# ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA

# AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES

# Y TRANSPORTES – ATT

---

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

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

**Noviembre 2018**

1-LP-15466

## CONTENIDO



I-LP-15466

I-LP-15466

I-LP-15466

# 1. INTRODUCCIÓN

## 1.1. PRESENTACIÓN

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

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

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

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

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

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

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

## 1.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

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

Versión: 2.0

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

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

I-LP-15466

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

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



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

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

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

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

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

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

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

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

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

Teléfono: (+591)2772266.

Fax: (+591)2772299.

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

## 1.3. PARTICIPANTES DE LA INFRAESTRUCTURA DE CERTIFICACIÓN DIGITAL DE BOLIVIA

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

Los participantes de la Infraestructura antes mencionada son:

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

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

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

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

I-LP-15466

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

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

## 1.4. USO DE LOS CERTIFICADOS

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

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

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

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

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

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

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

I-LP-15466

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

## 1.5. ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

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

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

## 1.6. PROCEDIMIENTO DE APROBACIÓN.

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

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

## 1.7. DEFINICIONES Y ABREVIATURAS

INCD: Infraestructura Nacional de Certificación Digital

EC: Entidad de Certificación o Entidad Certificadora

ECR: Entidad Certificadora Raíz

ECA: Entidad Certificadora Autorizada

ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes

AR: Agencia de Registro

CRL: (*CertificationRevocationList*) Lista de Certificados Revocados

OID: (*ObjectIdentifier*) Identificador de Objeto

PC: Política de Certificación

DPC: Declaración de Prácticas de Certificación.

DN: (*Distinguishedname*) Nombre distintivo

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

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

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

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

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

I-LP-15466

## 2. PUBLICACIÓN DE LA INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.

### 2.1. REPOSITORIO

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

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

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

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

### 2.2. PUBLICACIÓN

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

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

URL: www.ecrb.att.gob.bo

### 2.3. FRECUENCIA DE PUBLICACIÓN

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

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

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

### 2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS

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

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

1-LP-15466

## 2.5. DIVULGACIÓN DE INFORMACIÓN

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

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

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

## 3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

### 3.1. REGISTROS DE NOMBRES

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

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

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

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

### 3.2. VALIDACIÓN DE LA IDENTIDAD INICIAL

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

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

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

I-LP-15466

### 3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN.

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

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

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

## 4. CICLO DE VIDA DE LOS CERTIFICADOS

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

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

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

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

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

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

### 4.2. EMISIÓN DEL CERTIFICADO

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

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

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

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

I-LP-15466

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

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

### 4.3. ACEPTACIÓN DEL CERTIFICADO

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

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

### 4.4. REVOCACIÓN DEL CERTIFICADO DE UNA ECA

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

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

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

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

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

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

I-LP-15466

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

### 4.5. USO DEL CERTIFICADO Y DEL PAR DE CLAVES.

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

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

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

### 4.6. RENOVACIÓN DE UN CERTIFICADO

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

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

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

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

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

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

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

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

I-LP-15466

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

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

### 4.7. CAMBIO DE CLAVES DEL CERTIFICADO

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

### 4.8. MODIFICACIÓN DEL CERTIFICADO

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

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

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

### 4.10. SERVICIO DE ESTADO DE LOS CERTIFICADOS.

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

La CRL contiene la lista de certificados revocados.

### 4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

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

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

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

### 4.12. RECUPERACIÓN DE CLAVES

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

## 5. CONTROLES DE SEGURIDAD FÍSICA GESTIÓN Y DE OPERACIÓN

### 5.1. CONTROLES DE SEGURIDAD FÍSICA

#### 5.1.1. UBICACIÓN Y CONSTRUCCIÓN.

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

I-LP-15466

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

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

### 5.1.2. SEGURIDAD FÍSICA Y AMBIENTAL

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

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

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

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

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

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

Se tiene control en:

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

I-LP-15466

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

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

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

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

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

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

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

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

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

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

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

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

## 5.2. CONTROLES PROCEDIMENTALES

### 5.2.1. ROLES DE CONFIANZA

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

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

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

I-LP-15466

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

### 5.2.2. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

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

## 5.3. CONTROLES DE SEGURIDAD DEL PERSONAL

### 5.3.1. REQUERIMIENTO DE ANTECEDENTES

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

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

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

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

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

### 5.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES.

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

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

### 5.3.3. FORMACIÓN Y FRECUENCIA DE ACTUALIZACIÓN EN LA FORMACIÓN.

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

I-LP-15466

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

### 5.3.4. REQUERIMIENTOS DE CONTRATACIÓN DEL PERSONAL

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

### 5.3.5. CONTROLES PERIÓDICOS DE CUMPLIMIENTO.

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

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

### 5.3.6. FINALIZACIÓN DE LOS CONTRATOS.

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

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

## 5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

### 5.4.1. TIPOS DE EVENTOS REGISTRADOS

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

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

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

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

I-LP-15466

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

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

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

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

### 5.4.2. FRECUENCIA DEL PROCESAMIENTO DE LOG

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

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

### 5.4.3. REQUERIMIENTO DE AUDITORIA

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

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

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

### 5.4.4. ANÁLISIS DE VULNERABILIDADES

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

## 5.5. ARCHIVO DE INFORMACIÓN Y REGISTROS

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

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

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

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

I-LP-15466

## 5.6. CAMBIO DE CLAVES DEL CERTIFICADO

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

## 5.7. PROCEDIMIENTO DE RECUPERACIÓN DE LA CLAVE DE LA EC

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

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

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

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

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

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

I-LP-15466

## 5.8. TRANSFERENCIA DE UNA EC

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

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

## 5.9. CESE DE ACTIVIDADES DE LA EC

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

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

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

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

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

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

# 6. CONTROLES DE SEGURIDAD TÉCNICA

## 6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

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

I-LP-15466

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

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

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

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

## 6.2. PROTECCIÓN CRIPTOGRÁFICA DE LA CLAVE PRIVADA

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

## 6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

No aplicable.

## 6.4. DATOS DE ACTIVACIÓN

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

## 6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

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

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

I-LP-15466

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

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

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

## 6.7. SEGURIDAD DE LA RED

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

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

## 6.8. CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

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

I-LP-15466

## 7. PERFILES DE CERTIFICADOS Y CRL

### 7.1. PERFIL DE CERTIFICADO DE LA ECR

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

| Campos y atributos | Contenido |
|---|---|
| **Versión** | el valor del campo es 2. |
| **Número de Serie (serialNumber)** | Número asignado por la ECR, valor hasta de 20 octetos |
| **Algoritmo de firma (signatureAlgorithm)** | SHA256withRSA<br>1.2.840.113549.1.1.11 |
| **Nombre Distintivo del Emisor (Issuer DN)** | CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO estándar de acuerdo a ISO3166 |
| **Validez (desde, hasta) Validfrom/Valid to** | [20 años]<br>Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time). |
| **Nombre distintivo del suscriptor (Subject DN)** | CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO estándar de acuerdo a ISO3166. |
| **Clave Pública del suscriptor (SubjectPublic Key)** | Algoritmo: RSA, Longitud: 4096 bits. |
| **Extensiones** | |
| **Identificador de la clave del suscriptor (Suject Key Identifier)** | Función Hash (SHA1) del atributo subjectPublicKey |
| **Uso de claves (keyUsage)** | digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0. |
| **Políticas de Certificación (CertificatePolicies)** | URI: http://..... (Archivo en formato de texto). |
| **Restricciones Básicas (basicContraints)** | CA = TRUE, pathLenConstriant = "1". |
| **Punto de distribución de la Lista de certificados Revocados (CRL DistributionPoints)** | URI (1): http://..... (.crl)<br>URI (2): http://.....(.crl) |

### 7.2. PERFIL DE CERTIFICADO DE ECA

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

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

I-LP-15466

| | |
|---|---|
| | acuerdo al estándar ISO 3166 |
| **Clave Pública del suscriptor (SubjectPublic Key)** | Algoritmo: RSA, Longitud:2048 bits |
| **Extensiones** | |
| **Identificador de la clave del suscriptor (Suject Key Identifier)** | Función Hash (SHA1) del atributo subjectPublicKey |
| **Uso de claves (keyUsage)** | digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0. |
| **Políticas de Certificación (CertificatePolicies)** | URI: http://..... (Archivo en formato de texto). |
| **Restricciones Básicas (basicContraints)** | CA = TRUE, pathLenConstriant = "1". |
| **Punto de distribución de la Lista de certificados Revocados (CRL DistributionPoints)** | URI (1): http://..... (.crl)<br>URI (2): http://.....(.crl) |

## 7.3. PERFIL DE LA CRL DE LA ECR

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

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

I-LP-15466

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

Para los formatos y contenidos de todos los campos y extensiones no indicados expresamente en la presente sección, deberá seguirse los lineamientos del RFC 5280.

En la extensión conocida como código de razón (o reasonCode) que identifica el motivo de la pérdida de vigencia del certificado, se habilitan como opciones las siguientes:

- Unspecified (0) - No especificada, utilizada para revocaciones por motivos no contemplados en los otros códigos.
- keyCompromise (1) – Compromiso de clave, utilizada para la revocación de un certificado de usuario final, indicando que se sabe o sospecha que la clave privada del suscriptor ha sido comprometida
- cACompromise (2) – Compromiso de clave de la entidad certificadora, utilizada para indicar que se sabe o sospecha que la clave privada de la entidad certificadora que lo emitió ha sido comprometida
- affiliationChanged (3)– Cambio de afiliación, indica que el nombre del suscriptor u otra información contenida en el certificado ha sufrido modificaciones
- superseded (4) – sustituido, utilizado para indicar que el certificado revocado ha sido sustituido por otro certificado digital
- cessationOfOperation (5) - cesación de la operación, utilizado para indicar que el certificado ya no es necesario para el propósito para el cual fuera emitido
- certificateHold (6) – retención de certificado, utilizado para reflejar el estado de suspensión de un certificado
- removeFromCRL (8), retirado de la CRL, utilizado cuando por algún motivo un certificado digital es retirado de la CRL.
- privilegeWithdrawn (9) – retiro de privilegio, indicando que se ha revocado el certificado en razón de que ha cesado la titularidad de un privilegio por parte que su suscriptor
- aACompromise (10) – compromiso de la Autoridad de Atributo, indicando que se sabe o sospecha que uno o varios aspectos de la Autoridad de Atributo han sido comprometidos.

## 8. AUDITORÍA DE CONFORMIDAD

### 8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD

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

I-LP-15466

## 8.2. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

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

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

## 8.3. COMUNICACIÓN DE LOS RESULTADOS.

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

## 9. REQUISITOS COMERCIALES Y LEGALES.

## 9.1. TARIFAS

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

## 9.2. POLÍTICAS DE CONFIDENCIALIDAD

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

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

## 9.3. PROTECCIÓN DE LOS DATOS PERSONALES

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

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

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

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

I-LP-15466

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

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

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

### 9.4. OBLIGACIONES DE LOS PARTICIPANTES DE LA PKI

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

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

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

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

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

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

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

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

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

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

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

I-LP-15466

## 9.5. MODIFICACIONES AL PRESENTE DOCUMENTO

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

## 9.6. RESOLUCIÓN DE CONFLICTOS

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

## 9.7. LEGISLACIÓN APLICABLE

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

## 9.8. CONFORMIDAD CON LA LEY APLICABLE

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

I-LP-15466