ENTIDAD CERTFICADORA RAIZ

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	09 de enero de 2015
Autor	ATT
Versión	1
Comentario	
Publicación	Público

DIRECCIÓN JURÍDICA V°B° L.D.V.A. A.T.T.

JEFE DE OPERACIONES DIRECCIÓN JURÍDICA V°B° R.L.O.O. A.T.T.

ELABORADO POR: L.A.M.C. A.T.T.

DIRECCIÓN JURÍDICA V°B° P.D.B.S. A.T.T.

Enero 2015

CONTENIDO

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

DIRECCIÓN JURÍDICA V° B° L.D.V.A. A.T.T.

JEFE DE OPERACIONES ESTE DIRECCIÓN JURÍDICA V° B° R.L.O.O. A.T.T.

ELABORADO POR: E.A.M.C. A.T.T.

DIRECCIÓN JURÍDICA V° B° P.D.E.S.C. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

Línea Gratuita de Protección al Usuario 800-10-6000 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 Nº 164 de fecha 8 de agosto de 2011, en el Reglamento para el Desarrollo de las TIC, Decreto Supremos Nº 1793 del 13 de noviembre de 2013 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 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.

---

[1] Internet Engineering Task Force (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).

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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.

Las ECA emiten certificados digitales a las personas naturales, las personas jurídicas públicas o privadas y certificados para los cargos públicos. 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 Nº164.

1.1.1 OBLIGACIONES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS

En particular, de acuerdo al artículo 43 del Decreto Reglamentario, las ECA están obligadas a:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;

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;

c) Informar a los usuarios de las condiciones acordadas para la emisión, validación, renovación o 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;

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;

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 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;

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.

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 privadas deberán rendir una caución que será utilizada para responder por las eventuales consecuencias civiles contractuales o extracontractuales de su actividad.

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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

- 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: 1.0

Fecha de emisión del documento: 09/01/2015

Fecha de la última actualización: 09/01/2015

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

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

UNIDAD TIC 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.

Los participantes de la Infraestructura antes mencionada son:

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

- 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 38 del Decreto Supremo N° 1793, 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.

- 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 antes mencionado.

- ECA: Entidades Certificadoras Autorizadas, de segundo nivel subordinadas a la ECR, que cumplieron los requisitos exigidos para la autorización de prestación del servicio, emiten

DIRECCIÓN JURÍDICA V°B° R.L.O.V.A. A.T.T.
JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V°B° R.L.O.O. A.T.T.
ELABORADO POR: E.A.M.C. A.T.T.
DIRECCIÓN JURÍDICA V°B° P.M.R.S.A. A.T.T.

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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

certificados a los signatarios finales, sus funciones se establecen en el Artículo 39 del Decreto Supremo N° 1793 antes mencionado y 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 de la persona natural o jurídica;
e) Reconocer y validar los certificados digitales emitidos en el exterior;
f) Otras funciones relacionadas con la prestación de servicios de certificación Digital.

- 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, 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;

DIRECCIÓN JURÍDICA V° B° L.D.V.A. A.T.T.
JEFE DE OPERACIONES DIRECCIÓN JURÍDICA V° B° R.L.C.O. A.T.T.
FOLIADO POR: E.A.M.C. A.T.T.
DIRECCIÓN JURÍDICA V° B° R.D.E.S.C. A.T.T.

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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 emitido por una EC. 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 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, 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.

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

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 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 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 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.

DIRECCIÓN JURÍDICA V° B° I.D.V.A.Y. A.T.T.

1.6 DEFINICIONES Y ABREVIATURAS

JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V° B° A.T.T.

ITU-T: (*International Telecommunication Union*) Unión Internacional de Telecomunicaciones. Sector de Normalización de las Telecomunicaciones

ELABORADO POR: E.A.M.C. A.T.T.

IETF: (*Internet Engineering Task Force*) Grupo de Trabajo de Ingeniería de Internet

RFC: (*Request for 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

DIRECCIÓN JURÍDICA V° B° D.P.M.R.S. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 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 PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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.

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 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, 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

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

definición: CN (Common Name) = 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.

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, 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 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.

Luego, la ECA presenta la solicitud de emisión de certificado a la ATT 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

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 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, ATT podrá revocar su certificado, teniendo en cuento 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 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 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.

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

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

4.5. 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 cuenten con formal y debida autorización por parte de la ECA para efectuar dicha solicitud, la ATT o una autoridad judicial competente conforme a Ley. La presentación debe realizarse por escrito con nota dirigida a la ATT 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 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:

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;
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;
f) Cuando la ECA, luego de haber recibido una notificación de la ATT, 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 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.

DIRECCIÓN JURÍDICA V° B° L.D.V.A. A.T.T.
JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V° B° R.L.O. A.T.T.
ELABORADO POR E.A.M.C. A.T.T.

DIRECCIÓN JURÍDICA V° B° P.P.D.R.S.C. A.T.T.

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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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.

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

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.

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 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 certificado de cargos públicos, dos (2) años y seis (6) meses, antes de la fecha finalización de vigencia de su certificado.
- 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 tres 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, cuyo certificado tiene una vigencia de cinco (5) años. pasado los dos años, por ejemplo, no podrá emitir un certificado digital a una persona

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 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.

DIRECCIÓN JURÍDICA V°B° D.L.D.V.A. A.T.T.
JEFE DE OPERACIÓN JURÍDICA DIRECCIÓN JURÍDICA V°B° R.L.O.P. A.T.T.
ELABORADO POR: R.A.M.C. A.T.T.
DIRECCIÓN JURÍDICA V°B° P.P.P. R.S.C. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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

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.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 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.
- 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.

DIRECCIÓN JURÍDICA V° B° L.D.V.A. A.T.T.
JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V° B° R.L.O. A.T.T.
ELABORADO POR: E.A.M.C. A.T.T.
DIRECCIÓN JURÍDICA V° B° P.D.R.S.S. A.T.T.

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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 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.

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 mantiene registros de auditoria 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.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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

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 ha desarrollado 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 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.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 ha desarrollado 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.
- Falias 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 falla 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 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 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.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

- 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, con al menos tres (3) meses de anticipación sobre el destino que dará a los certificados digitales emitidos.

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 Nº 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;
- 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 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 Nº 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: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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 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 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 deberá resguardar de acuerdo a los procedimientos administrativos del Estados, 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 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.

Las ECA generan sus claves de acuerdo a lo establecido en el Manual de Ceremonias de generación de claves aprobado por la ATT 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.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

6.2. PROTECCIÓN CRIPTOGRÁFICA DE LA CLAVE PRIVADA

La debida protección de las claves de la ECR es responsabilidad de la ATT 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. 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 ha desarrollado 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 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.

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

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

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.

DIRECCIÓN JURÍDICA V° B° L.D.V.A. A.T.T.

JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V° B° R.L.O.O. A.T.T.

LABORADO POR: E.A.C.C. A.T.T.

DIRECCIÓN JURÍDICA V° B° P.D.L.S.V. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 de acuerdo a ISO3166
Validez (desde, hasta) Valid from/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 de acuerdo a ISO3166.
Clave Pública del suscriptor (Subject Public 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 (Certificate Policies)	URI: (Archivo en formato de texto).
Restricciones Básicas (basicContraints)	CA = TRUE, pathLenConstriant = "1".
Punto de distribución de la Lista de certificados Revocados (CRL Distribution Points)	URI: (.crl).

DIRECCIÓN JURÍDICA V° B° D.L.D.V.A. A.T.T.

JEFE DE OPERACIONES DIRECCIÓN JURÍDICA V° B° R.L.O.G. A.T.T.

ELABORADO POR: R.A.C.L.C. A.T.T.

DIRECCIÓN JURÍDICA V° B° P.L.R.S.A. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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) Valid from/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 (Subject Public 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 (Certificate Policies)	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).

DIRECCIÓN JURÍDICA V°B° D.L.D.V.A. A.T.T.

JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V°B° R.L.C.O. A.T.T.

ELABORADO POR: E.A.M.C. A.T.T.

DIRECCIÓN JURÍDICA V°B° D.R.S.Y. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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

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 (This Update)	Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
Próxima actualización (Next update)	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 (Revoked Certificate)	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

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio s/n esq. O´Connor - Piso 1 Telf.: 4-6644136 - 4-6666484 Fax.: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

- cACompromise (2) – Compromiso de clave de la entidad certificadora, utilizada para indicar que se sabe o sospecha que la clave privada de la entidad certificadora que lo emitió ha sido comprometida
- affiliationChanged (3)– Cambio de afiliación, indica que el nombre del suscriptor u otra información contenida en el certificado ha sufrido modificaciones
- superseded (4) – sustituido, utilizado para indicar que el certificado revocado ha sido sustituido por otro certificado digital
- cessationOfOperation (5) - cesación de la operación, utilizado para indicar que el certificado ya no es necesario para el propósito para el cual fuera emitido
- certificateHold (6) – retención de certificado, utilizado para reflejar el estado de suspensión de un certificado
- privilegeWithdrawn (9) -- retiro de privilegio, indicando que se ha revocado el certificado en razón de que ha cesado la titularidad de un privilegio por parte que su suscriptor
- aACompromise (10) – compromiso de la Autoridad de Atributo, indicando que se sabe o sospecha que uno o varios aspectos de la Autoridad de Atributo han sido comprometidos.

8. ADMINISTRACIÓN DOCUMENTAL

8.1. PROCEDIMIENTO DE CAMBIO DE ESPECIFICACIONES

ATT ha desarrollado procedimientos para la administración de los cambios a la presente Política de Certificación de la ECR.

8.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

ATT 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 procede de igual forma ante cambios sufrido 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, e informados a las ECA dependientes, así como su actualización.

DIRECCIÓN JURÍDICA V°B° L.D.V.A. A.T.T.

JEFE DE OPERACIONES LEGALES DIRECCIÓN JURÍDICA V°B° R.L.O.O. A.T.T.

ELABORADO POR: E.A.M.C. A.T.T.

DIRECCIÓN JURÍDICA V°B° P.D.R.S.Y. A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 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 4° y 5° anillo, calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2 Telf./Fax: 3-3120587 - 3-3120978

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

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