



Resolución Administrativa Regulatoria **ATT-DJ-RAR-TL LP 272/2017**

La Paz, 3 de mayo de 2017

Raquel Natalia Ossorio Baldivieso
TECNICO LEGAL
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

VISTOS:

El Informe Técnico ATT-DTLTIC-INF TEC LP 231/2017 de 18 de abril de 2017 y sus anexos; el Informe Jurídico ATT-DJ-INF-JUR LP 692/2017 de 3 de mayo de 2017; las normas aplicables y todo lo que convino ver y se tuvo presente;

CONSIDERANDO 1: (Antecedentes).-

Que, el Informe Técnico ATT-DTLTIC-INF TEC LP 231/2017 de 18 de abril de 2017, emitido por el Analista de Tecnologías de Información vía Jefe de Regulación de Tecnologías de Información y Director Técnico Sectorial de Telecomunicaciones y TIC concluyó señalando que: la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - **ATT**, ha analizado los estándares de Agencias de Registro y la normativa internacional disponible con el objeto de la elaboración de un primer documento para el funcionamiento de las Agencias de Registro en nuestro país. En este entendido, se remitieron notas a veinticinco (25) entidades entre públicas y privadas a objeto de que analicen el documento “Estándar Técnico para el funcionamiento de las Agencias de Registro” y que presenten sus comentarios y observaciones, mismas que fueron atendidas por la ATT convocando a una reunión a las entidades que tenían más observaciones y consultas a objeto de perfeccionar el referido Estándar. Asimismo, señala que, para normar el funcionamiento de las Agencias de Registro, se tomaron en cuenta los estándares internacionales RFC 5280, Public Key Infrastructure Certificate and Certificate Revocation List (CRL) y WebTrust, Trust Service Principles and Criteria for Certification Authorities Version 2.0.

Que, en este contexto, Informe Técnico precitado señala: *“Para dar cumplimiento al artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo N° 1793, se recomienda aprobar el “ESTÁNDAR TÉCNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO” y sus anexos que son parte indivisible de este acto administrativo.(...) Al tratarse de un Instrumento regulatorio con alcance nacional deberá publicarse el correspondiente edicto en un Matutino de circulación nacional, así como en el portal WEB de la Institución.*

CONSIDERANDO 2: (Marco normativo aplicable).-

Que, el parágrafo II, Artículo 103 de la Constitución Política del Estado, determina que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación (TIC).

Que, las competencias y atribuciones de la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes están definidas por el Decreto Supremo N° 0071 de 9 de abril de 2009 (D.S. N° 0071) que conforme a la Disposición Transitoria Novena de la Ley N° 164 de 8 de agosto de 2011 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación (Ley N° 164) se denomina: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - **ATT**, asumiendo las atribuciones, competencias, derechos y obligaciones en materia de telecomunicaciones, tecnologías de información y comunicación, transportes y servicio postal, bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda.

Que, los incisos d) y l), Artículo 17 del **D.S. N° 0071**, establece entre las competencias de la **ATT**: *“d) Regular, controlar, supervisar, fiscalizar y vigilar la prestación de los servicios y actividades por parte*



1-LP-12990



LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 entre Av. Los Saucos 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 - 4-44581184 - 4-4581185

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

TARIJA: Avenida Las Américas Esquina O'Connor. Edificio Lizzie
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-6000 1 de 4
www.att.gob.bo



Resolución Administrativa Regulatoria

ATT-DI-RAR-TL LP 272/2017

de las entidades y operadores bajo su jurisdicción reguladora, y el cumplimiento de sus obligaciones legales y contractuales"; y "l) Implementar aspectos relativos a la regulación, control, fiscalización y supervisión de los sectores de telecomunicaciones y transportes, en el marco de la CPE".

Que, los incisos a) y f) del Artículo 19 del **D.S. N° 0071**, especifican entre otras atribuciones del Director Ejecutivo de la **ATT**, el de ejercer la administración y representación legal de la **ATT**, y asumir la responsabilidad de sus actos legales y administrativos en el marco de la Ley N° 1178 de 20 de julio de 1990 de Administración y Control Gubernamentales, y demás disposiciones legales vigentes; y el de ordenar y realizar los actos necesarios para garantizar el cumplimiento de los fines relativos a la **ATT**.

Que, los numerales 2 y 5 del Artículo 2 de la **Ley N° 164**, señala como objetivos de la Ley, entre otros, el de asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; y el promover el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.

Que, el Artículo 71 de la **Ley N° 164**, declara como prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos.

Que, la Disposición Transitoria Sexta de la **Ley N° 164**, señala que todos los aspectos que se requieran para la aplicación de la citada Ley, serán reglamentados por el Órgano Ejecutivo y regulados por la **ATT**.

Que, el Decreto Supremo N° 1793 de 13 de noviembre de 2013 (**D.S. N° 1793**), aprueba el Reglamento a la **Ley N° 164**, para el Desarrollo de Tecnologías de Información y Comunicación (TIC). Asimismo, el Artículo 24 del señalado Decreto 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 Artículo 37 del **D.S. N° 1793**, determina la estructura jerárquica de la organización de la Infraestructura Nacional de Certificación Digital, estableciendo cuatro (4) niveles: En un primer nivel esta la **ATT** como **Entidad Certificadora de Raíz**. En un segundo nivel, se encuentran las **Entidades Certificadoras**, tanto la pública (ADSIB) como privadas subordinadas a la **ATT**. En un tercer nivel, se encuentra la **Agencia de Registro**, como dependiente de una entidad certificadora, encargada de realizar el **registro y la identificación de la persona natural o jurídica** en forma fehaciente y completa. Asimismo, puede **aprobar o revocar un Certificado Digital**; y, por último, en un cuarto nivel, se ubican los **Signatarios**, que son todos los usuarios y usuarias finales a quienes se les ha emitido un Certificado Digital por una entidad certificadora.

Que, los incisos c) y j), Artículo 38 del **D.S. N° 1793**, establece las atribuciones específicas asignadas a la **ATT** dentro de la Infraestructura Nacional de Certificación Digital, que señalan: "c) Definir los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación;" y "j) Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones".

Que, el Artículo 40 del **D.S. N° 1793**, contiene las funciones de una Agencia de Registro, entre otras, la de recepción de solicitudes de emisión de certificados, comprobando la identidad y autenticación de los datos de los titulares certificados; la remisión de las solicitudes aprobadas a la Entidad Certificadora



LA PAZ: Calle 13 de Calacoto
N° 8260 - 8280 entre Av. Los Sauces
y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

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

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

TARIJA: Avenida Las Américas
Esquina O'Connor, Edificio Lizzie
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

**Línea Gratuita de Protección al
Usuario**
800-10-6000 2 de 4
www.att.gov.bo

**Resolución Administrativa Regulatoria**

ATT-DJ-RAR-TL LP 272/2017

(EC) con la que se encuentre vinculada, cumpliendo las disposiciones que establezca la política de certificación y el manual de procedimiento de EC y las normas y recaudos establecidos para la protección de los datos personales, manteniendo un archivo y conservación de toda la documentación de respaldo del proceso de validación. Asimismo, puede identificar y autenticar a los solicitantes de revocación de certificados.

Que, el inciso a), Artículo 43 del **D.S. N° 1793**, establece como obligación de las Entidades Certificadoras, el cumplir con la normativa vigente y los estándares técnicos emitidos por la **ATT**, mismas que aplican a las Agencias de Registro como entidad dependiente de las Entidades Certificadoras.

Que, el Artículo 13 de los Estándares Técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras, aprobados mediante **RAR ATT-DJ-RA-TL LP 32/2015** de 9 de enero de 2015, señala: Las Entidades Certificadoras Autorizadas (ECA) deberán establecer los requisitos y condiciones que deben cumplir las Agencias de Registro, basándose en lo establecido en los requisitos legales, económicos y técnicos del referido estándar según corresponda a una Agencia de Registro de una ECA pública o una Agencia de Registro de una ECA Privada.

CONSIDERANDO 3: (Análisis).-

Que, es necesario aprobar los Estándares Técnicos para el Funcionamiento de las Agencias de Registro y sus anexos, documentos que establecerán las disposiciones de carácter complementario a los Estándares técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras Autorizadas, respecto al registro, autorización, requisitos y servicios que brindaran las Agencias de Registro, que estarán operativamente vinculadas a las Entidades Certificadoras Autorizadas, para que la **ATT** como Entidad Certificadora de Raíz y como Autoridad de regulación y fiscalización, asumiendo sus atribuciones y competencias en materia de tecnologías de información y comunicación, fiscalice el cumplimiento de lo establecido en el referido **ESTÁNDAR TÉCNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO** y en sus anexos.

Que, en este contexto, el Informe Técnico **ATT-DTLTIC-INF TEC LP 231/2017** recomienda que: Para dar cumplimiento al inciso j), Artículo 38 del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo N° 1793, y aprobar el “**ESTÁNDAR TÉCNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO**” y sus anexos; y que al tratarse de un instrumento regulatorio con alcance nacional deberá publicarse el correspondiente edicto en un Matutino de circulación nacional, así como en el portal **WEB** de la Institución.

Que, el Informe Jurídico, señala que “*En virtud a los antecedentes citados y las disposiciones de orden legal mencionadas, se considera que la solicitud de emisión de Resolución Administrativa Regulatoria que apruebe “ESTÁNDAR TÉCNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO” y sus anexos (Anexo 1: Modelo de Contrato entre la ECA y la AR; Anexo 2: Política de Sistema de Accesos y Comunicación; Anexo 3: Políticas de Control y Monitoreo de la ECA y la AR), no contraviene a las normas vigentes, por lo tanto, se recomienda emitir la correspondiente Resolución*”.

CONSIDERANDO 4: (Competencia):

Que, las competencias y atribuciones de la **ATT**, definidas por el Decreto Supremo N° 0071 de 09 de abril de 2009 y conforme a lo dispuesto en la Disposición Transitoria Novena de la Ley N° 164, quedan sometidas a ésta las personas naturales y jurídicas, privadas, comunitarias, públicas, mixtas y



LA PAZ: Calle 13 de Calacoto
N° 8260 - 8280 entre Av. Los Sauces
y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián
N° 683 esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-44581184
4-4581185

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

TARIJA: Avenida Las Américas
Esquina O' Connor, Edificio Lizzie
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-6000 3 de 4
www.att.gob.bo



Resolución Administrativa Regulatoria

ATT-DJ-RAR-TL LP 272/2017

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.

POR TANTO:

El Director Ejecutivo de la ATT, Ing. Roque Roy Méndez Soletto designado mediante Resolución Suprema N° 19249 de 3 de agosto de 2016, en uso de sus atribuciones conferidas por ley y demás normas vigentes, a nombre del Estado Plurinacional de Bolivia;

RESUELVE:

PRIMERO.- APROBAR, el Informe Técnico ATT-DTLTIC-INF TEC LP 231/2017 de 18 de abril de 2017 y el Informe Jurídico ATT-DJ-INF-JUR LP 692/2017 de 3 de mayo de 2017, que sustentan el presente acto administrativo, mismos que se adjuntan a la presente Resolución.

SEGUNDO.- APROBAR, el “ESTÁNDAR TÉCNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO” y sus anexos que forman parte indivisible e inseparable de la presente Resolución:

- Anexo 1: Modelo de Contrato entre la ECA y la AR;
- Anexo 2: Política de Sistema de Accesos y Comunicación;
- Anexo 3: Políticas de Control y Monitoreo de la ECA y la AR.

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

Regístrese, comuníquese y archívese.


Ing. Roque Roy Méndez Soletto
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



1-LP-12990



LA PAZ: Calle 13 de Calacoto
N° 8260 - 8280 entre Av. Los Sauces
y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián
N° 683 esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-44581184
4-4581185

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

TARIJA: Avenida Las Américas
Esquina O'Connor, Edificio Lizzie
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al
Usuario
800-10-6000 4 de 4
www.att.gob.bo



**AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES**

***ESTANDAR TECNICO PARA EL FUNCIONAMIENTO DE
LAS AGENCIAS DE REGISTRO***

Tabla de contenido

Capítulo I Disposiciones Preliminares	4
Artículo 1 (Objeto).-.....	4
Artículo 2 (Normativa Aplicable).-	4
Artículo 3 (Abreviaturas).-	4
Artículo 4 (Definiciones).-.....	4
Capítulo II Agencias de Registro.....	5
Artículo 5 (Dependencia de las Agencias de Registro).-.....	5
Artículo 6 (Objetivo de una AR).-.....	6
Artículo 7. (Servicios que brinda una AR).-	6
Artículo 8 (Oficiales de Registro - OR).-	6
Artículo 9 (Alcance de una AR).-	6
Artículo 10 (Sistemas de acceso entre la ECA y sus AR).-	6
Artículo 11 (Control y monitoreo de la ECA a sus AR).-.....	7
Artículo 12 (Vinculación con una ECA).-	7
Artículo 13 (Requisitos de una AR dependiendo de una ECA).-.....	7
Artículo 14 (Notificación para el registro de una AR a la ATT).-	7
Artículo 15 (Auditoría Técnica de cumplimiento a la AR).-	8
Artículo 16 (Tarifas por la prestación del servicio).-	8
Artículo 17 (Servicio de soporte).-.....	8
Artículo 18 (Responsabilidades).-.....	8
Capítulo III Procesos de una Agencia de Registro.....	9
Artículo 19 (Equipamiento y capacitación).-.....	9
Artículo 20 (Procesos de registro).-.....	9
Artículo 21 (Inventario de Dispositivos).-.....	9
Artículo 22 (Registro de pago por la emisión y entrega de certificados).-	9
Artículo 23(Autenticación de la identidad del solicitante del certificado).-	9
Artículo 24(Verificar impedimentos para la emisión del certificado).-.....	9
Artículo 25(Recolección de evidencia presencial).-.....	9
Artículo 26 (Verificación de requisitos).-.....	10
Artículo 27 (Recopilar información de contacto y revocación).-.....	10
Artículo 28 (Envío de la solicitud de los certificados digitales a la ECA).-	10
Artículo 29 (Revocación, suspensión y reactivación de certificados).-.....	10
Artículo 30 (Notificaciones al solicitante).-.....	10
Capítulo IV Otros Aspectos.....	10

Artículo 31 (Incumplimiento).-.....	10
Artículo 32 (Modificaciones al reglamento).-.....	10
Anexo 1	11
MODELO DE CONTRATO ENTRE LA ECA Y LA AR.....	11
Anexo 2	13
POLÍTICA DE SISTEMA DE ACCESOS Y COMUNICACIÓN	13
Anexo 3	16
POLÍTICAS DE CONTROL Y MONITOREO ENTRE LA ECA Y LA AR.....	16

ESTANDAR TECNICO PARA EL FUNCIONAMIENTO DE LAS AGENCIAS DE REGISTRO

Capítulo I Disposiciones Preliminares

Artículo 1 (Objeto).- Establecer las disposiciones de carácter complementario a los Estándares técnicos y otros lineamientos establecidos para el funcionamiento de las Entidades Certificadoras, con respecto a la autorización, requisitos y servicios que brindan las Agencias de Registro, que estarán operativamente vinculadas a las Entidades Certificadoras Autorizadas.

Artículo 2 (Normativa Aplicable).- La normativa aplicable al presente

- Los artículos del 78 al 84 de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, Ley N° 164, de 08 de agosto de 2011.
- Los artículos del 24 al 56 del Reglamento a la Ley N° 164, de 08 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación aprobado por el Decreto Supremo N° 1793.

Artículo 3 (Abreviaturas).-

ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

ADSIB: Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

ECA: Entidad Certificadora Autorizada.

AR: Agencia de Registro.

ECR: Entidad Certificadora Raíz.

HTTP (Hypertext Transfer Protocol): Protocolo de Transferencia de Hipertexto.

FTP (File Transfer Protocol): Protocolo de Transferencia de Ficheros.

CRL (Certificate Revocation List) Lista de Certificados Revocados.

OCSP (Online Certificate Status Protocol): Protocolo de Estado de Certificados en Línea.

PKI (Public Key Infrastructure): Infraestructura de Clave Pública.

ID: Identificador de Usuario.

Artículo 4 (Definiciones).-

Políticas de Certificación (PC): La Política de Certificación contiene las directivas generales de operación de la ECA, para la emisión de certificados digitales, el ámbito de aplicación y los lineamientos para su funcionamiento.

Declaración de Practicas de Certificación (DPC): Contiene las prácticas y/o actividades que realiza la ECA para realizar sus operaciones generales, la gestión del ciclo de vida de los certificados y de su Lista de Certificados Revocados - CRL.

Lineamientos para terceros aceptantes (LT): Establece 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.

Oficiales de Registro (OR): Personal dependiente de una Agencia de Registro que está encargado del proceso de registro de una persona natural o jurídica para la obtención de un Certificado Digital.



Handwritten signature or initials.

Dispositivos criptográficos: Es un dispositivo criptográfico (token o HSM) basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas. Estos dispositivos deben cumplir las especificaciones del estándar FIPS 140-2 dentro de la normativa boliviana.

FIPS 140-2: Estándar de seguridad que deben cumplir los dispositivos criptográficos (FIPS por sus siglas en inglés Federal Information Processing Standard).

PIN (Personal Identification Number)- Número de identificación personal: Es el tipo de dato de activación y es definido por el signatario. Tiene que ser protegido por el mismo con el fin de prevenir el uso no autorizado de las claves privadas de los certificados de firma digital almacenadas en un dispositivo criptográfico.

Solicitante: Persona natural o jurídica que, facultada por las políticas establecidas por la ECA, presenta una solicitud de emisión de un certificado digital.

Agencias de Registro públicas: Entidades públicas que se constituyen en Agencias de Registro.

Agencias de Registro privadas: Personas jurídicas que se constituye en Agencias de Registro.

Tercerización del servicio de registro: Es una forma de prestación de servicios de certificación digital de una ECA, la que se encarga o delega procedimientos propios especificados en su Política de Certificación y su Declaración de Prácticas de Certificación a una Agencia de Registro, los cuales corresponden al servicio de registro de personas naturales o jurídicas para la obtención de un certificado digital.

Firewall: es un mecanismo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Capítulo II

Agencias de Registro

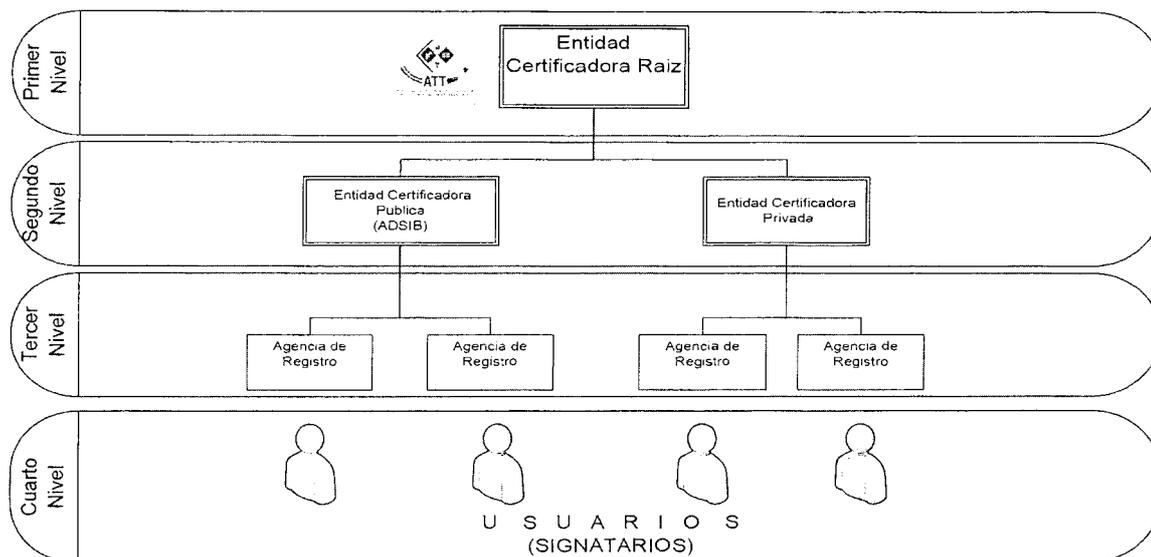
Artículo 5 (Dependencia de las Agencias de Registro).-

Dentro de la Jerarquía de la Infraestructura de Clave Pública del Estado Plurinacional de Bolivia la ATT se constituye en la Entidad Certificadora Raíz que autoriza a las Entidades Certificadoras Autorizadas tanto pública como privadas a brindar servicios de certificación digital.

Las Agencias de Registro, dependientes de una ECA, permiten realizar el registro y la identificación de los solicitantes, estableciéndose en diferentes regiones del país, ampliando de esta manera el campo de prestación del servicio de registro para solicitar el Certificado Digital.



[Handwritten signature]



Artículo 6 (Objetivo de una AR).-

El objetivo principal de una AR es la de tercerizar el servicio de registro de una ECA asegurándose de la veracidad de los datos de los solicitantes que son utilizados para solicitar un certificado digital, debiendo realizar este servicio de manera fehaciente y completa con absoluta fidelidad a la realidad.

La AR, no firma o emite certificados digitales, se encarga del registro e identificación de los solicitantes al momento de solicitar un certificado digital.

Artículo 7. (Servicios que brinda una AR).-De acuerdo al numeral 3), Artículo 37 del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que aprueba el Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación, una Agencia de Registro brinda los siguientes servicios:

- a) Registro e identificación de la persona natural o jurídica en forma fehaciente y completa.
- b) Se encarga de solicitar la aprobación o revocación de un certificado digital.

Artículo 8 (Oficiales de Registro - OR).- Una AR deberá asegurarse de que sus OR estén debidamente capacitados, asimismo la AR deberá remitir la lista de OR a su ECA para su verificación, posteriormente deberá remitir a la ATT la lista actualizada de dichos oficiales a efectos de registro en los procesos de auditoría.

Artículo 9 (Alcance de una AR).- I. Una Agencia de Registro vinculada operativamente a una ECA deberá especificar el alcance de sus servicios, los tipos de certificados digitales que comercializara que podrían estar de acuerdo a sus propósitos y/o líneas de negocio.

II. En el caso de las Agencias de Registro públicas el alcance podrá ser reducido a su sector de competencia.

Artículo 10 (Sistemas de acceso entre la ECA y sus AR).- I. La ECA y sus AR dependientes deben contar con conexión que garantice los procesos que requieran el intercambio de información entre estas instancias.



[Handwritten signature]

II. La ECA y sus AR deberán contar con un documento que explique las políticas de su sistema de accesos y comunicación para brindar servicios de acuerdo a los puntos descritos en el Anexo 2.

Artículo 11 (Control y monitoreo de la ECA a sus AR).- La ECA deberá tener un procedimiento de control y monitoreo constante a sus AR dependientes mínimamente de los puntos descritos en el Anexo 3.

Artículo 12 (Vinculación con una ECA).- Una Agencia de Registro se vinculará a una ECA mediante un contrato y/o convenio que especifique las funciones delegadas, el compromiso de cumplimiento con las políticas del ente dependiente y las responsabilidades administrativas que se acuerden entre las dos instancias, de acuerdo al Anexo 1.

Artículo 13 (Requisitos de una AR dependiendo de una ECA).- La ECA deberá publicar vía web los requisitos mínimos que debe cumplir una AR para que pueda brindar el servicio de registro bajo su dependencia, mínimamente se deben considerar los siguientes aspectos:

- Requisitos de conectividad, comunicación y seguridad entre la ECA y una AR.
- Requisitos del equipamiento que necesita una AR.
- Requisitos para el personal idóneo para ser un OR.
- Procedimientos de recepción, manejo, envío y archivo de la documentación de los signatarios.
- Procedimientos a cumplir por las AR de acuerdo a sus Políticas de Certificación y su Declaración de Practicas de Certificación.

Artículo 14 (Notificación para el registro de una AR a la ATT).- Toda organización que se constituya como Agencia de Registro de una ECA deberá ser registrada en la ATT para lo que tendrá que remitir la siguiente información:

1. Carta de solicitud:

- I. Nota o memorial de solicitud de registro de la AR con la siguiente información:
 - a. Empresa o institución:
 - i. Fotocopia de Documento de Constitución, debidamente registrado en Fundempresa, si correspondiese.
 - ii. Fotocopia de Testimonio del Poder registrado en FUNDEMPRESA, o de documento que acredite al personero que ejerce la representación legal.
 - iii. Número de Identificación Tributaria.
 - b. Dirección oficina central:
 - c. Pública o privada:
 - d. Numero de agencias:
 - e. Nombre, direcciones y teléfonos de cada agencia:
 - f. Lista de Oficiales de Registro:
 - g. Teléfono(s) y fax:
 - h. Correo electrónico:
 - i. Casilla postal:
 - j. Página web de referencia:

2. Contrato entre la ECA y la AR.

3. Solicitud de fecha y hora para la auditoría técnica de cumplimiento.



Artículo 15 (Auditoria Técnica de cumplimiento a la AR).- En cumplimiento de los procedimientos especificados en el artículo precedente, en la realización de la Auditoria Técnica de Cumplimiento, tanto la AR como la ECA podrán aportar elementos de juicio o indicios destinados a demostrar que el servicio se prestara cumpliendo los procedimientos de la presente normativa, las Políticas de Certificación, la Declaración de Practicas de Certificación y los procedimientos de registro de la ECA.

Verificación del cumplimiento de requisitos

- a) La verificación será realizada por la ATT, utilizando como herramienta una lista de verificación elaborada para el efecto.
- b) Una vez verificados y aprobados los requisitos establecidos en la lista de verificación, las entidades deben coordinar con la ATT el registro de la AR.

Este proceso debe realizarse conjuntamente entre el personal de la ATT y el personal técnico de las entidades involucradas con el objetivo de que pueda realizarse esta labor en un cronograma propuesto por la AR y la ECA, en forma previa al inicio de actividades de la AR.

Artículo 16 (Tarifas por la prestación del servicio).- I. La ECA y la AR establecerán sus tarifas considerando criterios sustentados y orientados a costos de registro para la certificación digital.

II. La ECA deberá presentar esta estructura tarifaria a la ATT para su registro.

Artículo 17 (Servicio de soporte).- La AR como parte del servicio de registro debe implementar los mecanismos necesarios para que, cada vez que entregue un certificado digital a un signatario, ésta informe, al menos sobre los siguientes tópicos:

- I. Servicio de soporte: La AR deberá brindar la asistencia necesaria a sus signatarios para ayudarles a resolver los problemas que se les pueda presentar mientras hacen uso de los servicios de firma y certificación digital y deberán informar a los mismos de los medios por los cuales podrán solicitar este servicio (vía web, telefónica u otros).
- II. Revocación de certificados: Informar al signatario que la revocación de los certificados la puede realizar por medio de la página de la ECA o la AR, presencialmente o por teléfono ante la AR y la ECA. Se debe instruir al signatario que la suspensión o revocación procede cuando sospeche del compromiso de su clave privada (robo, pérdida, extravío del Dispositivo de Hardware de Seguridad) o por voluntad propia decida no poseer más certificados digitales a su nombre.
- III. Informar que en el caso de que elija la revocación del certificado digital no podrá recuperar su clave privada; en el caso de que sea suspensión del certificado digital deberá indicarle al solicitante que tendrá un plazo para la reactivación sino, pasa a revocación definitiva.
- IV. Deberá proveer el software de instalación de dispositivos comercializados por la AR.
- V. La AR deberá poner a disposición de sus signatarios los mecanismos necesarios para la recepción de reclamos (ODECO).

Artículo 18 (Responsabilidades).- I. La operación de todo el ciclo de registro de los signatarios y la emisión de los certificados digitales es responsabilidad de la ECA. Para efectos de auditoría técnica la AR y la ECA deberán ser responsables de demostrar su funcionamiento adecuado.

II. La ATT podrá realizar auditorías programadas a la ECA y la AR en cualquier momento.



J
A

Capítulo III

Procesos de una Agencia de Registro

Artículo 19 (Equipamiento y capacitación).- La Agencia de Registro debe contar con equipamiento adecuado y personal capacitado de acuerdo a los requerimientos técnicos de la ECA de la cual depende.

Artículo 20 (Procesos de registro).- Una AR, mínimamente deberá tener los siguientes procesos de registro:

- a) Inventario de Dispositivos (Token o HSM).
- b) Registro de pago por la emisión y entrega de certificados.
- c) Autenticación de la identidad del solicitante del certificado.
- d) Verificación de impedimentos para emisión del certificado.
- e) Recolección de evidencia presencial.
- f) Verificación de requisitos
- g) Recopilación de información de contacto y revocación.
- h) Envío de la solicitud de la emisión de los certificados digitales a la ECA firmado digitalmente por la AR.
- i) Informar a la ECA para la Generación del Certificado Digital, Revocación, Suspensión y reactivación de certificados digitales.

Artículo 21 (Inventario de Dispositivos).-El registro del inventario de dispositivos de hardware de seguridad (token o HSM) del solicitante es un requisito previo por medio del cual se asocia al signatario el token que debe contar con el tipo de dispositivo, marca, modelo y/o número de serie.

Artículo 22 (Registro de pago por la emisión y entrega de certificados).- La ECA deberá definir un procedimiento de pagos y ponerlo a disposición de las AR por el servicio de Certificación Digital para sus signatarios.

Artículo 23 (Autenticación de la identidad del solicitante del certificado).-La ECA debe poner a disposición de las AR un sistema de autenticación de la identidad del solicitante para verificar los datos correctos mediante el número de carnet de identidad del mismo.

Artículo 24 (Verificar impedimentos para la emisión del certificado).-La AR deberá verificar con el sistema proporcionado por la ECA que no existan los siguientes impedimentos para la emisión del Certificado Digital:

- Que el solicitante sea menor de edad.
- Que el documento de identidad no esté vigente.
- Que no se valide la identidad.

En el caso de existir un impedimento no se emitirá ningún certificado digital. Cuando la AR detecte que el solicitante tiene alguno de los impedimentos señalados en los puntos anteriores, el sistema no permitirá continuar con el proceso y el OR debe proceder a explicarle al solicitante la causa del impedimento y recomendarle que se dirija a la autoridad competente para resolver su problema.

Artículo 25 (Recolección de evidencia presencial).- La AR debe recolectar y guardar en el sistema evidencia que permita dejar constancia de la presencia física del solicitante durante el proceso de registro de solicitudes.



[Handwritten signature]

Por esta razón, la AR debe tomar una fotografía al solicitante, capturar al menos una huella digital y especificar la información de contacto y revocación.

La AR no debe firmar ni continuar el proceso en caso de duda con respecto a lo anterior.

Artículo 26 (Verificación de requisitos).- I. La AR debe verificar los requisitos que debe cumplir el solicitante de acuerdo al tipo de certificado digital que se requiera.

II. En el caso de que el solicitante cuente con un dispositivo de hardware de seguridad propio, la AR debe verificar que el mismo cumpla con los estándares definidos por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT.

Artículo 27 (Recopilar información de contacto y revocación).- La AR debe garantizar que la información de contacto y revocación especificada fue definida por el solicitante durante el proceso de registro y que la misma fue confirmada. La AR debe comunicarle al solicitante la importancia de suministrar información veraz y que pueda recordar con facilidad ya que esta podrá ser utilizada para contactarlo o bien en caso de un eventual proceso de revocación del certificado.

Artículo 28 (Envío de la solicitud de los certificados digitales a la ECA).-La AR debe enviar todos los requisitos cumplidos por el signatario en formato digital junto a un requerimiento a la ECA firmada digitalmente.

Artículo 29 (Revocación, suspensión y reactivación de certificados).- El servicio de revocación, suspensión y reactivación de certificados al suscriptor se realizará través de los medios que disponga la ECA, en un horario de 24 horas diarias los 7 días de la semana, y que la AR debe comunicarle al signatario cuales son los medios para gestionar estos procesos.

Artículo 30 (Notificaciones al solicitante).- El solicitante deberá ser notificado por la AR una vez que la ECA haya firmado, revocado, suspendido o reactivado su Certificado Digital.

Capítulo IV Otros Aspectos

Artículo 31 (Incumplimiento).- El incumplimiento a cualquier disposición del mismo implica una infracción contra las atribuciones de la Autoridad Reguladora, de acuerdo a los alcances del Reglamento de Sanciones vigente.

Artículo 32 (Modificaciones al reglamento).- El presente estándar está sujeto a modificaciones de acuerdo al artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo N° 1793.



Anexo 1
MODELO DE CONTRATO ENTRE LA ECA Y LA AR

Conste por el tenor del presente Documento Privado, que los suscribientes acuerdan celebrar un Contrato la delegación del servicio de registro a la Agencia de Registro (AR) por parte de la Entidad Certificadora Autorizada (ECA).

PRIMERA (PARTES INTERVINIENTES).- Los datos de la ECA y la AR, así como de sus representantes.

SEGUNDA (ANTECEDENTES).- Normativa a la cual se rigen ambas instituciones, así como sus funciones y las motivaciones que hacen al contrato.

TERCERA (OBJETO DEL CONTRATO).- Describir el objeto del Contrato del servicio.

CUARTA (ALCANCE).- Las obligaciones, procedimientos entre las partes y los detalles de corresponsabilidad entre las mismas.

QUINTA (INVIOABILIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE LA USUARIA O USUARIO).- Establecer la manera de proteger la información proporcionada entre las partes, así como de sus usuarios finales o signatarios.

SEXTA (PROCESOS DE COORDINACION).- Establecer y describir los procesos establecidos para la coordinación entre las partes para brindar el servicio.

SÉPTIMA (SOLUCION DE CONTROVERSIAS).- Describir los procesos o procedimientos para la solución de controversias entre las partes.

OCTAVA (ESTRUCTURA TARIFARIA).- Establecer la estructura tarifaria de acuerdo a los términos en que la ECA delegara los servicios de registro a la AR.

NOVENA (FACTURACIÓN Y COBRANZA).- Establece los medios de pago entre las partes.

DÉCIMA (EXENCIONES DE RESPONSABILIDAD).- Descripción para ECA/ AGENCIA DE REGISTRO, en consideración a los marcos legales aplicables, sobre el servicio, la responsabilidad civil y penal u otro que se considere pertinente. Causales y condiciones bajo las cuales deba efectuarse la Revocatoria.

DÉCIMA PRIMERA (ATENCIÓN DE RECLAMOS Y SERVICIOS DE INFORMACION Y ASISTENCIA).- Establecer, y detallar los horarios días de atención, teléfono(s) y dirección del mismo entre las partes.

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

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

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



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



Anexo 2
POLÍTICA DE SISTEMA DE ACCESOS Y COMUNICACIÓN

De acuerdo al Estándar WebTrust, la Política de sistema de accesos y comunicación deberá contener el siguiente contenido mínimo:

Gestión de los Sistemas de Acceso

Criterio:

La ECA mantiene controles para proporcionar una seguridad razonable de que el acceso al sistema está limitado a las personas autorizadas. Estos controles ofrecen una seguridad razonable de que:

- el sistema operativo y la base de datos de acceso están limitados a las personas autorizadas con privilegios de tareas predeterminadas;
- el acceso a los segmentos de la red donde se encuentran los sistemas de la ECA se limita a las personas, las aplicaciones y servicios autorizados, y;
- el uso de la aplicación de la ECA está limitada a las personas autorizadas.

Controles Ilustrativos:

Gestión de acceso de usuarios

1. Los requerimientos del negocio de control de acceso son definidos y documentados en una política de control de acceso que incluya al menos lo siguiente:
 - a) roles y permisos de acceso correspondientes;
 - b) la identificación y el proceso de autenticación para cada usuario;
 - c) la separación de funciones, y;
 - d) el número de personas necesarias específicas para llevar a cabo operaciones entre la ECA y la AR.
- 2 Existe un procedimiento formal de registro de usuario y cancelación de registro para el acceso a los sistemas y servicios de información de la ECA y la AR.
- 3 La asignación y uso de privilegios está restringido y controlado.
- 4 La asignación de contraseñas se controla a través de un proceso formal de gestión.
- 5 Los derechos de acceso para usuarios con roles de confianza son revisados periódicamente y actualizados.
- 6 Los usuarios deben seguir las políticas y procedimientos definidos en la selección y uso de contraseñas.
- 7 Los usuarios deben asegurarse de que el equipamiento desatendido tiene la protección adecuada.

Control de Acceso a la Red

- 8 El personal empleado de la ECA y la AR tiene conexión directa sólo a los servicios que han sido específicamente autorizados para su uso. La ruta desde la terminal de usuario a los servicios informáticos es controlada.



[Handwritten signature]
[Handwritten signature]

9 El acceso remoto a los sistemas de la ECA, hecho por los empleados de la ECA y la AR o sistemas externos, si así se los permite requieren autenticación.

10 Las conexiones realizadas por los empleados o los sistemas de la ECA a sistemas informáticos remotos se autentican.

11 El acceso a los puertos de diagnóstico está bien controlado.

12 Existen los controles (por ejemplo, firewalls) para proteger el dominio de la red interna de la ECA y la AR de cualquier acceso no autorizado de cualquier otro dominio.

13 Los controles limitan los servicios de red (por ejemplo, HTTP, FTP, etc.) y están disponibles para los usuarios autorizados de conformidad con las políticas de control de acceso de la ECA y la AR. Los atributos de seguridad de todos los servicios de red utilizados por la organización de la ECA son documentados por la ECA y la AR.

14 Existen los controles de enrutamiento para asegurar que las conexiones de las computadoras y los flujos de información no violan la política de control de acceso de la ECA.

15 La ECA y la AR de acuerdo a sus características, mantienen los componentes del equipamiento y de la red local (por ejemplo, firewalls y routers) en un entorno físicamente seguro y audita periódicamente sus configuraciones para el cumplimiento de los requisitos de configuración de la EC.

16 Los datos confidenciales son encriptados cuando se intercambian a través de redes públicas o no confiables

El Sistema Operativo y el control de acceso a las Bases de Datos

17 Los sistemas operativos y las bases de datos se configuran de acuerdo con las normas de configuración de sistema de la ECA y periódicamente revisados y actualizados.

18 El sistema operativo y los parches de base de datos y las actualizaciones se aplican de manera oportuna cuando se consideran necesarias en función de una evaluación de riesgos.

19 La identificación automática de la terminal se utiliza para autenticar las conexiones a lugares específicos y a equipos portátiles.

20 El acceso a los sistemas de la ECA requiere un proceso de inicio de sesión seguro.

21 Todos los usuarios que sean empleados de la ECA y de la AR tienen un identificador único (ID de usuario) para su uso personal para que las actividades realizadas se puedan rastrear hasta la persona responsable. Dónde se requieren cuentas de grupo, existen otros controles de vigilancia que se aplican para mantener la responsabilidad individual.

22 El uso de las utilidades de los programas del sistema están restringidos a personal autorizado y están estrictamente controlados.

23 Las terminales inactivas de la ECA y la AR requieren re-autenticación antes de su uso.

24 Las restricciones en los tiempos de conexión se utilizan para proporcionar seguridad adicional para aplicaciones de alto riesgo.

25 Los datos confidenciales están protegidos contra la divulgación a los usuarios no autorizados.



J
R

Control de Acceso a las Aplicaciones

26 El acceso a las funciones de información y sistemas de aplicaciones está restringidos de acuerdo con la política de control de acceso de la ECA y la AR.

27 El personal de la ECA y de la AR se identifica y autentica con éxito, antes de utilizar aplicaciones críticas relacionadas con la administración de certificados.



*J
R*

Anexo 3

POLÍTICAS DE CONTROL Y MONITOREO ENTRE LA ECA Y LA AR

La ECA mantiene controles efectivos para proporcionar una seguridad razonable de que las solicitudes de certificados digitales de la AR son exactas, autenticados y autorizados.

Gestión del ciclo de vida de un certificado digital de una AR

Criterio:

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

- Las solicitudes de certificados digitales de la AR son exactas, y los datos autenticados y autorizados;
- Las solicitudes de renovación de certificados digitales de la AR son exactos, autorizados, completos;
- Las solicitudes nuevas y renovaciones de certificados digitales de la AR se generan y se emiten de conformidad en la ECA de acuerdo a sus políticas de certificación y declaración de prácticas;
- La información al signatario del estado de certificados es oportuna, completa, exacta (incluyendo el acceso a las CRL y otros mecanismos de estado de certificados) y se pone a disposición de cualquier entidad, de acuerdo con las prácticas comerciales divulgadas de la ECA.

Controles Ilustrativos:

Registros de una AR

- 1 La ECA autentica las solicitudes de certificados de la AR de conformidad con la PC.
- 2 La ECA lleva a cabo una evaluación del cumplimiento de los requisitos del certificado digital del solicitante con los requisitos de la PC de la AR antes de aprobar una solicitud de certificado.

Distribución de certificados de la AR

- 3 La ECA firma certificados digitales de acuerdo a las solicitudes de la AR para los usuarios finales o signatarios utilizando un mecanismo establecido de conformidad con la PC.
- 4 La ECA verifica la identidad y la autoridad de la AR que solicita la revocación de un certificado de conformidad con la PC de la AR.
- 5 La ECA actualiza la lista de revocación de certificados (CRL) y otros mecanismos de estado de certificados sobre la revocación del certificado de conformidad con la PC.
- 6 La ECA hace que la información de estado de los certificados digitales solicitados por la AR se encuentren disponibles para las Partes que Confían usando un mecanismo establecido (por ejemplo, CRL, OCSP, etc.), de conformidad con la PC de la ECA.



J
R