificado revocado lo invalida para emitir certificados digitales nuevos y su CRL.

El certificado emitido por la ECR contiene un número único de serie que identifica al certificado, responde al formato establecido en los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente y a estándares internacionales, contiene la información necesaria para la verificación de la ATT en su calidad de ECR y la identificación de la presente Declaración de Prácticas de Certificación.

4.3. ACEPTACIÓN DEL CERTIFICADO

La aceptación del certificado que fue solicitado y generado de acuerdo a los párrafos precedentes por parte de la ECR está dada cuando se formalice su recepción por la autoridad de máximo nivel jerárquico, del representante autorizado o apoderado de la ECA o a quien se ha designado para el acto. Luego dicho certificado debe ser instalado por la ECA en el equipo destinado a la generación de sus propios certificados para la PC que se solicitó ese certificado.

La ATT en su calidad de ECR luego de entregado y con la constancia de la recepción del citado certificado, publicará en su sitio web el certificado de manera permanente durante todo su periodo de validez y con la publicación en un medio de comunicación escrito oficial a nivel nacional por un (1) día. En el momento de la publicación se considera que la ECA se encuentra en plenas condiciones de operación.

4.4. REVOCACIÓN DEL CERTIFICADO DE UNA ECA

La solicitud de revocación deberá ser realizada en todos los casos por una de las siguientes personas: la autoridad con máximo nivel jerárquico de la ECA, las personas que se cuenten con formal y debida autorización por parte de la ECA para efectuar dicha solicitud, la ATT en su calidad de ECR o una autoridad judicial competente conforme a Ley. La presentación debe realizarse por escrito, con nota dirigida a la ATT y deberá incluir toda la información necesaria para cumplir con el proceso que permita validar la identidad de quien se presenta, su autorización para solicitar la revocación y la identificación del certificado a revocar, así como los motivos que originan la solicitud.

La revocación de un certificado de ECA se realiza a partir de la recepción de la solicitud de revocación y termina cuando el número de serie de ese certificado es incluido en la CRL y ésta se publica.

Las causas de revocación se encuentran descriptas en la PC de la ECR.

Recibida la solicitud o ante decisión fundada, la ATT en su calidad de ECR validará los datos contenidos en la nota de solicitud de revocación o de los datos incluidos en la decisión y si procede, realizará la revocación del certificado en un plazo no mayor a veinticuatro (24) horas, registrando toda la actividad. La documentación generada se guardará por 5 años.

La revocación del certificado digital no exime a la ECA del cumplimiento de las obligaciones contraídas durante la vigencia de su certificado.

El trámite de solicitud de revocación tendrá un plazo máximo entre su inicio y la actualización de la CRL de veinticuatro (24) hora. Se indicarán asimismo los motivos por los que se realiza tal solicitud.

I-LP-15466

En caso de revocatoria de una autorización, a la ECA debe comunicar inmediatamente a los titulares de certificados digitales esta situación para el traspaso de los certificados digitales a otra ECA, cumpliéndose lo indicado en el punto 5.8 de la Política de Certificación.

4.5. USO DEL CERTIFICADO Y DEL PAR DE CLAVES.

El uso del certificado emitido por la ECR a una ECA se encuentra expresado en la Política de Certificación de la ECR. Los usos de las claves correspondientes se encuentran directamente vinculados al uso del certificado.

El certificado digital de una ECA emitido con el correspondiente certificado de la ECR es válido durante su periodo de vigencia y siempre que no haya sido revocado. La firma digital de la ECA es válida cuando se realiza con un certificado digital válido y se verifica la cadena de confianza, en este caso, deberá verificarse que el certificado digital de la ECR que firmó, también es válido, es decir, que está en su periodo de vigencia y no ha sido revocado).

Los estados de suspensión no son contemplados para los certificados de la ECR, ni para los certificados de las ECA.

4.6. RENOVACIÓN DE UN CERTIFICADO

La renovación de un certificado de una ECA se realiza con el fin de que dicha entidad pueda continuar operando luego de expirado su periodo de vigencia.

La solicitud de renovación debe realizarse por escrito con nota dirigida a la ATT en su calidad de ECR e incluir toda la información necesaria para cumplir con el proceso, que permita validar la identidad de quien se presenta, su autorización para realizar el requerimiento y la identificación del certificado a renovar.

Adicionalmente al fin de la vigencia del certificado, las causas de renovación pueden darse ante la modificación de la información contenida en el certificado o cuando se realicen cambios que lo ameriten en la Política de Certificación asociada al certificado.

La renovación de un certificado implica en todos los casos el cambio de claves, y el procedimiento a seguir es idéntico al descripto para la emisión, realizándose una nueva ceremonia de emisión de certificado.

La solicitud de renovación de un certificado de ECA, deberá realizarse con los siguientes plazos de anticipación:

- Cuando la ECA emita certificados de persona natural o jurídica, tres (3) años antes de la fecha de finalización de vigencia de su certificado

Si la ECA emitiera los tipos de certificados previstos, se tomará el plazo mayor de anticipación.

Esta previsión se realiza porque una entidad certificadora no puede emitir un certificado con una fecha de finalización de vigencia que supere a la fecha de finalización de vigencia de certificado. Por lo tanto una ECA, cuya certificado tiene una vigencia de cinco (5) años, pasado los dos años, por ejemplo, no podrá emitir un certificado digital a una persona natural que tiene una vigencia de 3 años, porque la fecha de finalización de la vigencia del certificado de la persona natural sería posterior al de la fecha de finalización de vigencia del certificado de la ECA que se lo emite.

I-LP-15466

La clave privada asociada al certificado que se renovará debe conservarse para firmar las CRL hasta la fecha de expiración del último certificado emitido por la ECA con ese certificado. En ese momento, solicitará a la ECR la revocación de su certificado de ECA y se destruirá la clave privada.

Se aclara que en el caso en que el certificado de la ECA efectivamente fuera a expirar en un plazo menor al de vigencia de los certificados que emite, de continuar con sus servicios, deberá solicitar un nuevo certificado a la ECR con la debida antelación. Esta previsión debe realizarse teniendo en cuenta los plazos previstos para la tramitación vinculada a la renovación de un certificado por parte de la ECR.

4.7. CAMBIO DE CLAVES DEL CERTIFICADO

Un cambio de claves en todos los casos que se refiera a una ECA, requerirá la emisión de un nuevo certificado por parte de la ECR, debiendo la ECA solicitar una renovación o solicitud de nuevo certificado, según corresponda.

4.8. MODIFICACIÓN DEL CERTIFICADO

El certificado de una ECA puede ser modificado, hasta tanto el mismo no se haya aceptado formalmente. Después de la aceptación, sólo puede ser revocado si se requiere una modificación.

4.9. SUSPENSIÓN Y REEMISIÓN DE LAS CLAVES DE UN CERTIFICADO DE ECA

No se contempla el estado de suspensión para un certificado emitido a un ECA.

4.10. SERVICIO DE ESTADO DE LOS CERTIFICADOS.

El servicio de estado del certificado informa a usuarios y terceros aceptantes el estado en el momento del uso del certificado, a fin de validar la firma o transacción.

La CRL contiene la lista de certificados revocados.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción finaliza por la expiración del certificado o cuando este se revoca, por las causas mencionadas en la Política de Certificación.

Las consecuencias del fin de la suscripción de una ECA como signatario son las que corresponden a las consecuencias por la expiración o revocación de su certificado.

Una ECA que ha finalizado su condición de suscriptor no podrá emitir certificados ni firmar CRL digitalmente.

4.12. RECUPERACIÓN DE CLAVES

No se permitirá la recuperación de la clave salvo para el caso del uso en el Plan de Recuperación ante desastres y para continuar con la operación ante una contingencia.

5. CONTROLES DE SEGURIDAD FÍSICA GESTIÓN Y DE OPERACIÓN

5.1. CONTROLES DE SEGURIDAD FÍSICA

5.1.1. UBICACIÓN Y CONSTRUCCIÓN.

La ATT ubica sus oficinas administrativas en la calle 13 de Calacoto entre Sauces y Costanera # 8260, en las que ha delimitado sus oficinas administrativas y sus equipos Asimismo ha desarrollado controles adecuados para los espacios en los que se realiza las actividades de autorización de las ECA.

I-LP-15466

Su infraestructura tecnológica esta resguardada en la bóveda del Banco Central de Bolivia donde se ha desarrollado controles adecuados para los espacios en los que se realiza las actividades de certificación de la ECR y de las ECA.

La infraestructura tecnológica de la ECR se encuentra en una ubicación física señalizada identificando los perímetros de acuerdo a los distintos niveles de seguridad requeridos, con los correspondientes controles de acceso a los recintos. Toda entrada y salida del personal es registrada con la respectiva autorización cuando corresponda, así como la indicación del motivo, la fecha y la hora de ocurrencia, extremando los controles para evitar el acceso a personas no autorizadas.

5.1.2. SEGURIDAD FÍSICA Y AMBIENTAL

La ECR adopta las medidas de protección física y ambiental para garantizar la seguridad de las personas, los equipos informáticos y de comunicaciones, los documentos, las claves criptográficas y la información en general relativos a los procesos de certificación digital de la ECR.

El personal que circule por las instalaciones de la ECR y en donde residen sus equipos deberá estar perfectamente identificado. Los recintos que alojen los equipos informáticos y de certificación digital cuentan con protección contra incendios e inundaciones, la ventilación adecuada, una provisión de energía asegurada y controles de humedad y temperatura, tanto en los sitios de producción como en los de contingencia.

La documentación relativa a los procesos de certificación es resguardada con los controles adecuados para la protección contra incendios, inundaciones y humedad y de accesos de terceros no autorizados ajenos a la ECR.

Los medios de almacenamiento de la información crítica cuentan con adecuada protección contra daños accidentales y a fin de impedir, detectar y prevenir su uso no autorizado o la divulgación de información que se ha clasificado como confidencial.

La eliminación de medios de almacenamientos utilizados en procesos críticos, se realiza mediante procedimientos que aseguran la eliminación completa de la información contenida en ellos.

Asimismo, se han desarrollado procedimientos para el tratamiento de los elementos descartados en los procesos críticos de la ECR con el objeto de prevenir el acceso, el uso o la divulgación de información no autorizada.

Se tiene control en:

a) delimitación de las áreas seguras e inseguras en las instalaciones donde se procesan o almacenan claves criptográficas y certificados;
b) medidas para impedir el acceso no autorizado a las instalaciones a través de puertas, ventanas y muros;
c) medidas de control de acceso físico que permiten identificar y autorizar a los individuos que ingresan y egresan de la organización (lectores biométricos, tarjetas de aproximación, guardias de seguridad);
d) medidas restrictivas para el acceso a las áreas seguras dentro de la organización (ingreso del mínimo personal requerido);

I-LP-15466

e) medidas de detección del acceso en áreas vacantes (sensores de movimientos, alarmas, cámaras de video);

f) medidas para el control de la temperatura del equipamiento en funcionamiento;

g) medidas de protección contra incendios (detectores de humo, extintores de polvo);

h) medidas de protección contra inundaciones (de acuerdo a la evaluación de riesgos de inundación);

i) utilización de cerraduras y racks cerrados para la protección de sistemas e información crítica

Para la protección del equipamiento de las áreas de trabajo, se implementan las siguientes medidas:

a) Inventario actualizado de los sistemas y medios de almacenamiento de la organización;

b) procedimientos para el ingreso y egreso de sistemas y medios a la organización, que requieren la aprobación explícita de los niveles gerenciales;

c) procedimientos para la destrucción física de medios de almacenamiento;

d) política de escritorios limpios, retirando de las áreas de trabajo aquella información que no esté siendo utilizada;

e) separación entre los ambientes de producción, copias de seguridad y test;

f) copias de seguridad periódicas almacenadas en instalaciones geográficamente distantes y bajo las mismas medidas de protección.

5.2. CONTROLES PROCEDIMENTALES

5.2.1. ROLES DE CONFIANZA

Los procedimientos son realizados por el personal designado específicamente por la ATT en su calidad de ECR de acuerdo a sus conocimientos y aptitudes y en cumplimiento de sus roles y funciones, con las siguientes pautas:

- Las actividades y procedimientos tienen asignadas responsabilidades para su cumplimiento.
- Los roles asignados para cumplir funciones críticas de la ECR tienen al menos una persona como alternativa además del titular.
- Los roles asignados para el cumplimiento de las críticas de la ECR se han evaluado a fin de que se realice la correcta separación de funciones.

La ATT en su calidad de ECR ha desarrollado estrictos controles procedimentales para la protección y el resguardo de las claves criptográficas y de los equipos afectados a los procesos de certificación, de la información y documentos de la ECR, así como los controles sobre las aplicaciones y sistemas operativos.

I-LP-15466

Los controles se aplican en forma proporcional a la criticidad de la información y los recursos utilizados para gestionarla, sobre la base de las evaluaciones de riesgos realizadas.

5.2.2. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada función en la ECR es cumplida de acuerdo a las asignaciones formales realizadas por la ATT en su calidad de ECR para su personal o respaldada por una contratación. En la asignación de funciones se encuentra enumeradas las tareas generales del personal. Para el ejercicio de los diferentes roles internos, la ECR brinda los medios de autenticación que aseguran la correcta identificación de su personal, resguardando en cada caso la protección de la información y la documentación propia y aquella que le fue conferida para su tratamiento.

5.3. CONTROLES DE SEGURIDAD DEL PERSONAL

5.3.1. REQUERIMIENTO DE ANTECEDENTES

El personal de la ATT que realiza tareas en los procesos de certificación digital se ha designado de acuerdo a sus antecedentes, conocimientos y aptitudes y en cumplimiento de sus roles y funciones formalmente.

La ATT en su calidad de ECR ha desarrollado procedimientos a fin de que el personal reciba la adecuada instrucción desde su ingreso y de manera planificada, sobre los procedimientos operativos y de seguridad.

Todo el personal es informado sobre la existencia de documentos confidenciales y las medidas necesarias para su protección, y este compromiso es documentado con el objeto de impedir el uso no autorizado de la información, evitar fallas previsibles y promover la protección de la información, los sistemas, los equipos y las comunicaciones. Todo el personal recibe sus credenciales para autenticación así como sus dispositivos criptográficos de acuerdo al caso, para asegurar el adecuado control de acceso.

Los procedimientos de ingreso para el personal que realiza funciones vinculadas a la ECR contienen pautas para el análisis de antecedentes laborales, experiencia y responsabilidad, de acuerdo al rol a cumplir.

Cuando los procedimientos cambien o se actualicen, el personal es instruido y capacitado para su correcta implementación e intervención de los involucrados.

5.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES.

De acuerdo a las funciones requeridas, ATT en su calidad de ECR ha elaborado perfiles para la contratación del personal que cumpla con las características requeridas. La comprobación se realiza mediante la evaluación de las hojas de vida y la presentación de sus certificaciones y títulos de grado, o postgrado, de acuerdo a las habilidades requeridas.

Asimismo, también se evaluarán antecedentes penales, de buena conducta y aquellos que se consideren pertinentes al puesto a desempeñar.

5.3.3. FORMACIÓN Y FRECUENCIA DE ACTUALIZACIÓN EN LA FORMACIÓN.

El desarrollo de las tareas de certificación digital está sometido al avance de las tecnologías de información y comunicación, por los que ATT en su calidad de ECR ha desarrollado un plan de actualización para sus integrantes que prevé la formación continua en materia de criptografía asimétrica, uso de dispositivos criptográficos, tecnología de cifrado, implementación de algoritmos de firma digital y de digestos (o hash).

I-LP-15466

La ATT en su calidad de ECR ha previsto la creación de una base de conocimientos que recopile la información sobre certificación digital en general y sobre su propio desarrollo, de manera de no perder información si uno de sus integrantes se desvincula.

5.3.4. REQUERIMIENTOS DE CONTRATACIÓN DEL PERSONAL

Anualmente la ATT en su calidad de ECR realizará una evaluación interna de su personal a fin de indicar el cumplimiento de sus objetivos, la necesidad de personal y las características o perfiles de los mismos en caso de ser necesario. Este informe puede ser realizado antes del año si se detecta la falta de un área de conocimiento específico. En todos los casos se fundamenta el requerimiento y el impacto de la falta de ese recurso.

5.3.5. CONTROLES PERIÓDICOS DE CUMPLIMIENTO.

El personal que desarrolla las tareas relacionadas con los procesos de certificación digital conoce los riesgos de seguridad respecto a la protección de la información, los procedimientos a cumplir en cada caso, los mecanismos de alarma y las acciones a seguir en caso de incidentes de seguridad, a fin de prevenir su ocurrencia y mitigar los efectos, si es que ocurren.

Anualmente se realiza un informe de cumplimiento del plan de formación, y de los procedimientos críticos regulares que hacen a la seguridad y formación del personal.

5.3.6. FINALIZACIÓN DE LOS CONTRATOS.

Una vez finalizados los contratos del personal o empresas que desarrollan funciones para la ECR, estos deberán mantener confidencialidad sobre los aspectos que hacen a la seguridad de la INCD del Estado Plurinacional de Bolivia por al menos 5 años.

Las condiciones laborales quedan fuera del alcance de esta Declaración de Prácticas de Certificación.

5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

5.4.1. TIPOS DE EVENTOS REGISTRADOS

La ATT en su calidad de ECR mantendrá los registros de auditoría de los eventos vinculados a su actividad, con el fin de supervisar las tareas operativas y de seguridad que se llevan a cabo en todos los procesos de gestión del ciclo de vida de los certificados digitales y de sus servicios de publicación, dejando de este modo evidencia de las acciones realizadas u ocurridas.

Se realizan registros de eventos para su control, a fin de brindar seguridad sobre las siguientes actividades:

- La operación de la ECR, en su infraestructura tecnológica.
- La gestión del ciclo de vida de las claves y de los certificados que emite.
- El registro de eventos respecto de la información de los titulares de certificados.
- El registro de eventos de seguridad críticos.
- La operación de su servicio de publicación y la gestión de su repositorio.

Los controles implementados se realizan también con la finalidad de brindar seguridad razonable, respecto de la confidencialidad, integridad y disponibilidad de los registros de auditoría en producción y los almacenados.

I-LP-15466

Los eventos que por configuración resultaran en alertas, son atendidos de manera inmediata de acuerdo a la política de gestión de incidentes.

Los registros de auditoría son accedidos sólo por personal de seguridad autorizado, por razones operativas o de seguridad.

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos para supervisar el ciclo de vida de los equipos y sus vulnerabilidades conocidas, a fin de no incurrir en el uso de equipos obsoletos o sin soporte y prevenir amenazas que aprovechen las vulnerabilidades existentes.

Los equipos informáticos y de comunicaciones se encuentran inventariados, con el registro de sus fechas de adquisición, proveedor, propietario, número de inventario y sistemas informáticos asociados. Este inventario se encuentra actualizado y es periódicamente controlado.

5.4.2. FRECUENCIA DEL PROCESAMIENTO DE LOG

El procesamiento de logs se realizar automáticamente y de acuerdo a las pautas establecidas en la Política de Seguridad de la ECR.

Las alertas que surgen del procesamiento de logs se atienden a través del sistema de gestión de incidentes y de acuerdo a las reglas establecidas.

5.4.3. REQUERIMIENTO DE AUDITORIA

Los log de auditoría, así como los registros de eventos y seguridad se resguardan para ser evidencia de auditoría cuando ésta los requiera. La ATT en su calidad de ECR realiza el resguardo de log de acuerdo al sistema del que se trate y los eventos determinados.

Los procedimientos de registros de logs, se encuentran detallados en la documentación interna de la entidad. La ATT en su calidad de ECR toma las previsiones para su resguardo respecto de la información crítica y define plazos para el resto de los registros de eventos de acuerdo a los sistemas implicados.

Las actividades (borrado, modificación, compresión, copias de seguridad, etc.) sobre los registros de auditoría y de los registros de eventos y de seguridad se registran en actas y se resguardan en un área segura.

5.4.4. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades se encuentra previsto en la Política de Seguridad de la ECR.

5.5. ARCHIVO DE INFORMACIÓN Y REGISTROS

Los registros de los eventos sujetos a auditoría se archivan de manera completa, y confidencial, son resguardados de manera segura y pueden ser revisados de forma automática o por el personal, de acuerdo a las pautas establecidas y planificadas.

La ATT en su calidad de ECR almacena los registros de la operación de la ECR y de su gestión administrativa y aquellos registros relativos al ciclo de vida de las claves y los certificados.

Las actividades de la ECR en sus procesos de certificación digital y su propia gestión interna se registran de manera de completa y resguardan en forma segura, preservándose su integridad, su confidencialidad y disponibilidad.

Los registros relacionados al ciclo de vida de las claves y los certificados se mantienen por diez (10) años, asegurándose durante ese periodo su acceso para consulta y revisión.

I-LP-15466

5.6. CAMBIO DE CLAVES DEL CERTIFICADO

Para la ECR y las ECA, el cambio de clave implica la emisión de un nuevo certificado, por lo se deberá seguir los pasos indicados en el punto referido a la emisión de un nuevo certificado para la ECA.

5.7. PROCEDIMIENTO DE RECUPERACIÓN DE LA CLAVE DE LA EC

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos que considera escenarios de riesgo vinculados a la imposibilidad de seguir operando en el sitio principal de la ECR, por la ocurrencia de uno o varios de los siguientes eventos, sin perjuicio de otros que pudieran determinarse a futuro:

- Fallas graves del equipamiento y de los dispositivos criptográficos utilizados para el almacenamiento y la gestión de las claves privadas de la ECR que impidan su funcionamiento normal y que no puedan ser remediados con los elementos disponibles en el sitio principal.
- Fallas grave o interrupción en la alimentación eléctrica que superen el respaldo del sistema de emergencia del sitio principal.
- Fallas graves o interrupción en la conectividad que impidan la operatoria de la ECR, incluyendo la publicación de la información relativa a los certificados digitales que emite, las correspondientes políticas de certificación y la lista de Certificados Revocados, siempre que dichas fallas que excedan la capacidad de respuesta de los respaldos inmediatos disponibles en el sitio principal.
- Imposibilidad de acceso a las instalaciones de la ECR por parte del personal que lleva a cabo las operaciones de certificación digital o participa en las ceremonias de emisión o revocación de certificados digitales y listas de revocación, siempre que no sea posible su reemplazo.

La ATT en su calidad de ECR dispone de un plan de recuperación ante desastres documentado y aprobado formalmente, que como mínimo establece:

- Las condiciones y procedimientos para la activación del plan para operar y los procedimientos de emergencias
- Las condiciones y procedimientos de reanudación en el sitio principal, una vez que ha cesado la contingencia
- Un programa de mantenimiento del plan
- Los requisitos de educación y sensibilización para el personal involucrado
- Las responsabilidades de los actores involucrados
- El tiempo estimado de recuperación que se considera aceptable para los procesos que se llevan a cabo en la ECR
- Un programa de inspecciones y pruebas periódicas del plan
- El listado completo de personal involucrado en las actividades de contingencia, incluyendo titulares y suplentes, y sus datos de contacto actualizados, de manera de permitir su convocatoria inmediata ante la activación del plan

Se prevé la realización de pruebas periódicas y simulacros de transferencia de operaciones al sitio alternativo, que tendrán lugar con una periodicidad no inferior a una vez al año o cada vez que se registre un cambio significativo en el equipamiento o en los procesos afectados a las actividades de certificación de la ECR.

Las pruebas de contingencia serán debidamente documentadas y revisadas para posibilitar un proceso de mejora continua.

I-LP-15466

5.8. TRANSFERENCIA DE UNA EC

No se contempla la transferencia de la ECR a otra Entidad.

La ECA que transfiera la autorización para prestación de servicios de certificación digital a otra comunicará a la ATT en su calidad de ECR, con al menos tres (3) meses de anticipación sobre el destino que dará a los certificados digitales emitidos, y deberá presentar un plan de transferencia con una descripción respecto de las condiciones de transferencia de las operaciones de certificación para revisión de la ATT en su calidad de ECR.

5.9. CESE DE ACTIVIDADES DE LA EC

Las ECA poseen un Plan de Cese que ha sido presentado en su proceso de autorización y de acuerdo al artículo 51 del Reglamento para el Desarrollo de las TIC, Decreto Supremos N° 1793, y a los estándares técnicos normativos establecidos.

El plan de cese refiere a la finalización de las operaciones de una ECA deberá prever como mínimo lo siguiente:

- Una notificación a la ATT con al menos noventa (90) días de anticipación, que indique los motivos, el estado de situación general de la ECA que contenga además los datos relativos a los certificados emitidos y las instalaciones de su infraestructura tecnológica.
- La publicación del cese de la ECA por un (1) día en un medio de comunicación escrito oficial del Estado y,
- La notificación a todos los suscriptores de su PC con un plazo de sesenta (60) días antes de la finalización.

La ECA que finalice sus operaciones revocará todos los certificados emitidos que se encuentren vigentes a esa fecha y procederá a la destrucción de sus claves mediante procedimientos seguros que impidan su reconstrucción o uso.

La documentación relativa a la emisión de certificados y validación de identidad de los suscriptores de sus certificados deberá ser transferida a la ATT en su calidad de ECR de acuerdo a los procedimientos establecidos por esa Autoridad, así como toda documentación relativa a su administración que considere relevante.

En caso de finalización de operaciones de la ECR, la ATT en su calidad de ECR deberá notificar a todas las ECA con una antelación de (90) días de anticipación y publicar tal situación en la publicación oficial del Estado por tres (3) días. La ATT en su calidad de ECR deberá resguardar de acuerdo a los procedimientos administrativos del Estado, toda la información y los documentos relativos a su gestión y a las de las Entidades Certificadoras que hubieran sido autorizadas hasta la fecha finalización de las operaciones.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

La ATT en su calidad de ECR genera las claves de la ECR en su propia infraestructura tecnológica, con todas las medidas de seguridad. En particular, la ECR genera y almacena sus claves en un dispositivo

I-LP-15466

criptográfico basado en hardware (HSM) que cuenta con la certificación de NIST FIPS 140-2 nivel 3 considerada de ALTA SEGURIDAD según Resolución Administrativa de la ATT.

La longitud de las claves utilizadas por la ECR para la emisión y revocación de certificados y emisión de la CRL es de 4096 bits, generada con el algoritmo RSA.

Las ECA generan sus claves de acuerdo a lo establecido en el Manual de Ceremonias de generación de claves aprobado por la ATT en su calidad de ECR y en presencia de personal de la ATT que cumple funciones en la ECR, una vez que ya fuera autorizada formalmente.

La ECA es responsable por la generación y custodia de sus claves de acuerdo a la normativa vigente, debe crear sus claves y almacenarlas en un dispositivo seguro (HSM) que cumpla con la certificación de NIST de acuerdo a FIPS 140-2 nivel 3, con todos los controles de seguridad de sus instalaciones.

6.2. PROTECCIÓN CRIPTOGRÁFICA DE LA CLAVE PRIVADA

La debida protección de las claves de la ECR es responsabilidad de la ATT en su calidad de ECR y se reguardan a través de procedimientos y sistemas desarrollados a tal fin, incluyendo la asignación de responsabilidades para su administración, en particular, su custodia, activación segura y su destrucción, en caso de que fueran comprometidas o al término de su vida útil.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

No aplicable.

6.4. DATOS DE ACTIVACIÓN

El método de activación de la clave utilizada por la ECR se basa en el esquema de control compartido de autenticación "M de N", con M mayor a 2. Los datos necesarios para la activación se consideran confidenciales y no se exponen a terceros en ninguna circunstancia. Los responsables de su custodia mantienen un acuerdo de confidencialidad a fin de evitar su divulgación, tanto de las claves como de los procedimientos y otra información de similar tenor.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

La ATT en su calidad de ECR evaluará y actualizará una vez al año los procedimientos para la protección de los equipos informáticos y de comunicación y contempla procedimientos para la seguridad de la información, los sistemas y aplicaciones, para los que ha desarrollado un Plan de Seguridad para tal efecto.

Acorde a la Política de Seguridad establecida, la ATT en su calidad de ECR garantiza:

- La administración sobre la identificación y autenticación para el acceso a la infraestructura tecnológica de la ECR, del personal involucrado en las funciones críticas de certificación y publicación.
- La administración del personal con los controles necesarios para una adecuada separación de funciones.
- El registro de los eventos que pueden ser analizados a fin de minimizar riesgos de seguridad y prevenir amenazas conocidas.

I-LP-15466

- El resguardo de la integridad, confidencialidad y disponibilidad de los datos críticos.
- Una gestión de incidentes planificada, a fin de mitigar los efectos de los eventos no previstos que pueden amenazar la operación de la ECR.

6.6. CONTROLES DE SEGURIDAD SOBRE EL CICLO DE VIDA DE LOS SISTEMAS

Los controles de seguridad sobre el ciclo de vida de los sistemas se basan en el cumplimiento de los procedimientos establecidos por el personal y en las características de seguridad determinadas para los equipos involucrados en la generación y almacenamiento de las claves, así como en las configuraciones de seguridad de los sistemas y en los equipos de gestión de la información.

6.7. SEGURIDAD DE LA RED

La operación de los servicios de certificación de la ECR se realiza fuera de línea, asegurando su protección de accesos no autorizados.

La seguridad de los servicios de publicación se basa en los controles sobre la infraestructura y su equipamiento, los controles de acceso a los servicios y equipos, así como en aquellos aplicables a los medios de almacenamiento y los sistemas informáticos asociados.

6.8. CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

Los equipos y sistemas de la ECR asociados a la gestión del ciclo de vida de los certificados, así como su servicio de publicación y de repositorio toman una fuente horaria confiable, a fin de que las operaciones puedan realizarse tomando una marca de tiempo confiable. De este modo, los registros de eventos y auditorías reflejan el momento de ocurrencia de manera ajustada y precisa.

I-LP-15466

7. PERFILES DE CERTIFICADOS Y CRL

7.1. PERFIL DE CERTIFICADO DE LA ECR

El siguiente perfil de certificado se corresponde con la Versión 3 del estándar X.509

Campos y atributos	Contenido
Versión	el valor del campo es 2.
Número de Serie (serialNumber)	Número asignado por la ECR, valor hasta de 20 octetos
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre Distintivo del Emisor (Issuer DN)	CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO estándar de acuerdo a ISO3166
Validez (desde, hasta) Validfrom/Valid to	[20 años] Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time).
Nombre distintivo del suscriptor (Subject DN)	CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO estándar de acuerdo a ISO3166.
Clave Pública del suscriptor (SubjectPublic Key)	Algoritmo: RSA, Longitud: 4096 bits.
Extensiones	
Identificador de la clave del suscriptor (Suject Key Identifier)	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.
Políticas de Certificación (CertificatePolicies)	URI: http://..... (Archivo en formato de texto).
Restricciones Básicas (basicContraints)	CA = TRUE, pathLenConstriant = "1".
Punto de distribución de la Lista de certificados Revocados (CRL DistributionPoints)	URI (1): http://..... (.crl) URI (2): http://.....(.crl)

7.2. PERFIL DE CERTIFICADO DE ECA

El siguiente perfil de certificado se corresponde con la Versión 3 del estándar X.509

Campos y Atributos	Contenido
Versión	el valor del campo es 2.
Número de Serie (serialNumber)	Número asignado por la ECR, valor hasta de 20 octetos.
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre Distintivo del Emisor (Issuer DN)	CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO estándar de acuerdo a ISO3166.
Validez (desde, hasta) Validfrom/Valid to	[10 años] Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time
Nombre distintivo del suscriptor (Subject DN)	CN = Nombre de la Entidad Certificadora Autorizada, O = Razón Social de la Entidad Certificadora Autorizada, C = BO de

I-LP-15466

	acuerdo al estándar ISO 3166
Clave Pública del suscriptor (SubjectPublic Key)	Algoritmo: RSA, Longitud:2048 bits
Extensiones	
Identificador de la clave del suscriptor (Suject Key Identifier)	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.
Políticas de Certificación (CertificatePolicies)	URI: http://..... (Archivo en formato de texto).
Restricciones Básicas (basicContraints)	CA = TRUE, pathLenConstriant = "1".
Punto de distribución de la Lista de certificados Revocados (CRL DistributionPoints)	URI (1): http://..... (.crl) URI (2): http://.....(.crl)

7.3. PERFIL DE LA CRL DE LA ECR

El siguiente perfil de certificado se corresponde con la Versión 2 del estándar X.509

Campos y atributos	**Contenido**
Versión	el valor del campo es 1 (corresponde a versión 2)
Algoritmo de firma (signatureAlgorithm)	SHA256withRSA 1.2.840.113549.1.1.11
Nombre Distintivo del Emisor (Issuer DN)	CN = Nombre de la Entidad Certificadora Autorizada, O = Razón Social de la Entidad Certificadora Autorizada, C = BO de acuerdo al estándar ISO 3166
Día y hora de Validez (Efective Date) o	Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
Próxima actualización (Nextupdate)	Día y hora de la próxima actualización de la CRL [seis (6) meses y cada vez que se emite o revoca un certificado] a) Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
Certificados revocados (RevokedCertificate)	b) Contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas
Extensiones	
Identificador de la clave delaEntidad Certificadora (Authority Key Identifier)	a) Función Hash (SHA1) del atributo SujectPublicKey (clave pública correspondiente a la clave privada usada para firmar la Lista de

I-LP-15466

	Certificados Revocados).
Número de CRL	Número entero de secuencia incremental para una CRL y una Entidad Certificadora Autorizada determinada.

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.

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:

- Unspecified (0) - No especificada, utilizada para revocaciones por motivos no contemplados en los otros códigos.
- 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
- removeFromCRL (8), retirado de la CRL, utilizado cuando por algún motivo un certificado digital es retirado de la CRL.
- 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.

8. AUDITORÍA DE CONFORMIDAD

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD

La ATT en su rol de Entidad Certificadora Raíz está sometida a las auditorías de la Contraloría General del Estado y demás instituciones administrativas del ámbito público con competencia a la que rinde cuenta de sus acciones, de acuerdo a sus programas de auditoría.

I-LP-15466

8.2. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

El auditor desempeña su rol en conformidad con las leyes y normas aplicables, con independencia de criterio y aplicación de las metodologías establecidas.

La ATT en su calidad de ECR brindará toda la documentación e información que solicite el auditor en el ejercicio de sus tareas y guardará reserva sobre los datos de carácter confidencial que hayan sido clasificados.

8.3. COMUNICACIÓN DE LOS RESULTADOS.

Los resultados de la Auditoría serán informados y aprobados por el organismo Auditor y luego comunicados a las autoridades de la ATT en un Informe con las recomendaciones que considere pertinentes. En todos los casos, la ATT en su calidad de ECR atenderá las recomendaciones, y las responderá en tiempo y forma.

9. REQUISITOS COMERCIALES Y LEGALES.

9.1. TARIFAS

Los aranceles de las ECA, están establecidos en el Decreto Supremo N° 1793.

9.2. POLÍTICAS DE CONFIDENCIALIDAD

Los documentos y la información obtenida por la ECR de los solicitantes de autorización para constituirse en ECA recibidos por ATT en su calidad de ECR, se mantendrán con carácter de confidencial por razones de seguridad, no así su denominación, razón social o comercial y su carácter de solicitante, ya que estos constituyen datos públicos.

Asimismo, la ECR mantiene la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso.

9.3. PROTECCIÓN DE LOS DATOS PERSONALES

La ATT en su calidad de ECR cumple con lo dispuesto en el Art. 56 del Decreto Supremo N° 1793, sobre la protección de datos personales a fin de garantizar la seguridad informática de los mismos, adoptando las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de

I-LP-15466

tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

9.4. OBLIGACIONES DE LOS PARTICIPANTES DE LA PKI

La ATT en su calidad de ECR es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las ECA.

Las obligaciones de las ECA figuran en la PC de la ECR. Asimismo, como titulares de certificados emitidos por la ECR, las ECA tiene las siguientes obligaciones:

a) Proporcionar información fidedigna y susceptible de verificación a la entidad certificadora;

b) Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado;

c) Observar las condiciones establecidas por la entidad certificadora para la utilización del certificado digital y la generación de la firma digital;

d) Notificar oportunamente a la certificadora que los datos de creación de su firma digital han sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada, en este caso deberá solicitar la baja de su certificado digital;

e) Actuar con diligencia y tomar medidas de seguridad necesarias para mantener los datos de generación de la firma digital bajo su estricto control, evitando la utilización no autorizada del certificado digital;

f) Comunicar a la entidad certificadora, cuando exista el riesgo de que los datos de su firma digital sean de conocimiento no autorizado de terceros, por el titular y pueda ser utilizada indebidamente;

g) No utilizar los datos de creación de firma digital cuando haya expirado el período de validez del certificado digital; o la entidad de certificación le notifique la suspensión de su vigencia o la conclusión de su validez.

El incumplimiento de las obligaciones antes detalladas, hará responsable al titular de la firma digital de las consecuencias generadas por el uso indebido de su firma digital.

Los terceros aceptantes están obligados a realizar la validación de la cadena de confianza de un certificado cuando reciban una firma digital basada en un certificado emitido por la Entidad Certificadora Raíz del Estado Plurinacional de Bolivia.

I-LP-15466

9.5. MODIFICACIONES AL PRESENTE DOCUMENTO

El presente documento podrá ser modificado de acuerdo a las actualizaciones que se considere conveniente incorporar y sus procedimientos internos, y deberá ser aprobado por ATT en su calidad de ECR.

9.6. RESOLUCIÓN DE CONFLICTOS

La ATT en su calidad de ECR recibe y resuelve los reclamos por conflictos de las ECA vinculados al funcionamiento de la ECR, en forma escrita, detallada y de acuerdo a los procedimientos administrativos vigentes.

9.7. LEGISLACIÓN APLICABLE

Son de aplicación específica, la Ley N° 164 de fecha 8 de agosto de 2011, el Reglamento para el Desarrollo de las TIC, Decreto Supremos N° 1793 del 13 de noviembre de 2013 y su modificación aprobada mediante Decreto Supremo N° 3257 de 11 de abril de 2018 y a los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente.

9.8. CONFORMIDAD CON LA LEY APLICABLE

Las normativas y documentación elaborada por ATT en su calidad de ECR para el funcionamiento de la ECR se ajustan a la normativa vigente en materia administrativa y de certificación digital y su funcionamiento se realiza en el marco legal enumerado en el punto anterior así como la correspondiente al Sector Público, que sea aplicable, incluyendo entre otras la Ley de Ministerios, la de la Contraloría General, la normativa referida a la Estructura orgánica de ATT, la designación de cargos en la Administración Pública, etc.

I-LP-15466

ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA

AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT

LINEAMIENTOS PARA TERCEROS ACEPTANTES QUE ACTÚEN EN EL MARCO DE LA INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN DIGITAL DEL ESTADO PLURINACIONAL DE BOLIVIA - LT

Datos del documento	
Título del documento	Lineamientos para terceros aceptantes que actúen en el marco de la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia
Identificador documental	ECR-Lineamientos para Terceros (LT)
Criticidad:	Alta
Fecha	13 de noviembre de 2018
Autor	ATT
Versión	2.0
Comentario	
Publicación	Público

I-LP-15466

Noviembre 2018

CONTENIDO

I-LP-15466

1. ÁMBITO DE APLICACIÓN

El presente documento contiene los lineamientos generales que deben seguir los terceros aceptantes que actúen en el marco de la Infraestructura Nacional de Certificación Digital de Bolivia – INCD, cuando verifiquen la validez de las firmas digitales.

En su redacción se han tenido en cuenta lo establecido enlos "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, en el Decreto Supremo N° 1793, así como los estándares RFC 3647 y 5280 del IETF (Internet Engeneering Task Force) e ITU-T X.509, entre otros, y las buenas prácticas y experiencias internacionales en la materia.

Cabe aclarar en cuanto a la figura del tercero aceptante, que la Declaración de Prácticas de Certificación, introduce esta figura como uno de los participantes de la PKI (Infraestructura de Claves Públicas, por sus siglas en inglés).

A la luz de esta incorporación y de las experiencias normativas internacionales, un tercero aceptante puede ser definido comola persona natural o jurídica que recibe un documento firmado digitalmente y que debiendo verificar dicha firma digital, realiza una serie de acciones, entre las cuales se encuentra la generación de una consulta para corroborar la validez del certificado digital correspondiente.

2. OBJETIVO GENERAL Y ALCANCE

Es objetivo de este documento es establecer los lineamientos técnicos generales relativos a los pasos necesarios que debe seguir un tercero aceptante para validar una firma digital, desde la perspectiva tanto de un tercero aceptante individual como la de un sistema informático que realice dicho proceso en forma automática.

Se aclara que el presente documento no constituye una guía exhaustiva de los procesos técnicos que se desarrollan a partir de la voluntad de un tercero aceptante de validar una firma digital.

Su alcance es la identificación de los principales aspectos técnicos a tener en cuenta al momento de desarrollar los procedimientos específicos que un tercero aceptante individual o una aplicación deben seguir para validarlas firmas digitales y los certificados correspondientes.

3. RESPONSABILIDADES GENERALES

Las responsabilidades de cumplimiento de lo indicado en este documento corresponden a todo aquel que deba determinar la validez de una firma digital y de los certificados involucrados, en el marco de la INCD del Estado Plurinacional de Bolivia. Comprende también a los responsables de desarrollos informáticos de cualquier naturaleza, que tengan por objetivo realizar las verificaciones antes mencionadas de manera automática.

I-LP-15466

4. DESPLIEGUE Y DESARROLLO

4.1 ASPECTOS GENERALES

La validación de una firma digital y de los certificados involucrados, comprende las siguientes verificaciones:

a. Que los certificados involucrados hayan sido emitidos usando los formatos y contenidos establecidos en el marco legal aplicable a la INCD;

b. Que la firma digital haya sido generada durante el período de vigencia del certificado correspondiente y cuando éste no se encontraba revocado;

c. Que el certificado que contiene la clave pública correspondiente a la firma digital que se pretende verificar fue emitido por una Entidad Certificadora Autorizada – ECA, en el marco de la INCD de Bolivia y que la cadena de verificación correspondiente pueda ser apropiadamente verificada.

d. Que el certificado y las claves están siendo utilizados dentro de los usos permitidos en la Política de Certificación correspondiente.

A continuación, se describen con mayor detalle los pasos de verificación señalados.

4.2 VALIDACIÓN LOCAL DEL CERTIFICADO

Este primer paso comprende la verificación de la validez de un certificado digital que es efectuada localmente, es decir sin necesidad de recurrir a entidades externas.

Generalmente es realizada en forma automática por el sistema informático involucrado, ya sea que se trate de un producto comercial adquirido, como puede ser el caso de un cliente de correo electrónico, o como un desarrollo particular realizado con un fin específico.

En líneas generales, comprende los siguientes pasos:

a. Corroboración de que el certificado es un documento en notación ASN.1

b. Verificación de que su estructura se corresponde con un certificado X.509

c. Obtención del contendido del campo *Nombre Distintivo* (DISTINGUISHED NAME) de la entidad emisora (ISSUER) y opcionalmente, de la extensión *Identificador de la clave de la Autoridad* (AUTHORITY KEYIDENTIFIER), para acceder al certificado de la Entidad Certificadora Autorizada - ECA que lo emitió (ver punto siguiente respecto a la cadena de certificación). Esto último se puede realizar accediendo al almacén de certificados de la instalación utilizada o bien, bajándolo del sitio de la ECA o de la Entidad Certificadora Raíz – ECR.

d. Obtención de la clave pública contenida en el certificado para verificar la firma digital.

Si como resultado de los pasos antes indicados, la verificación es exitosa, se concluye que el certificado presentado fue emitido por una ECA de la INCD del Estado Plurinacional de Bolivia y por lo tanto, es válida.

I-LP-15466

Si en cambio, algunos de los pasos descritos arrojan un resultado erróneo debe rechazarse la firma digital por inválida.

4.3 VALIDACIÓN DE LA CADENA DE CERTIFICACIÓN

Para la validación de la cadena de certificación, es decir la verificación de que los certificados digitales son válidos, debe controlarse o verificarse lo siguiente para el certificado correspondiente a la firma digital del documento o transacción:

- Ha sido emitido por una ECA,
- Que el certificado se encuentra dentro de su período de vigencia
- Que no se encuentre revocado ni suspendido

Respecto al certificado de la ECA se debe corroborar que:

- Ha sido emitido por la ECR de la INCD,
- Que el certificado se encuentra dentro de su período de vigencia
- Que no se encuentre revocado

En ambos casos corresponde la verificación de las correspondientes Listas de Certificados Revocados - CRL, por sus siglas en inglés, tanto de la ECA que emitió el certificado digital como de la ECR.

Cabe añadir que en el largo plazo, la verificación de una firma digital implica la determinación de que la misma fue producida durante el plazo de vigencia del certificado digital, considerando su eventual revocación o suspensión. Esto implica la disposición de mecanismos tales como los sellos de tiempo ("time stamps") y de estándares de conservación en el largo plazo de documentación electrónica firmada digitalmente.

Alternativamente puede recurrirse a otros mecanismos indirectos, como la prueba de que un documento fue aceptado por un sistema solo en razón de que en su momento se pudo realizar tales verificaciones. Sin embargo, estos mecanismos pueden resultar más complejos a la hora de ofrecerlos como prueba.

Otra cuestión a tener en cuenta, es que se debe verificar si se trata de un certificado emitido para un usuario final (persona natural o jurídica o de cargo) o para una entidad certificadora. Para el utilizado para verificar la firma digital del documento o de la transacción, debe corroborarse el primer caso mientras que, a lo largo de toda la cadena de confianza, que cada certificado involucrado es un certificado de Entidad Certificadora.

Esta información surge del propio certificado digital, bajo la extensión Restricciones Básicas (*basic Constraints*) y se la identifica con la sigla CA.

Por consiguiente, si CA=True, entonces se trata de un certificado de una entidad certificadora y su suscriptor se encuentra habilitado para emitir certificados. Son los casos de la ECR y la ECA. Si en cambio CA=False, entonces no puede ser usado para emitir certificados. Como consecuencia, la validación de una cadena de confianza con un certificado intermedio que contenga el valor CA=False debe ser rechazada y lo mismo ocurriría en el caso de un certificado de persona natural o jurídica o de cargo, si CA=True.

I-LP-15466

4.4 VALIDACIÓN DEL USO DEL CERTIFICADO

Dentro de las Políticas de Certificación de la ECR y de una ECA, se establece que se deberán detallar los usos permitidos para dichos certificados, así como también, las restricciones impuestas a tal utilización.

En consiguiente, se interpreta que cada Política de Certificación de una ECA bajo la cual se emiten determinados certificados tiene asociado una serie de usos específicos, que deben ser corroborados y verificados por el tercero aceptante antes de dar por válida una firma digital. Esto es así ya que un uso no permitido podría invalidar la firma, restando validez jurídica al documento o a la transacción con la cual se encuentra vinculada.

Para revisar si el uso se encuentra dentro de lo permitido, el tercero aceptante debe tener acceso a la Política de Certificación correspondiente. Para ello, el propio certificado digital involucrado contiene la extensión Políticas de Certificación (*certificate Policies*) que contiene un enlace (URI) de Internet donde se encuentra publicada la Política de Certificación.

Adicionalmente, el tercero aceptante debe verificar una serie de datos que también se encuentran en el certificado digital, con el fin de determinar si el uso que se le está dando corresponde con el contexto en el que está siendo empleado.

En este sentido, se debe validar la extensión Uso de Claves (*keyUsage*) que se define como un campo crítico para todos los certificados que describe los usos permitidos de la clave pública mediante la habilitación o deshabilitación de una serie de campos.

En otras palabras, en esta extensión se registran una serie de bits que al encontrarse habilitados tomando el valor "1", se permiten usos para la clave pública incluida en el certificado. Dichos usos se registran a través de los siguientes atributos, de acuerdo a lo indicado en el artículo referido en el párrafo anterior, que a su vez refleja el texto del RFC 5280 y son los siguientes:

- 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: Utilizado para cifrar claves u otra información de seguridad.
- dataEncipherment: Utilizado para cifrar datos de usuario, pero no claves u otra información de seguridad
- keyAgreement: Utilizado para indicar que se utiliza la clave pública para realizar un acuerdo de claves
- keyCertSign: Utilizado para indicar que se utiliza la clave pública para verificar las firmas en los certificados

I-LP-15466

- cRLSign: Utilizado para indicar que la clave pública es empleada para la verificación de firmas en las listas de revocación de certificados

- encipherOnly: Utilizada 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

Al respecto y dentro del marco de la INCD según lo establecen los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, según el tipo de certificado, estos bits deben reflejar lo siguiente:

Tipo de certificado	Uso de clave
ECR	keyCertSign = 1, cRLSign = 1
ECA	keyCertSign = 1, cRLSign = 1
Persona Natural	digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1
Persona Jurídica	digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1

Finalmente, otra extensión a tener en cuenta es la denominada Uso de claves extendido (*extendedKeyUsage*). Esta extensión describe usos adicionales a los antes mencionados, mediante la habilitación de distintos atributos. De acuerdo al estándar RFC 5280, pueden usarse los siguientes:

- Autenticación de SSL/TLS en modo servidor (Certificado de Sitio) - serverAuth
- Autenticación de SSL/TLS en modo cliente - clientAuth
- Firma de código - codeSigning
- Autenticación, firma y cifrado de correo electrónico - emailProtection
- Firma de Sellos de Tiempo (Timestamping) - timeStamping
- Firma de respuestas para el Protocolo de en línea del estado de un certificado (OCSP) -
- OCSPSigning

En los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigentese toman los siguientes valores:

Tipo de certificado	Uso extendido de clave
Persona Natural	clientAuth, EmailProtection
Persona Jurídica	clientAuth, EmailProtection, serverAuth

I-LP-15466

5. LISTA DE CERTIFICADOS REVOCADOS

Las listas de certificados son archivos digitales que contienen la lista con los números de serie de los certificados muestran el estado del certificado a los fines de su verificación, como revocado. Las listas de revocación son obligatorias las ECA deben implementar servicios de validación del estado del certificado en línea (OCSP), dada la criticidad de las operaciones y su utilización en tiempo real de forma permanente.

6. REVISIÓN Y ACTUALIZACIÓN DEL DOCUMENTO

Estos lineamientos serán revisados al menos una vez al año, salvo consideraciones contrarias tomadas por la ATT en su calidad de ECR en las que requiera hacerlo antes, por razones operativas, originadas en un cambio tecnológico o vinculadas a un cambio de normativa aplicable.

7. REFERENCIAS NORMATIVAS COMPLEMENTARIAS

El presente documento complementa los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente y demás normativa aplicable y ha sido elaborado teniendo en cuenta los estándares internacionales citados precedentemente.

I-LP-15466

ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA

AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT

PROCEDIMIENTO DE AUTORIZACIÓN DE ENTIDADES CERTIFICADORAS – AEC

Datos del documento	
Título del documento	Procedimiento de Autorización de Entidades Certificadoras
Identificador documental	ECR-PAEC
Criticidad:	Alta
Fecha	13 de noviembre de 2018
Autor	ATT
Versión	2.0
Comentario	
Publicación	Público

Noviembre 2018

I-LP-15466

CONTENIDO

I-LP-15466

1. ÁMBITO DE APLICACIÓN DEL PROCEDIMIENTO DE AUTORIZACIÓN

El presente Procedimiento de Autorización de Entidades Certificadoras, se aplica en la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT del Estado Plurinacional de Bolivia, específicamente para las actividades que lleva adelante en calidad de Entidad Certificadora Raíz - ECR, en el cumplimiento de sus misiones y funciones.

En su redacción se han tenido en cuenta los lineamientos incluidos en el Decreto Supremo N° 1793 de 13 de noviembre de 2013, en las modificaciones al Decreto Supremo N° 1793 aprobadas mediante Decreto Supremo N° 3257 de 11 de abril de 2018 y demás normativa aplicable, así como los estándares y documentos técnicos internacionales RFC 3647 del IETF (Internet Engeneering Task Force), el estándar Web Trust para los "Principios y Criterios para Autoridades de Certificación", la ISO 21188:2006, ISO 9001:2008, ISO 22301:2012, ISO 27001:2013, ISO 27002:2013, ISO 30300:2011, ISO 3166:1997 e ITU-T X.509, entre otros, y las buenas prácticas y experiencias internacionales en la materia.

2. OBJETIVO GENERAL

Son objetivos de este documento establecer los pasos a seguir para la autorización de entidades certificadoras, incluyendo la revisión y aprobación de los requisitos legales, económicos y técnicos, que debe llevar adelante la AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES – ATT, en su calidad de Entidad Certificadora Raíz ECR.

3. RESPONSABILIDADES GENERALES

Las responsabilidades de cumplimiento de lo indicado en este documento corresponden a la totalidad del personal que sea designado para participar en el proceso de autorización de Entidades Certificadoras, sea éste perteneciente a la Unidad de Regulación de Tecnologías de Información, tanto temporario o permanente, interno o externo a dicha Unidad, como al personal de ATT asignado a las tareas descritas en el presente documento.

Es responsabilidad del Jefe de la Unidad de Regulación de Tecnologías de Información hacer conocer y cumplir lo dispuesto para este proceso de autorización.

I-LP-15466

4. DESPLIEGUE Y DESARROLLO

4.1 ASPECTOS GENERALES.

La ATT en su calidad de ECR y en uso de sus atribuciones, otorgará la autorización para su funcionamiento a las Entidades Certificadoras – EC, de carácter Público o Privado, con vigencia de cinco años, previo cumplimiento de una serie de requisitos y condiciones que se encuentran enumerados en la normativa vigente.

En el mismo sentido, la normativa aplicable establece que la ATT, en su calidad de ECR es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las EC. Por lo que corresponde a dicha Autoridad, en su calidad de ECR en consiguiente, conducir el proceso de autorización y en particular, a la Unidad de Regulación de Tecnologías de la Información coordinar todas las actividades necesarias a tal fin, correspondiendo también a su jefatura la comunicación de todo requerimiento a las entidades solicitantes, sin perjuicio de la participación de otro personal de ATT asignado especialmente para el cumplimiento de tareas específicas.

Cabe acotar que de acuerdo al artículo 47 del Decreto Supremo 1793, la ATT en su calidad de ECR autoriza a las EC que así lo soliciten, mediante un contrato para la prestación de servicios de certificación digital, el cual tiene una vigencia de cinco (5) años. Dicho contrato es firmado una vez culminado satisfactoriamente el proceso de autorización y como paso previo a la emisión de la Resolución Administrativa Regulatoria de ATT y de la emisión del certificado digital para la ECA por parte de la ECR.

En el proceso de autorización de una EC, de acuerdo a la normativa aplicable, los requisitos legales son evaluados por un analista legal de la Dirección Jurídica de ATT en su calidad de ECR, los requisitos técnicos y económicos por al menos un analista de la Unidad de Regulación de Tecnologías de Información y uno o varios analistas de la misma unidad, según sea el caso, lleva adelante la auditoría o verificación in situ.

La asignación de analistas pertenecientes a la Unidad de Regulación de Tecnologías de Información es llevada a cabo por la Jefatura de dicha Unidad mientras que la designación de personal perteneciente a otras áreas de ATT en su calidad de ECR, es decidida por el máximo responsable de cada área.

Si bien se les asignan funciones específicas, este grupo de analistas conformará un equipo, debiendo trabajar en forma colaborativa durante todo el proceso de autorización, de manera de permitir un análisis pormenorizado e integral del nivel de cumplimiento de las condiciones establecidas en la normativa aplicable y en el presente documento.

I-LP-15466

A continuación, se detallan los pasos a seguir para el proceso de autorización de EC a los fines de su incorporación a la Infraestructura de Certificación Digital de Bolivia o bien, al rechazo de la solicitud.

4.2 RECEPCIÓN DEL TRÁMITE.

La EC interesada debe presentar su solicitud de autorización de funcionamiento ante el Director Ejecutivo de la ATT quien remitirá a la Dirección Administrativa Financiera de la ATT, junto a la totalidad de la documentación requerida en la normativa aplicable y en el presente procedimiento.

La Dirección Administrativa Financiera asigna un número de hoja de ruta al expediente que contenga toda la documentación presentada. Todas las actuaciones que se generen en vinculación con el trámite de autorización de la EC deben reunirse bajo el número asignado, sin excepción, tanto sean estas generadas por la EC solicitante o por personal de ATT.

Una vez asignado el número referido, se procederá a su registro en el sistema de gestión de expedientes de la ATT, de manera de proceder a su seguimiento durante el proceso de autorización, y a la derivación de la documentación legal, económica y técnica al área Archivo.

Se establece que esta etapa no debe exceder de dos días.

4.3. REVISIÓN DE LA DOCUMENTACIÓN.

El área de Archivo asigna el código de expediente y N° de Trámite y remite las actuaciones a la Jefatura de la Unidad de Regulación de Tecnologías de Información, la cual procede a asignar el trámite a uno o varios analistas, según el tenor de la solicitud de autorización y la disponibilidad de personal.

Dicho personal se aboca a realizar un análisis de la documentación desde las perspectivas técnica y económica, en cuanto a la verificación de los requisitos exigidos. Realiza también una evaluación de las capacidades económicas y técnicas para el cumplimiento de las funciones de emisión de certificados, según el alcance establecido en la presentación de la EC solicitante.

4.3.1. REQUERIMIENTOS ECONÓMICOS PARA EC PÚBLICAS.

Los requisitos económicos que deben corroborarse en el caso de EC Públicas son los siguientes:

a. Estados Financieros (Certificado de solvencia Fiscal otorgado por la Contraloría General del Estado)
b. Balance de apertura o balance general correspondiente al último ejercicio anual presentado al Servicio de Impuestos Nacionales, verificando la constancia de presentación
c. Plan de negocio proyectado para todo un período de cinco años, vinculados a la licencia, el cual debe contener además el programa de inversiones generales a efectuar.

I-LP-15466

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

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

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

TARIJA: Calle Alejandro del Carpio N° 720 esq. O´Connor Piso 1 Telf.: 4-644136

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

d. Boleta de garantía de cumplimiento del contrato, por el siete por ciento (7%) sobre sus proyecciones para el primer año, que respalde su actividad para prestación de servicio de certificación digital, de acuerdo al artículo 45 del Decreto Supremo N° 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018.

e. Pago por adelantado a la ATT del uno por ciento 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, según el artículo 48 del Decreto Supremo N° 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018.

f. Estructura tarifaria de acuerdo al artículo 42 del Decreto Supremo N° 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018. En este punto debe dejar constancia de los criterios sustentados y orientados utilizados para la determinación de los costos de los servicios de certificación digital que se propone brindar

g. Copia del acto administrativo o resolutorio que autoriza a la entidad pública a actuar como EC

Se aclara que los requisitos d y e deben ser cumplidos una vez obtenida la autorización, debiendo la EC manifestar formalmente en este paso su voluntad de dar cumplimiento a lo requerido.

4.3.2. REQUERIMIENTOS ECONÓMICOS PARA EC PRIVADAS.

Las EC Privadas deben presentar la misma documentación citada precedentemente con el agregado de:

a. Documentación que acredite las fuentes de financiamiento, o bien la demostración de que cuenta con los recursos necesarios para implementar el proyecto técnico presentado.

Corresponde asimismo indicar que los requisitos d y e del listado del título anterior deben ser complementados una vez obtenida la autorización, debiendo la EC manifestar formalmente en este paso su voluntad de dar cumplimiento a lo requerido.

4.3.3. ASPECTOS COMPLEMENTARIOS.

4.3.3.1. PLAZO DE PAGO:

I. Las Entidades Certificadoras deberán efectuar un solo pago anual del 1% de sus ingresos brutos de operación del servicios de certificación digital correspondiente al año anterior por Tasa de Fiscalización y Regulación hasta el 30 de Junio de cada gestión, para lo cual deberán presentar hasta el 15 de Junio de cada gestión los Estados Financieros Auditados, el formulario 605 del Servicio de Impuestos Nacionales y su Declaración Jurada en el Formulario de Declaración Jurada habilitada a través de la Plataforma Virtual de la ATT .

I-LP-15466

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

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

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

TARIJA: Calle Alejandro del Carpio N° 720 esq. O´Connor Piso 1 Telf.: 4-644136

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

Para el primer año de operaciones, la entidad certificadora cancelará por adelantado la Tasa de Fiscalización y Regulación, en base a la proyección de sus ingresos brutos de operación del servicio de Certificación Digital dentro de los 10 días a partir de la notificación al operador con la nota de cobranza emitida por la ATT, pasado este plazo y de no haberse concretizado el pago, se desestimará de oficio la solicitud de autorización para la prestación del servicio de certificados digitales.

II. En caso de que las fechas establecidas coincidan con días sábados, domingos o feriados deberán ser trasladada al siguiente día hábil.

4.3.3.2. MOROSIDAD EN EL PAGO:

Cuando exista incumplimiento en el plazo de pago por concepto de Tasa de Fiscalización y Regulación:

I. El operador será considerado operador en mora sin necesidad de intimación o requerimiento alguno.

II. La ATT establecerá las siguientes penalidades en caso de mora del pago de la Tasa de Fiscalización y Regulación:

a) Multa del diez por ciento (10%) sobre el monto total adeudado.

b) Tasa de interés del seis por ciento (6%) anual sobre el monto adeudado.

III. Los intereses corren a partir del día siguiente de la fecha de vencimiento del pago.

IV. El pago por concepto de la multa y los intereses correspondientes deberán cancelarse de forma conjunta con la Tasa de Fiscalización y Regulación vencida.

4.3.3.3. CÁLCULO DE GESTIONES NO DECLARADAS O DECLARADAS EN CERO:

I. En el caso de que el operador no hubiese presentado sus Estados Financieros para la verificación del importe a ser pagado en el plazo establecidos del servicio de Certificación Digital la ATT aplicara como base de cálculo el monto más alto de ingresos brutos de operación reportados por un operador equivalente determinado de manera conjunta por la Dirección Administrativa Financiera y Dirección Técnica Sectorial de Telecomunicaciones y TIC de la ATT en su calidad de ECR.

II. La Aplicación del método de cálculo establecido en los parágrafos anteriores del presente artículo, no eximen al operador de su obligación de remitir los Estados Financieros de la forma y plazos establecidos, ni constituyen óbice para la aplicación de sanciones y acciones legales correspondientes. El operador que incumpla con la fecha establecida para el pago de la Tasa de Fiscalización y Regulación, será considerado operador en mora sin necesidad de intimación o requerimiento alguno y pasible a la aplicación del inciso g) del artículo 50 del D.S. N° 1793.

I-LP-15466

4.3.4. REQUERIMIENTOS TÉCNICOS PARA EC PÚBLICAS Y PRIVADAS.

Con relación a los aspectos técnicos que deben cumplimentarse, tanto las EC Públicas como las Privadas, deben presentar:

a. Descripción de servicios a prestar, incluyendo duración y alcance de los mismos
b. Política de Certificación, cuyos contenidos deben ajustarse a la Política de Certificación Modelo para las ECA y al RFC 3647 del IETF
c. Declaración de Prácticas de Certificación, cuyos contenidos deben ajustarse a la Declaración de Practicas de Certificación Modelo para las ECA y al RFC 3647 del IETF.
d. Documento con la descripción de la infraestructura tecnológica, detallando los aspectos técnicos de la plataforma tecnológica e incluyendo el hardware, software, dispositivos de comunicación y seguridad con los que cuenta, sus características, funcionalidad y modos de operación. En este sentido, cuando sea aplicable, se debe demostrar que se han implementado procesos que garanticen la confiabilidad y el buen funcionamiento de la plataforma de gestión de certificados, que todos los elementos utilizados cuentan con las garantías y el nivel de funcionamiento debido y que el personal involucrados ha recibido la capacitación necesaria para operarlos
e. Política de protección de datos personales, garantizando las consideraciones del artículo 56 del Decreto Supremo 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018. En este aspecto deben demostrar que han adoptado todas las medidas necesarias para dar a los datos personales de solicitantes y signatarios de los certificados digitales que emitan de ser autorizados, el tratamiento técnico debido, en todas las etapas (recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones).

   Deben demostrar asimismo que se cumplirá con el requisito de contar con el conocimiento previo y el consentimiento expreso de los titulares de los datos. Dicho consentimiento podrá ser dado por escrito o por cualquier otro medio equiparable. El solicitante incluirá también un detalle de las medidas de índole técnica y organizativa que ha adoptado la EC para garantizar la seguridad de los datos personales objeto de tratamiento, en coincidencia con lo requerido en el punto e) del artículo 56 del Decreto Supremo 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018. Este detalle no debe ser necesariamente exclusivo para la emisión de certificados, si la organización posee una política amplia que alcance a todas sus líneas de actividad, si bien debe demostrarse que la actividad de emisión de certificados se encuentra alcanzada.
f. Planes y procedimientos para asegurar la continuidad del servicio de la EC, cuyos contenidos deben ajustarse al Modelo para las ECA de acuerdo a lo indicado en el capítulo correspondiente de la ISO 27002 y de la ISO 22301 de continuidad de las operaciones. El plan a presentar debe contener todas

I-LP-15466

las actividades que se llevarán a cabo para garantizar la minimización del impacto de un evento no esperado de manera que se pueda dar continuidad a las funciones críticas, las cuales deben estar identificadas claramente e incluir como mínimo, la emisión de la Lista de Certificados Revocados y la posibilidad de revocar o suspender un certificado digital emitido, de ser necesario. Debe prever asimismo la realización de pruebas periódicas.

g. Planes y procedimientos de seguridad de la EC, cuyos contenidos deben ajustarse al Modelo para las ECA y de acuerdo a lo indicado en las normas ISO 27001 e ISO 27002 sobre el sistema de gestión de la seguridad de la información y de las buenas prácticas en seguridad de la información, respectivamente. Este plan debe contemplar los aspectos relativos a:

- La seguridad física y ambiental, demostrando que se mantienen adecuados controles para asegurar las áreas en las que se desarrolla cada etapa del ciclo de vida de los certificados.
- El sistema de control de accesos.
- La seguridad lógica de aplicaciones y sistemas operativos involucrados en las tareas de certificación digital.
- El registro de eventos, incluyendo todas las actividades realizadas en el ciclo de vida de los certificados y su debida protección.
- El resguardo de la información que gestiona la EC, en particular aquella relativa a los certificados emitidos, cualquiera sea el soporte o medio utilizado y el formato de los datos, en todas las etapas del ciclo de vida de la información (planeamiento, diseño, construcción/adquisición, uso/operación, monitoreo y archivo/destrucción).

h. Planes de cese de actividades de la EC, de acuerdo a lo indicado en artículo 51 del Decreto Supremo 1793 y su modificación mediante Decreto Supremo N° 3257 de 11 de abril de 2018. Este plan debe contemplar como mínimo, la manera en que se comunicará el cese de operaciones a la ATT, a los titulares de los certificados y a otros interesados, los plazos en que se llevarán a cabo las actividades de cese, la manera en que se destruirán las claves de la ECA y los pasos que se seguirán. Se debe contemplar asimismo la instancia de revocatoria de la autorización y la obligación de comunicar a ATT con al menos dos meses de anticipación el destino que se dará a los datos de los certificados digitales emitidos por la EC.

i. Planes y procedimientos para la administración de las operaciones de la EC, cuyos contenidos deben ajustarse al Modelo para las ECA y de acuerdo a los lineamientos de la ISO 9001.

j. Procedimientos y condiciones que deben cumplir las EC para la conservación de documentos físicos y digitalizados, cuyos contenidos deben ajustarse al Modelo para las ECA asegurando su

I-LP-15466

almacenamiento en servidores ubicados en el territorio y bajo la legislación del Estado Plurinacional de Bolivia, siguiendo los lineamientos de la ISO 30300.

k. Evidencia que demuestre que la EC cuenta con un sistema de información permanente, actualizado y de acceso libre vía web, con la siguiente información:
   - Procedimientos de certificación digital.
   - Condiciones de validación, renovación, baja, suspensión, tarifas y usos de los certificados digitales que emite.
   - Certificados digitales emitidos, suspendidos y revocados con los siguientes datos:
     i. Número de serie.
     ii. Fecha de emisión.
     iii. Vigencia y restricciones aplicables.
   - Procedimientos de reclamo
   - Política de Certificación, Modelo de contrato tipo con suscriptores y demás documentos de carácter público que genere.
   - Domicilio legal, teléfonos y correo electrónico de contacto.

l. Modelo de contrato tipo con Suscriptores cuyos contenidos deben ajustarse al Modelo para las ECA.

m. Términos y condiciones de servicio con los suscriptores cuyos contenidos deben ajustarse al Modelo para las ECA.

n. Contratos de servicios de tercerización, si corresponde.

o. Requisitos y condiciones que se le impondrán a las Autoridades de Registro.

En el proceso de revisión de la documentación, el o los analistas asignados debe verificar que la EC ha desarrollado procedimientos que aseguren una comunicación clara y fehaciente a los solicitantes, suscriptores y todo otro posible interesado, de las condiciones de utilización del certificado digital, su tramitación, renovación, suspensión y revocación y del contenido de la Política de Certificación que le es aplicable.

En el mismo sentido, debe verificar la coherencia entre los contenidos de los distintos documentos presentados y la existencia de adecuados procedimientos para su administración, de modo que se asegure que todo cambio dispuesto en la operatoria o en los requerimientos legales, quede reflejado en ellos y que toda modificación se realice mediando las correspondientes autorizaciones.

Durante el proceso de revisión, el o los analistas designados elaboran las notas de requerimiento de información complementaria y/o adicional que considere necesarias cuando encuentre requerimientos

I-LP-15466

observados, las cuales serán de conocimiento del Jefe de la Unidad de Regulación de Tecnologías de Información. Este proceso tendrá una duración máxima de veinte (20) días.

La EC tiene un plazo máximo de quince (15) días para subsanar la documentación o expresar por escrito su intención de retirarse del proceso de autorización. Todo reingreso de información debe realizarse siguiendo los plazos establecidos en el punto 4.1 de la presente sección.

Una vez subsanadas las observaciones, el trámite reingresa y dentro de los quince (15) días, se emite el informe técnico de cumplimiento con los requisitos económicos y técnicos y se procede a su remisión a la Dirección Jurídica de la ATT.

En caso de no haber subsanado las observaciones, uno de los analistas asignados redacta, en un plazo no superior a quince (15) días, un informe técnico de rechazo y una nota dirigida a la EC solicitante, dándole a conocer los motivos del rechazo de su solicitud. Dicha nota es de conocimiento del Jefe de la Unidad de Regulación de Tecnologías de Información.

Se establece que esta etapa no debe exceder los setenta (70) días, entendiendo que este plazo se suspende cada vez que la EC solicitante deba subsanar una o varias observaciones, volviendo a reiniciarse la contabilización cuando las actuaciones son recibidas en la Unidad de Regulación de Tecnologías de Información.

4.4. REVISIÓN Y APROBACIÓN DE LOS REQUISITOS LEGALES.

Recibido el expediente de autorización, la máxima autoridad de la Dirección Jurídica de la ATT lo asigna a uno o varios analistas del área legal, quienes tendrán a su cargo la verificación del cumplimiento de los requisitos legales establecidos en la normativa aplicable.

4.4.1. REQUERIMIENTOS LEGALES PARA EC PÚBLICAS.

En particular para el caso de las EC solicitantes Públicas, los requisitos legales que dicho analista debe verificar son los siguientes:

a. Presentación de la nota o memorial de solicitud de acreditación debidamente firmado por autoridad responsable de la entidad solicitante, que incluya la siguiente información:
   1) Nombre de la EC
   2) Dirección postal de la EC
   3) Teléfonos de la EC
   4) Correo electrónico de la EC
   5) Fax y casilla postal, de corresponder

1-LP-15466

b. Norma jurídica de creación y disposición de nombramiento del Titular y de un suplente que eventualmente pueda reemplazarlo en las tramitaciones, como documentos que certifiquen la naturaleza del solicitante
c. Fotocopia legalizada del Documento de Identidad del Titular designado y de un suplemente
d. Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributario)
e. 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
f. Certificado de antecedentes penales judiciales del Representante Legal expedido por autoridad competente

4.4.2. REQUERIMIENTOS LEGALES PARA EC PRIVADAS.

Para el caso de las EC solicitantes Privadas y comprenden la presentación de los siguientes documentos:

a. Nota o memorial de solicitud de acreditación debidamente firmada por autoridad responsable de la entidad solicitante, que incluya la siguiente información:
    1) Nombre de la EC
    2) Dirección postal de la EC
    3) Teléfonos de la EC
    4) Correo electrónico de la EC
    5) Fax y casilla postal, de corresponder
b. Documentos que certifiquen la naturaleza del solicitante como empresa privada, mixta 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
c. Fotocopia legalizada del Documento de Identidad del Representante Legal
d. Poder Especial que acredite la personería del representante legal y que especifique las facultades de apersonamiento y para realizar trámites ante ATT
e. Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributario)
f. Nómina y fotocopias o documentos de identidad de todos los miembros de juntas y consejos directivos o socios de personas jurídicas

I-LP-15466

g. Declaración Jurada de la personas naturales o jurídicas, de todos los miembros de juntas o consejos directivos 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

h. Certificado de antecedentes penales judiciales del propietario o Representante Legal, expedido por autoridad competente

En el caso de existir observaciones a los requisitos legales tanto de EC Públicas como Privadas, incluyendo faltantes de documentación o incumplimiento de aspectos formales o de fondo, el analista asignado, en un plazo máximo de diez (10) días, elaborará las notas de requerimiento de información complementaria y/o adicional, dando un plazo máximo de quince (15) días a la EC solicitante para subsanar las observaciones o manifestar su intención de retirar su presentación, en nota debidamente fundada.

El trámite reingresa de acuerdo a lo indicado en el punto 4.2 de esta sección. En el caso de haber subsanado las observaciones, se emite un informe legal de cumplimiento y se remite el trámite a la Unidad de Regulación de Tecnologías de Información, en un plazo máximo de diez (10) días.

Para el caso en que la EC no hubiera subsanado las observaciones, o bien hubiera manifestado por escrito que se retira del proceso de autorización, el analista redactará el informe legal de rechazo, el cual debe ser de conocimiento de la máxima autoridad de la Dirección Jurídica y lo remitirá en un plazo de 8 días, a la Unidad de Regulación de Tecnologías de Información.

El analista asignado en dicha Unidad, según lo indicado en el punto 4.3 de esta sección, redactará dentro del plazo máximo de dos días de recibido el informe, la nota correspondiente haciéndole conocer a la EC el rechazo de su solicitud y fundamentando debidamente tal decisión. Dicha nota es de conocimiento del Jefe de la Unidad de Regulación de Tecnologías de Información.

4.5. AUDITORÍA DE CUMPLIMIENTO.

Cumplidos los requisitos legales, económicos y técnicos exigidos a la EC, la Unidad de Regulación de Tecnologías de Información designa a uno o varios analistas, según el tenor de la presentación y la disponibilidad del personal, para la realización de la auditoría de cumplimiento y verificación in situ de los requisitos exigidos. El plazo máximo de realización de la auditoría será de cuarenta y cinco (45) días.

El proceso de auditoría se inicia mediante nota de comunicación del inicio de la revisión firmada por el Jefe de la Unidad de Regulación de Tecnologías de Información, en la que conste:

- Fecha de inicio y duración estimada
- Datos de identificación del equipo de auditoría

I-LP-15466

- De ser necesarios, requerimientos administrativos para el desarrollo de los trabajos, como por ejemplo la disponibilidad de una oficina, una PC, una impresora y un gabinete cerrado
- Programa de auditoría a llevar a cabo durante la revisión
- Requerimiento de nombramiento de un contacto de la EC para coordinar los trabajos de auditoría y de un listado que contenga los nombres y datos de contacto (correo electrónico y teléfonos y función) de todo el personal vinculado a la actividad de certificación, de manera de planificar las entrevistas y visitas necesarias

Una vez cumplimentado el proceso de revisión, el o los analistas involucrados preparan un informe que debe contener:

- Nombre e identificación del equipo de auditoría.
- Fecha de inicio y terminación de la auditoría.
- Breve descripción de las tareas realizadas.
- Detalle en anexo de las instalaciones visitadas y del personal entrevistado.
- Declaración de conformidad de cada una de las condiciones previstas en los requisitos para EC aprobadas por la ATT en su calidad de ECR y su congruencia con la normativa vigente.
- Manifestación de conformidad de la política de certificación y la declaración de prácticas de certificación, así como la evaluación de la efectividad de los planes y procedimientos de seguridad y de contingencia contenidos tanto en la declaración como los exigidos en los Anexos correspondientes a los requisitos.
- Conformidad respecto a la confiabilidad y calidad de los sistemas utilizados.
- Confiabilidad y disponibilidad de los datos.
- Firma de los analistas que integran el equipo de auditoría designado.

El personal de ATT involucrado en la realización de la auditoría de una EC debe confeccionar debidamente los papeles de trabajo que respalden cada hallazgo y resguardar adecuadamente dicha documentación.

El proceso de revisión de auditoría se lleva a cabo en base a lo indicado en el Decreto Supremo 1793 y en el Estándar ISO 21188:2006, que establece una serie de controles para las Infraestructuras de Clave Pública.

De corresponder, el proceso de revisión debe abarcar también a los servicios terciarizados, como por ejemplo, las instalaciones de Data Centers de terceros contratados, teniendo especialmente en cuenta que toda la información debe residir en servidores que se encuentren dentro del Estado Plurinacional de Bolivia y alcanzados por su legislación.

I-LP-15466

En el caso que como resultado de la auditoría se formulen observaciones, el o los analistas designados elaboran el informe detallando los aspectos a subsanar y la nota correspondiente, la cual será de conocimiento del Jefe de la Unidad de Regulación de Tecnologías de Información. En dicho informe se indican los plazos máximos que la EC tendrá para reparar las observaciones encontradas, según el tenor de los hallazgos de auditoría. Dichos plazos no podrán exceder en ningún caso los treinta (30) días.

La EC solicitante debe acompañar en su respuesta toda la documentación y demás evidencia que permita la verificación de que se han adoptado las medidas necesarias para subsanar los aspectos observados, sin perjuicio de que el Jefe de la Unidad de Regulación de Tecnologías de Información pueda realizar una nueva revisión in situ para corroborar la evidencia remitida por la EC.

Todo reingreso de información debe realizare siguiendo los plazos establecidos en el punto 4.2 de la presente sección.

Una vez subsanadas las observaciones y realizadas las revisiones in situ, si fuera el caso, el o los analistas designados elaboran el informe de cumplimiento de la auditoría realizada, el cual es remitido a la Jefatura de la Unidad de Regulación de Tecnologías de Información, en un plazo que no debe exceder los quince (15) días.

Si en cambio, no se hubieran subsanado debidamente las observaciones formuladas, el o los analistas redactan, en un plazo máximo de 10 días, un informe de rechazo, el cual acompañado por la nota en la que haga conocer a la EC los motivos por los cuales no se continuará con el proceso de autorización, es remitido a la Unidad de Regulación de Tecnologías de Información. El Jefe de dicha Unidad tendrá conocimiento de la nota que es remitida a la EC solicitante.

4.6. TRAMITES ADMINISTRATIVOS.

Una vez que se han producido los informes favorables que cubran los aspectos técnicos, económicos y legales y el dictamen de auditoría, coincidiendo todos ellos respecto a la consecución del proceso de autorización de la EC solicitante, la ATT en su calidad de ECR da a conocer a dicha entidad, las obligaciones económicas que le caben en esta etapa del proceso.

La EC debe cumplimentarlas en un plazo máximo de diez días y con carácter previo a la firma del contrato para la autorización de su funcionamiento. En caso de no cumplir con dichas obligaciones, se da por desestimado el trámite, salvo que la EC explicite formalmente los motivos de la demora y la ATT en su calidad de ECR considere que dichos motivos justifican una prórroga.

I-LP-15466

4.7. INFORME FINAL.

Una vez cumplidas las obligaciones económicas, la Unidad de Regulación de Tecnologías de Información elaborará el informe técnico de cumplimiento de los requisitos exigidos y la recomendación a la Dirección Jurídica para la elaboración del contrato de cumplimiento y acto administrativo por el cual se otorga la autorización para su operación a la EC. Esta etapa debe cumplirse en un plazo máximo de quince días. Producidas las acciones antes indicadas, la ECR procede a la emisión del certificado digital de la ECA.

5. RESPONSABILIDADES ESPECÍFICAS

La Unidad de Regulación de Tecnologías de Información tiene asignadas las funciones de participar en la revisión de las solicitudes de las EC y de elaborar el dictamen para la autorización de aquellas que han cumplido con los requisitos legales, económicos y técnicos requeridos.

El Jefe de la Unidad de Regulación de Tecnologías de Información es responsable de coordinar las actividades de autorización de la EC y de remitir todas las comunicaciones en las que se requieran mayor información, la subsanación de observaciones de cualquier tenor o el rechazo de la solicitud.

Es responsabilidad de los Analistas asignados trabajar en equipo para autorizar a las EC que lo soliciten y elaborar los proyectos de dictamen de autorización correspondientes.

Otro personal que cumpla funciones en la Unidad de Regulación de Tecnologías de Información y todo aquel con acceso a las oficinas administrativas es responsable por el cumplimiento de las tareas que se describen en este documento, en cuanto les corresponda.

La Dirección Jurídica de ATT verifica el cumplimiento de los requisitos legales de las EC solicitantes y de la elaboración de los informes correspondientes.

Las Áreas Administrativo Financiera y de Archivo de la ATT deben cumplir con las funciones que les competen cuando den tratamiento a actuaciones vinculadas a solicitudes de autorización que presenten las EC, en los plazos y de acuerdo a las indicaciones incluidas en el presente documento.

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes es la responsable de la aprobación del presente documento.

I-LP-15466

6. REVISIÓN Y ACTUALIZACIÓN DEL PROCEDIMIENTO.

Este Procedimiento será revisado al menos una vez al año, salvo consideraciones contrarias tomadas por la ATT en las que requiera hacerlo antes, por razones operativas o por cambio de normativa aplicable.

7. REFERENCIAS NORMATIVAS COMPLEMENTARIAS.

El presente documento complementa lo establecido en el Decreto Supremo N° 1793 y demás normativa aplicable, y ha sido elaborado teniendo en cuenta los estándares internacionales citados precedentes.

I-LP-15466

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

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

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

TARIJA: Calle Alejandro del Carpio N° 720 esq. O´Connor
Piso 1
Telf.: 4-644136

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