adsib agencia para el desarrollo de la sociedad de la información en Bolivia

POLÍTICA DE CERTIFICACIÓN DE LA ENTIDAD CERTIFICADORA PÚBLICA ADSIB

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

ADSIB

La Paz - Bolivia

Índice de contenido

Apéndice 1. Plan de Cese de Actividades
Apéndice 2. Política de Protección de Datos

1. Introducción

1.1. Descripción general.

Este documento presenta la Política de Certificación de la Entidad Certificadora Pública – ADSIB, que define los términos que rigen para la implementación del servicio de Certificación Digital, en el marco de La Ley N°164 General de Telecomunicaciones, Tecnologías de Información y Comunicación y el Decreto Supremo 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

La Política de Certificación es un instrumento que establece las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados. La misma ha sido desarrollada por ADSIB y aprobada por la ATT.

La ADSIB presenta este documento en cumplimiento a las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015, ATT-DJ-RA TL LP 32/2015** y **ATT-DJ-RA TL LP 1538/2015** emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la Ley N° 164 General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

- **Descripción del servicio**

Un certificado digital, emitido por la ADSIB en tanto Entidad Certificadora Pública, es un archivo digital firmado digitalmente por una entidad certificadora autorizada, que vincula una clave pública a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.

A nivel conceptual, la Firma Digital es un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un documento digital, o un correo electrónico, que certifica la identidad del signatario y la integridad del documento digital firmado. La firma digital esta compuesta por el hash del documento digital cifrado por la clave privada del signatario, y por el certificado digital del signatario.

La certificación que emite ADSIB contempla tres destinatarios:

a) Cargo público.- certificado expedido únicamente a servidores públicos, según lo establecido en la Ley 2027 Estatuto del funcionario público, a solicitud expresa de la Máxima Autoridad Ejecutiva de su

entidad.

b) Persona jurídica.- certificado expedido únicamente a personas bajo relación jurídica con una persona jurídica, a solicitud expresa del representante legal de dicha persona.

c) Persona natural.- certificado expedido a cualquier ciudadana o ciudadano mayor de edad y hábil por derecho para realizar actos jurídicamente válidos.

- **Descripción**

Los certificados digitales deben ser emitidos por una entidad certificadora autorizada, responder a formatos y estándares reconocidos internacionalmente y fijados por la ATT, contener como mínimo los datos que permitan identificar a su titular, a la entidad certificadora que lo emitió, su período de vigencia y contemplar la información necesaria para la verificación de la firma digital.

- **Propósito**

El certificado digital cumple las siguientes funciones:

a) Acredita la identidad del titular de la firma digital
b) Legítima la autoría de la firma digital que certifica
c) Vincula un documento digital o mensaje electrónico de datos, con la firma digital y la persona
d) Garantiza la integridad del documento digital o mensaje electrónico con firma digital.

Descripción de la Entidad Certificadora.

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) es una entidad pública, domiciliada en nuestra señora de La Paz, creada el 19 de marzo de 2002, mediante el Decreto Supremo 26553.

Se constituye como una entidad descentralizada bajo tuición de la Vicepresidencia del Estado Plurinacional de Bolivia. La ADSIB es la encargada de proponer políticas, implementar estrategias y coordinar acciones orientadas a reducir la brecha digital en el país, a través del impulso de las Tecnologías de la Información y Comunicación en todos sus ámbitos, teniendo como principal misión favorecer relaciones del Gobierno con la Sociedad, mediante el uso de tecnologías adecuadas.

La ADSIB cuenta con sus oficinas ubicas en la calle Ayacucho y Mercado No 308 - Edificio de la Vicepresidencia del Estado Piso 3, así mismo, las dependencias de su Data Center se encuentran en las

mismas instalaciones en la parte del subsuelo.

En tanto la ADSIB se constituya en Entidad Certificadora Pública, sus funciones serán:

- Emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales.
- Facilitar servicios de generación de firmas digitales
- Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario.
- Validar y comprobar cuando corresponda, la identidad y existencia real de la personal natural o jurídica.
- Reconocer y validar los certificado digitales emitidos en el exterior.
- Otras funciones relacionadas con la prestación de servicios de certificación digital.

En ese marco, la ADSIB desempeña coadyuva en el proceso de modernización del Estado Plurinacional de Bolivia al constituirse como la Entidad Certificadora Pública, gira su trabajo en la consolidación de la Firma Digital, además emite certificados digitales manteniendo planes y procedimientos de calidad para efectuar su trabajo.

Derechos y Obligaciones de la Entidad Certificadora Publica.

Derechos de la Entidad Certificadora Publica

De conformidad a lo establecido en el Art.58 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, **la Entidad Certificadora Pública tiene los siguientes derechos**:

a) Recibir oportunamente el pago por los servicios provistos, de conformidad con los precios o tarifas establecidas.
b) Cortar el servicio provisto por falta de pago por parte de las usuarias o usuarios, previa comunicación, conforme a lo establecido por reglamento.
c) Recibir protección frente a interferencias perjudiciales a operaciones debidamente autorizadas.
d) Otros que se deriven de la aplicación de la Constitución Política del Estado, la Ley N° 164 y demás normas aplicables.

Obligaciones de la Entidad Certificadora Publica

De conformidad a lo establecido en el Art.59 de la Ley N° 164 Ley General de Telecomunicaciones,

Tecnologías de Información y Comunicación, l**a Entidad Certificadora Pública tiene las siguientes obligaciones**:

a) Someterse a la jurisdicción y competencia de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
b) Proveer en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida, los servicios de telecomunicaciones y tecnologías de información y comunicación.
c) Proporcionar información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a las usuarias o los usuarios.
d) Proporcionar información clara, precisa, cierta, completa y oportuna a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
e) Proveer gratuitamente los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, que determine la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
f) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
g) Efectuar el reintegro o devolución de montos que resulten a favor de las usuarias o los usuarios por errores de facturación, deficiencias o corte del servicio, con los respectivos intereses legales.
h) Atender las solicitudes y las reclamaciones realizadas por las usuarias o los usuarios.
i) Informar oportunamente la desconexión o cortes programados de los servicios.
j) Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley.
k) Facilitar a las usuarias o usuarios en situación de discapacidad y personas de la tercera edad, el acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en reglamento.
l) Proveer servicios que no causen daños a la salud y al medio ambiente.
m) Cumplir las instrucciones y planes que se emitan en casos de emergencia y seguridad del Estado.
n) Actualizar periódicamente su plataforma tecnológica y los procesos de atención a las usuarias y los usuarios.
o) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables .

Para garantizar la publicidad, seguridad, integridad y eficacia de la firma y certificado digital, la Entidad Certificadora Pública tiene las siguientes **obligaciones** de acuerdo a lo establecido en el Art. 43 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;
b) Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT;
c) Informar a los usuarios de las condiciones de emisión, validación, renovación, baja, suspensión, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web entre otros medios;
d) Mantener el control, reserva y cuidado de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Cualquier anomalía que pueda comprometer su confidencialidad deberá ser comunicada inmediatamente a la ATT;
e) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
f) Mantener un sistema de información de acceso libre, permanente y actualizado donde se publiquen los procedimientos de certificación digital, así como los certificados digitales emitidos consignando, su número único de serie, su fecha de emisión, vigencia y restricciones aplicables, así como el detalle de los certificados digitales suspendidos y revocados;
g) Las entidades certificadoras que derivan de la certificadora raíz (ATT) deberán mantener un sistema de información con las mismas características mencionadas en el punto anterior, ubicado en territorio y bajo legislación del Estado Plurinacional de Bolivia;
h) Revocar el certificado digital al producirse alguna de las causales señaladas en los puntos anteriores;
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.

Derechos y Obligaciones de la Entidad Certificadora Publica y ante Terceros que confían:

De conformidad a lo establecido en el Art. 44 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación y la Resolución Administrativa **RAR -DJ-RA TL LP 31/2015** emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, la **Responsablidad de la Entidad Certificadora Pública ante terceros**, se da en los siguientes casos:

a) Será responsable por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios o usuarios.
b) La entidad certificadora se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.
c) La entidad certificadora responderá 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.

Derechos y Obligaciones de las Usuarias y Usuarios en relacion al Servicio

Titulares del Certificado Digital

De acuerdo a lo establecido en el Art. 52 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, son titulares de la firma digital y del certificado digital las personas naturales y las personas jurídicas que a través de sus representantes legales hayan solicitado por sí y para sí una certificación que acredite su firma digital. En este sentido, se establece que la persona autorizada por el Representante Legal será el responsable para todos los efectos de la firma y certificado digital.

Responsabilidad del titular

De acuerdo a lo establecido en el Art. 53 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, **el titular será responsable en los siguientes casos**:
a) Por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como titular.
b) Los datos de creación de la firma digital vinculado a cada certificado digital de una persona jurídica, será responsabilidad del representante legal, cuya identificación se incluirá en el certificado digital.
c) El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
d) Asimismo, acorde a los procedimientos de la ADSIB, la entidad no podrá acceder en ningún

momento a la clave privada del usuario, por lo que éste es el único responsable de su generación, administración, uso y custodia. En caso de verse comprometida por cualquier razón dicha clave, el usuario deberá informar a la ADSIB a la brevedad posible y solicitar su revocatoria. Todos los efectos o daños que pudieran ocasionarse al usuario o a terceros, en el transcurso comprendido entre la generación de la firma y su revocatoria, son de exclusiva responsabilidad del usuario.

Derechos del Titular del Certificado

De conformidad a lo señalado en el Art. 54 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, e**l titular del certificado digital tiene los siguientes derechos**:

a) A ser informado por la entidad certificadora de las características generales, de los procedimientos de creación y verificación de firma digital, así como de las reglas sobre prácticas de certificación y toda información generada que guarde relación con la prestación del servicio con carácter previo al inicio del mismo, así como de toda modificación posterior;
b) A la confidencialidad de la información proporcionada a la entidad certificadora;
c) A recibir información de las características generales del servicio, con carácter previo al inicio de la prestación del mismo;
d) A ser informado, antes de la suscripción del contrato para la emisión de certificados digitales, acerca del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, de las condiciones precisas para la utilización del certificado, de las limitaciones de uso, de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o los que se acordaren;
e) A que la entidad certificadora le proporcione la información sobre su domicilio legal en el país y sobre todos los medios a los que el titular pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del servicio contratado, o la forma en que presentará sus reclamos;
f) A ser informado, al menos con dos (2) meses de anticipación, por la entidad certificadora del cese de sus actividades, con el fin de hacer valer su aceptación u oposición al traspaso de los datos de sus certificados a otra entidad certificadora.

Obligaciones del Titular del certificado

De conformidad a lo señalado en el Art. 55 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, **el titular del certificado digital tiene las siguientes obligaciones:**

I.El titular de la firma digital mediante el certificado digital correspondiente 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.

II. 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.

Derechos y Obligaciones de los Signatarios

Derechos de los Signatarios

De conformidad a lo señalado en el Art. 54 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, **las usuarias y usuarios tienen los siguientes derechos**:
a) Acceder en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida a los servicios de telecomunicaciones y tecnologías de información y comunicación.
b) Acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a ser proporcionada por la Entidad Certificadora Pública.
c) Acceder gratuitamente a los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, de acuerdo a determinación de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
d) Recibir de forma oportuna, comprensible y veraz la factura mensual desglosada de todos los cargos y servicios del cual es usuario, en la forma y por el medio en que se garantice su privacidad.

e) Exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.
f) Conocer los indicadores de calidad de prestación de los servicios al público de los proveedores de telecomunicaciones y tecnologías de información y comunicación.
g) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
h) Ser informado por la Entidad Certificadora Pública oportunamente, cuando se produzca un cambio de los precios, las tarifas o los planes contratados previamente.
i) Recibir el reintegro o devolución de montos que resulten a su favor por errores de facturación, deficiencias o corte del servicio.
j) Obtener respuesta efectiva a las solicitudes realizadas a la Entidad Certificadora Pública.
k) Reclamar ante la Entidad Certificadora Pública y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna.
l) Disponer, como usuaria o usuario en situación de discapacidad y persona de la tercera edad facilidades de acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en un reglamento especial.
m) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

Obligaciones de las usuarias y usuarios.-

De conformidad a lo establecido en el Art.55 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, **las usuarias y usuarios tienen las siguientes obligaciones:**
a) Pagar sus facturas por los servicios recibidos, de conformidad con los precios o tarifas establecidas.
b) Responder por la utilización de los servicios por parte de todas las personas que tienen acceso al mismo, en sus instalaciones o que hacen uso del servicio bajo su supervisión o control.
c) No causar daño a las instalaciones, redes y equipos de la Entidad Certificadora Pública.
d) Cumplir con las instrucciones y planes que emita la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes en casos de emergencia y seguridad del Estado.
e) No causar interferencias perjudiciales a operaciones debidamente autorizadas.
f) Otros que se deriven de la aplicación de la Constitución Política del Estado, las leyes y demás normas aplicables.
Asimismo, en lo que corresponda, se aplicará lo establecido en los Arts. 52 al 55 del Decreto Supremo N° 1793, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

1.2. Identificación y nombre del documento.

- **Identificación de la Política de Certificación**

La Política de Certificación de la ADSIB contempla a partir de un conjunto de principios y normas que describen el perfil de un certificado, sus usos permitidos, los derechos y obligaciones de todos los actores involucrados en su utilización, los procesos mediante los cuales se verifica la identidad del titular del certificado, se generan las claves, se emite y se revoca el certificado y las garantías tecnológicas de seguridad que la ADSIB aplica en cada caso. Este documento ha sido elaborado por ADSIB y aprobado por la ATT.

Este documento se concentra en el Anexo 4: contenido mínimo de las políticas de certificación para una ECA. Políticas de certificación, en conformidad con lo establecido en las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015**, **ATT-DJ-RA TL LP 32/2015**, y **ATT-DJ-RA TL 1538/2015** emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), en cumplimiento a la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

- **Nombre**

El presente documento lleva como titulo "Política de Certificación de la Entidad Certificadora Pública ADSIB"**.** Se constituye en su versión final.

- **Versión fecha de elaboración**

El documento fue elaborado desde el 21 de noviembre hasta el 21 de diciembre del año 2014.

- **Fecha de actualización**

Última actualización el 2 de febrero de 2016.

- **Sitio web de consulta.**

El sitio web de consulta es: www.firmadigital.bo.

1.3. Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia

La Jerarquía Nacional de Certificación Digital, según el artículo 36 del Decreto Supremo Reglamentario 1793, establece los niveles de Infraestructura Nacional de Certificación Digital (INCD).

Descripción breve de la jerarquía nacional de Certificación Digital del Estado Plurinacional de Bolivia y de cada uno de sus componentes.

Se describe a continuación la jerarquía nacional de certificación digital y cada uno de sus componentes:

- **Primer nivel: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes: Entidad Certificadora Raíz.**

De acuerdo a la Ley N° 164 y el Decreto Supremo N° 1793 la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), es la Entidad Certificadora de Raíz.

La ATT es la entidad de certificación de nivel superior dentro de la Jerarquía Nacional de Certificación Digital que auto firmará su certificado y emitirá certificados digitales a las entidades certificadoras pública y privadas subordinadas.

- **Segundo Nivel: Entidad de Certificación**

Son las entidades certificadoras públicas o privadas subordinadas de la Entidad Certificadora Raíz. La entidad certificadora pública es la ADSIB y las entidades certificadoras privadas, son todas aquellas autorizadas por ATT a prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

- **Tercer nivel: Agencia de Registro**

Es la agencia dependiente de una entidad certificadora, 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

La agencia de registro es la ADSIB, tiene como objetivo asegurarse de la veracidad de los datos que

fueron utilizados para solicitar el certificado digital.

- **Cuarto nivel: Signatarios**

Son todos los usuarios y usuarias finales a quienes se les ha emitido un certificado por una entidad certificadora, dentro de la Jerarquía Nacional de Certificación Digital.

- **Otros: Terceros aceptantes.**

Son cualquier persona física u organización que confía en los certificados de la ADSIB, al autenticar a una persona física o al aceptar una Firma Digital, están obligados a comprobar la validez del certificado.

1.4. Uso de los certificados.

Descripción de los siguientes usos de acuerdo al D.S. 1793 Reglamento para el Desarrollo de las TIC:

- **Características del certificado digital**

Según el artículo 27 del D.S 1793, los certificados digitales, deben contener mínimamente las siguientes características:

a) La emisión debe ser realizada por una entidad de certificación autorizada:
b) Contener el número único de serie que identifica el certificado
c) Responder a formatos estándares reconocidos internacionalmente
d) Periodo de validez
e) Ser susceptibles de verificación respecto de su estado de revocación
f) Acreditar en los supuestos de representación. Las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente
g) Contemplar la información necesaria para la verificación de la firma
h) Identificar la política de certificación bajo la cual fue emitido
i) Contemplar los límites de uso del certificado, si se prevén
j) Validar la correspondencia jurídica entre el certificado digital, la firma digital y la persona
k) Identificar inequívocamente a su titular y al certificador autorizado que lo emitió.

- **Usos Permitidos de los Certificados**

La ADSIB estará limitado a la firma de certificados digitales para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en el presente documento.

El uso de los certificados emitidos por la ADSIB estará limitado según el tipo de certificado, y a continuación se menciona los usos de cada uno de ellos:

TIPOS DE CERTIFICADO	USO
Persona natural	Firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático
Persona jurídica	En representación de una persona jurídica: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático
Cargo público	Como servidor público: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático.
Lista de Revocación de Certificado	Firma de Lista de Revocación de Certificado
OCSP	Firma de OCSP

- **Restricciones en el Uso de los Certificados.**

El usuario contratante de certificados digitales generados por la ADSIB esta obligado a utilizarlos conforme a los usos permitidos y señalados en la sección anterior o cualquier texto normativo que los sustituya y regule la actividad de certificación digital dentro del Estado Plurinacional de Bolivia y para el uso para el cual fue adquirido, quedando expresamente indicado que cualquier violación a las normas, usos y/o leyes del Estado Plurinacional de Bolivia queda bajo la responsabilidad del usuario contratante, así como los daños y perjuicios que ocasionare le será aplicable un proceso penal establecido en el Código Penal, artículo 363 (alteración, acceso y uso indebido de datos informáticos).

Adicionalmente le será revocado el certificado digital y el usuario contratante asume la responsabilidad de indemnizar a ADSIB por daños y perjuicios ocasionados a terceros derivados de

reclamos, acciones, efectos de acción, pérdidas o daños (incluyendo multas legales) que se generaren por el uso indebido, por parte del usuario contratante del servicio contratado con ADSIB.

1.5. Administración de la Política de Certificación.
Responsabilidad de la administración de la Política de Certificación.

La responsabilidad de la administración de la Política de Certificación depende de la ADSIB en tanto Entidad Certificadora Pública, quien presentara el documento final para su revisión a la ATT.

A su vez, la ADSIB presentara a la ATT un documento denominado Declaración de Prácticas de Certificación en el cual declara los procedimientos administrativos y técnicos mediante los cuales se satisface lo exigido por la Política de Certificación.

1.6. Definiciones y abreviaturas.

- **Abreviaturas**

- **EC:** Entidad Certificadora.
- **ECR:** Entidad Certificadora Raíz.
- **AR:** Agencia de Registro.
- **URI:** Identificador Uniforme de Recursos
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **SHA**: (Secure Hash Algorithm) Algoritmo de Hash Seguro.
- **RFC:** ([1]Request For Comments) Requerimiento de Comentarios.
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **HSM:** (Hardware Security Module) Modulo de Hardware de Seguridad[2].
- **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
- **ADSIB:** Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- **ATT:** Autoridad de Regulación y Fiscalización de Transportes y Telecomunicaciones.
- **CP:** (Certificate Policy) Política de Certificación.

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

2 Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptograicas y suele aportar aceleración hardware para operaciones criptográficas

- **CPS:** (Certification Practice Statement) Declaración de Prácticas de Certificación.
- **TIC:** Tecnologías de Información y Comunicación.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.

- **Definiciones**

1. **Certificado digital:** Es un archivo digital firmado digitalmente por una entidad certificadora autorizada que vincula una clave pública a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.
2. **Clave privada:** Archivo digital que contiene un conjunto de caracteres alfanuméricos únicos generados mediante un sistema criptográfico, que el signatario emplea en la firma digital de un documento. La clave privada es estrictamente confidencial e individual, y su perdida posibilita la usurpación de identidad del signatario.
3. **Clave pública:** Archivo digital que contiene un conjunto de caracteres alfanuméricos únicos, generados al mismo momento que la clave privada por el mismo sistema criptográfico. La clave pública esta contenida en el certificado digital, junto a los datos de identidad del signatario. Tiene vocación a ser de conocimiento público, y permite verificar la firma digital de un documento.
4. **Firma digital:** Es un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un documento digital, o un correo electrónico, que certifica la identidad del signatario y la integridad del documento digital firmado. La firma digital esta compuesta por el hash del documento digital cifrado por la clave privada del signatario, y por el certificado digital del signatario.

2. Responsabilidad del repositorio y su publicación.

- **2.1 Repositorios.**

Los repositorios públicos de información de la ADSIB están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la ADSIB, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

A fin de garantizar la completa disponibilidad de este documento y demás documentos esenciales, la ADSIB mantiene un repositorio dentro de su página web. El repositorio público de la ADSIB, no contiene ninguna información confidencial o privada.

- **2.2 Publicación.**

Es obligación de la ADSIB publicar la información relativa a sus prácticas y sus certificados revocados. Las publicaciones que realice la ADSIB, de toda la información clasificada como pública, se anunciara en su respectiva página web.

Este servicio de publicación de información del certificador está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la ADSIB, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

3. Identificación y Autenticación.

Formato del Nombre Distinguido

- **Tipos de nombres**

La norma vigente define los tipos de nombres para cada uno de los tres tipos de certificado. Para las personas naturales, el nombre se compone de: CN = Nombres y Apellidos de la persona natural; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

Para las personas jurídicas, el nombre se compone de: CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón social de la empresa o institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

Para las cargos públicos, el nombre se compone de: CN = Nombres y Apellidos del servidor público; O = Nombre de la institución pública a la que pertenece; OU = Unidad Organizacional de la que depende el funcionario público (opcional); T = Cargo del servidor público; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

- **Significado de los nombres**

La ADSIB requerirá de los clientes contratantes de certificados digitales sus nombres y apellidos completos conforme figuran en la cédula de identidad que presente el solicitante de la firma digital.

No serán admitidos o procesados por la ADSIB los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el usuario. En el caso de las poblaciones indígenas serán considerados los nombres que figuran en su cédula de identidad o pasaporte.

En todo caso la ADSIB garantiza que los nombres distintivos contenidos en los campos de los certificados son lo suficientemente distintivos y significativos para poder vincular la identidad de un usuario a su firma digital.

- **Interpretación de formatos de nombres**

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritos en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos por la ADSIB utilizan codificación UTF-8 para todos los atributos, según la RFC 3280 ("Internet X.509 Public Key Infraestructure and Certificate Revocation List (CRL) Profile").

- **Unicidad de nombres**

La ADSIB define como campo del nombre distintivo del certificado de autoridad como único y sin ambigüedad. Para ello se incluirá como parte del nombre distintivo, específicamente en el campo correspondiente, el nombre o razón social de la ADSIB, por lo tanto la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro nacional.

Adicionalmente y respecto a los clientes; si existe un usuario que mantenga contrato y haya adquirido más de un tipo de certificado digital, la base de datos de la ADSIB mantendrá un esquema uniforme e igualitario de datos del usuario contratante y no será permitido o procesado en cuanto a datos personales disimiles y que correspondan a un mismo usuario.

- **Resolución de conflictos relativos a nombres**

En el caso de una ocurrencia de conflicto de nombre entre clientes y que corresponda a nombre y apellidos iguales, la ADSIB procederá a realizar las distinción de identidad y autenticación de la misma a través del uso del número de cédula de identidad y NIT personal de cada usuario de la ADSIB con las cuales se haya generado el conflicto de nombre.

Validación de la identidad inicial

- **Métodos de prueba de posesión de la clave privada**

El esquema de operación de la ADSIB y su sistema de certificación, se encuentran configurados para generar las claves pública y privada.

En virtud de lo anterior, una vez emitido cada certificado, es el usuario quien tiene la custodia y resguardo de su clave privada, presumiendo que el mismo la posee y resguarda, salvo denuncia de él mismo usuario de la perdida de su clave privada, caso en el cual se procederá a la suspensión y/o revocación de la firma digital que corresponda.

- **Autenticación de la identidad de una persona natural, jurídica o cargo público**

La ADSIB procederá a autenticar y validar la identidad de los usuarios dependiendo del tipo de certificado que soliciten.

Personal Natural

La ADSIB verificará los requisitos del solicitante con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

Persona Jurídica

La ADSIB procederá a comprobar la validez de la información del usuario con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

Cargo Público

La ADSIB procederá a comprobar la documentación requerida, a través de llamadas telefónicas y con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

- **Autenticación de la identidad de un individuo**

La persona física designada para tramitar la emisión de un certificado, además de presentar la resolución de acreditación vigente ante la ADSIB, deberá demostrar su identidad de la siguiente forma:

a) cédula de identidad.
b) fotografía.

Se verifica que dichos datos además coincidan con los establecidos en la resolución de acreditación y con el sistema del SEGIP.

Identificación y autenticación para solicitudes de revocación.

- **Identificación y autenticación de las solicitudes de renovación rutinarias**

La identificación y autenticación para la renovación del certificado se realizará de la siguiente manera:

a) El usuario solicitará la renovación a través de su cuenta de usuario.
b) La ADSIB realizará la verificación de la solicitud y pago en un plazo no mayor a 72 horas mediante los procedimientos establecidos.
c) De no ser posible la verificación se emitirá un informe que detallen los esfuerzos realizados y se esperará que el usuario se ponga nuevamente en contacto a través de los teléfonos, correo electrónico, fax, etc. de la ADSIB.
d) La ADSIB podrá o no requerir al usuario presentarse personalmente en oficinas de la entidad, dependiendo del proceso de verificación.
e) En un plazo no mayor a 72 horas desde concluida la verificación, la ADSIB pondrá a disposición del usuario su nuevo certificado a través de su cuenta de usuario.

El proceso de renovación rutinario podrá realizarse únicamente por tres veces consecutivas, Al cabo de la misma el usuario deberá generar un nuevo par de claves e iniciar el proceso como la solicitud de un nuevo certificado.

- **Solicitudes de renovación clave.**

El procedimiento es el mismo al de la solicitud de un nuevo certificado y el usuario deberá completar todos los pasos necesarios.

4. Requerimientos Operativos del Ciclo de Vida de los Certificados.

Requisitos mínimos para la obtención de Certificados Digitales

Se detallan los requisitos mínimos para la obtención de un Certificado digital:

Para personas naturales:

a) Fotocopia simple de carnet de identidad o carnet de extranjero.

b) Fotocopia de la última factura de pago de luz, agua o teléfono que permita verificar su dirección actual.

c) Dispositivo que permita firmar un documento, donde sea almacenado el certificado digital y custodiado (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2.

Para personas jurídicas:

a) Fotocopia simple de carnet de identidad o carnet de extranjero.

b) Autorización original de la persona jurídica firmada por el Representante Legal.

c) En función al tipo de información que utiliza una organización las claves pública y privada podrán ser emitidas a:

d) Dispositivo que permita firmar un documento, donde sea almacenado el certificado digital y custodiado (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2.

Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 31/2015, donde sea almacenado el certificado digital que permita firmar uno o varios documentos y que cumpla con sistemas de seguridad reconocidos internacionalmente, garantizando la confiabilidad del mismo a sus usuarios o signatarios.

Fotocopia simple del certificado de inscripción al padrón nacional de contribuyentes biométrico digital (PBD-11) y/o documento de Exhibición del NIT (Número de identificación tributaria).

Para cargos públicos:

a) Fotocopia simple de carnet de identidad o carnet de extranjero.

b) Fotocopia del memorándum de designación firmado por el Representante de la Entidad.

c) Autorización del servidor público firmada por el Representante de la Entidad.

d) La documentación debe ser validada por la Entidad de Certificación / Agencia de Registro con la presentación de la documentación original por parte del solicitante.

e) Dispositivo que permita firmar un documento, donde sea almacenado y custodiado (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140-2

La información que sea otorgada por el usuario a la ADSIB sera cerciorada con datos del Servicio General de Identificación Personal (SEGIP).

Requisitos Técnicos para Acceder al Servicio

Para que un usuario pueda acceder al servicio de certificación digital deberá contar con las especificaciones técnicas detalladas a continuación:

- Dispositivo que permita firmar una documento al signatario, donde sean almacenados y custodiados el certificado digital y su clave privada (Token o tarjetas inteligentes – smart cards) que cumpla con el estándar FIPS 140-2 – Personas Naturales, Personas Jurídicas y Cargos públicos. El mismo podrá ser adquirido por el usuario en empresas que serán publicadas en la página web: www.firmadigital.bo; y/o

Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 32/2015, donde sea almacenado el certificado digital que permita firmar uno o varios documentos y que cumpla con sistemas de seguridad reconocidos internacionalmente, garantizando la confiabilidad del mismo. - Personas Jurídicas.

- El usuario deberá generar una cuenta de usuario y una contraseña para acceder y llenar el

formulario de solicitud.

- El usuario deberá crear su par de claves y enviar su clave pública a través de su cuenta de usuario en el sistema. Si el usuario no supiera como realizar la operación, la ECP le proporcionará soporte técnico. La ECP no podrá intervenir de ninguna manera en la generación del par de claves del usuario, lo que constituye una acción privada.

Procesamiento de solicitud del certificado

Las personas que deseen obtener un certificado digital deberán:

a) Crear una cuenta de usuario en el sistema de la página web: www.firmadigital.bo
b) Solicitar mediante su cuenta de usuario el tipo de certificado digital y completar el formulario de solicitud.
c) Aproximarse a las oficinas de la ADSIB, junto con los requisitos que se le especificarán una vez realizada su solicitud.
d) Realizar el pago correspondiente.
e) Ingresar el número de depósito o subir una imagen del comprobante bancario en su cuenta de usuario.
f) Es responsabilidad del usuario proteger la contraseña de su cuenta de usuario.
g) Entregar al momento de presentar la solicitud el token según los estándares técnicos requeridos. En la página www.firmadigital.bo se publicará una lista de proveedores de token que cumplan con los estándares solicitados.
h) Aceptar la políticas y contrato correspondiente a la prestación del servicio.

*La apertura de la cuenta es gratuita y está disponible en línea.

Emisión del certificado

La ADSIB, una vez validada la identidad del signatario y verificado el pago correspondiente, aprobará la firma del certificado correspondiente.

La ADSIB cuenta con procedimientos internos para la ceremonia de la Firma Digital.

Una vez verificados la identidad y el pago correspondiente la ADSIB tendrá un plazo máximo de 72 horas para poner a disposición del usuario su certificado firmado en su cuenta de usuario, salvo caso

fortuito, fuerza mayor o decisión técnicamente justificada, casos en que la entidad deberá informar las razones del retraso al usuario.

Aceptación del certificado

La ADSIB, una vez comprobado y validado la información y los requisitos presentados por el usuario, dispondrá el certificado y firma digital en la cuenta del usuario disponible a través del sistema.

La firma del contrato entre el usuario y la ADSIB implica que el usuario acepta los términos y condiciones del uso del certificado y firma digital.

Generación del par de claves y uso del certificado

La generación de las claves para la firma

El usuario deberá generar el par de claves pública y privada en su dispositivo de firma digital. Al contar el usuario con su clave pública y privada, el usuario pondrá su clave pública a disposición de la ADSIB a través de su cuenta de usuario. El proceso de la generación de claves es privado, la ADSIB no intervendrá en ningún momento del mismo, así el usuario garantizará que un tercer no ha tenido conocimiento de su clave privada.

El titular sólo puede utilizar la clave privada y el certificado para usos autorizados en este documento.

El usuario es el único responsable de la custodia y cuidado de su clave privada.

En caso de verse comprometida su clave privada, el usuario deberá suspender o revocar su firma a través de su cuenta de usuario o contactarse con la ADSIB, sin menoscabo de responder personalmente por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados por parte de terceras personas.

Renovación del certificado

Se realizará la renovación del certificado cuando se haya cumplido la validez del certificado, de 365 días calendario. Todo certificado generado por la ADSIB podrá ser renovado, siempre y cuando sean cumplidas las siguientes condiciones:

1. Que la firma o certificado digital no haya sido revocado por la ADSIB por razones de uso

ilícito de la firma o certificado electrónico, según corresponda.

2. Que el solicitante cumpla con el proceso de solicitud y validación.

Suspensión y reactivación del certificado

No se realizan cambios de clave de certificados. En caso de ser necesario, el usuario podrá optar por la suspensión del certificado y su posterior reactivación.
La suspensión del certificado generado por ADSIB, precede a la reactivación o revocación, y se realiza a solicitud del titular del certificado.

Todo certificado generado por ADSIB podrá ser reactivado, siempre y cuando el usuario haya solicitado la misma. En caso de lo contrario, se procede a la revocación de la certificación.

Se procederá a la suspensión del certificado, siempre y cuando se cumplan las siguientes condiciones:

1. Que el usuario haya notificado la posibilidad de perdida del token que contiene el certificado digital.
2. Que el usuario haya notificado la posibilidad de que su clave privada ha sido comprometida por algún motivo.

Procedimiento de reactivación de claves del certificado

Las personas que deseen reactivar su par de claves deberán seguir el siguiente procedimiento.

a) Ingresar a su cuenta de usuario en el sistema de la página web: www.firmadigital.bo.
b) Solicitar mediante su cuenta de usuario la reactivación.
c) Si el usuario evidencia que su clave ha sido comprometida o notifica la perdida podrá solicitar la revocación de su certificado mediante su cuenta de usuario.

Reemisión de claves del certificado

Se procederá a la reemisión de un nuevo certificado, siempre y cuando se cumplan las siguientes condiciones:

1. Que el usuario haya notificado la perdida del token (hsm) que contiene el certificado digital.
2. Que el usuario haya notificado que su clave privada ha sido comprometida por algún motivo

En estos casos, el usuario deberá seguir los siguientes pasos:

a) Ingresar a su cuenta de usuario en el sistema de solicitud de certificados disponible en la página web www.firmadigital.bo.
b) Solicitar mediante su cuenta de usuario la revocación del certificado comprometido.
c) Solicitar mediante su cuenta de usuario la remisión del certificado; de esta manera no realizará el pago por la emisión del nuevo certificado.
d) Realizar el procedimiento inicial de registro y proceder con la generación de su nuevo par de claves como se indica anteriormente.

El usuario podrá solicitar la reemisión de certificados por pérdida del token o encontrarse comprometida su clave privada por un máximo de tres veces, al cabo de las cuales deberá cancelar nuevamente por el servicio de certificación digital.

Suspensión y revocación del Certificado

La suspensión del certificado generado por la ADSIB, usualmente precede a la revocación. Ambos se harán de acuerdo a los procedimientos internos con los que la ADSIB trabaja y a solicitud del usuario o autoridad competente. La ADSIB podrá suspender o revocar un certificado por motivos fundamentados técnica y legalmente, interés nacional, resguardo de la seguridad del Estado Plurinacional de Bolivia o interés del pueblo boliviano, mediante Resolución Administrativa de su Máxima Autoridad Ejecutiva.

Procedimiento de revocación

Se procederá a la revocación de un certificado en los siguiente casos:

a. En caso que el usuario haya notificado la perdida del dispositivo y/o que su clave privada haya estado comprometida en algún caso.
b. Por vencimiento de la validez del certificado.

En estos casos, el usuario deberá seguir los siguientes casos.

a) Ingresar a su cuenta de usuario en el sistema de solicitud de certificados disponible en el sistema de solicitud de certificado de la página web www.firmadigital.bo.
b) Solicitar media su cuenta de usuario la revocación del certificado.

La ECP verificará la validez de la solicitud de revocación, llamándole al teléfono celular del cliente y

preguntándole si ¿realmente quiere realizar la revocación de su certificado?.

Servicios de estado de certificados

La ADSIB posee servicios de comprobación de estado de los certificados. Dichos servicios son la lista de certificados revocados y el acceso OCSP para acceso en línea a la comprobación del estado de las mismas.

Fin de la suscripción

El usuario podrá dar el uso permitido al certificado durante su período de vigencia. Llegado a término del período de vigencia del certificado, el usuario podrá optar al proceso de renovación. Si el usuario no opta por la renovación, tendrá a su disponibilidad en los archivos de la ADSIB por un lapso 5 años los registros correspondientes a la generación de su certificado.

Depósito de las claves y recuperación.

Si el usuario no opta por la renovación o reactivación, tendrá a su disponibilidad en los archivos de la ADSIB por un lapso de 5 (cinco) años, los registros correspondientes a la generación de su certificado.

La clave privada de la ADSIB se custodia en un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas es necesario el uso de tarjetas inteligentes.

Si el usuario extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado debiendo cumplir los requisitos nombrados en este documento.

5. Controles operacionales o de gestión.

Controles de seguridad física

Los controles de seguridad se enmarcan en los lineamientos establecidos en la Resolución Administrativa RAR -DJ-RA TL LP 31/2015 emitida por la ATT.

La ubicación del Centro de Datos de la ADSIB está en el Edificio de la Vicepresidencia del Estado Plurinacional de Bolivia, ubicado en el centro de la ciudad de La Paz, entre las calles Ayacucho y Mercado No 308.

La construcción del Centro de Datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa en materia de seguridad. El Centro de Datos opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

Adicionalmente el Centro de Datos reúne condiciones y características de construcción para hacer frente a diferentes situaciones de emergencia. Igualmente, mantiene un perímetro de seguridad y cuenta con cinco (5) niveles de acceso biométrico.

El Centro de Datos desde donde opera la ADSIB, mantiene respaldos en caso de ocurrencia de una contingencia que afecta la integridad física y digital de la referida sede administrativa y puede ofrecer de esa manera una garantía de su continuidad operacional.

- **Acceso físico**

Mantiene medidas de control de acceso tanto lógicas (aplicativo de certificación) como físicas (equipos) garantizando la integridad y seguridad de los servicios prestados. Para el control de acceso físico existen cinco (5) capas de seguridad, desde el exterior hasta los servidores donde está instalado el aplicativo de certificación.

Además de procedimientos de seguridad que restringe el acceso solo a personal autorizado para el acceso a cada una de las cinco (5) capas de seguridad física y conocer la información de acceso (login y password) del sistema operativo de los equipos que conforman la cabina de la Firma Digital.

- **Alimentación eléctrica y aire acondicionado**

La construcción donde se encuentran instalados los servidores de la cabina de la Firma Digital de la ADSIB cuenta con dos (2) líneas de tensión distintas, una principal y otra auxiliar, dichas líneas de tensión están conectadas a dos (2) fuentes de energía ininterrumpida (UPS), los cuales a su vez están conectadas a una (1) planta generadora de energía.

La construcción cuenta con su sistema de aire acondicionado, que recibe el mantenimiento necesario para su uso regular.

- **Exposición al agua**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad.

- **Protección y prevención de incendios**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad, al contar con un sistema anti- incendios.

- **Sistema de almacenamiento**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad, al contar con planes y procedimientos de mantenimiento.

- **Eliminación de residuos**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad.

- **Copia de seguridad**

El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad, al contar con planes y procedimientos de gestión de incidentes.

Controles procedimentales

- **Roles de confianza**

La ADSIB mantendrá un esquema de gestión y operación basado en una estructura plana, sustentada sobre la interacción e interdependencia del personal en sus diversos roles y funciones.

La ADSIB, se encuentra dividida en funciones de operación y administración. La Dirección Ejecutiva se constituye en el nivel con mayor poder de decisión y mando dentro de la organización. Las actividades de planificación serán coordinadas por la Encargada de Planificación y Proyectos en adición a las Unidades encargadas de la implementación, mantenimiento y actualización del Centro de Datos.

Todas las decisiones que se realizaren a las operaciones técnicas y administrativa serán evaluadas por

el Comité de Gestión de Calidad.

- **Número de personas requerida por tarea**

El número de personas requeridas por tarea, y el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección Ejecutiva.

- **Identificación y autenticación para cada rol.**

La identificación y autenticación de cada rol, así como el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección Ejecutiva.

Controles de seguridad del personal

- **Requerimientos de calificación, experiencia y acreditación**

El personal involucrado en el control y la operación de la firma y certificado digital estará suficientemente calificado y con la experiencia necesaria para cumplir con las funciones asignadas a su rol y recibirá entrenamiento continuo para garantizar los niveles de calidad sobre las políticas de seguridad y los procedimientos.

- **Formación y frecuencia de actualización de la formación.**

El personal de la ADSIB recibe al menos una vez al año capacitación en áreas de desarrollo asociada a su labor directa u orientadas al desarrollo de destrezas necesarias para la prestación acorde y conforme de sus servicios.

- **Frecuencia y secuencia de rotación de tareas**

La asignaciones de roles y funciones dentro de la ADSIB se encuentran asociadas a la descripción del cargo que ocupa cada empleado dentro de la organización y al esquema de trabajo marcado en el organigrama interno.

- **Sanciones por acciones no autorizadas**

Todo procedimiento no contemplado en el presente documento de Políticas de Certificación, deberá contar con la aprobación expresa y por escrito de la Dirección Ejecutiva de la ADSIB, de lo contrario

será considerado como acto de sabotaje a los fines internos de la ADSIB y será sancionado con despido justificado, por incumplimiento de las obligaciones que impone la relación de trabajo.

- **Requerimientos de contratación de personal, controles periódicos de cumplimiento, finalización de los contratos.**

La ADSIB sigue la normativa configurada bajo el sistema de contratación estipulado por el Estado Plurinacional de Bolivia. La ADSIB tiene un sistema de control periódico a través de la presentación de informes internos relacionado a cada acción llevada a cabo que deba ser informada.

Controles para registros de auditoría

- **Tipos de eventos registrados**

La ADSIB, almacena registros electrónicos de eventos (logs) relativos a su actividad como Entidad Certificadora Pública. Estos registros son almacenados, de forma automática y electrónica y en los casos del acceso físico en formato papel y otros medios.

Cada registro de eventos incluye datos relativos a la fecha y hora en que se produjo, número de serie, descripción del evento y el sistema o persona que lo origino. Los records mínimos de auditoría que deben ser mantenidos incluyen:

- Instalación y Configuración del Sistema Operativo.
- Instalación y Configuración de cualquier aplicación instalada en el equipo.
- Instalación y Configuración de la Autoridad de Certificación.
- Instalación y Configuración del Módulo Criptográfico.
- Accesos o intentos de acceso al equipo.
- Actualizaciones.
- Mantenimientos.
-Realización de copias de seguridad.

- Eventos del software de certificación:

- Gestión de usuarios.
- Gestión de Roles.
- Gestión de Plantillas de Certificados.
- Lista de control de acceso.

- Gestión de Certificados (todo lo contemplado en el ciclo su vida)

- Eventos relacionados con el acceso físico:

- Acceso del personal al Data Center.
- Acceso del personal a los equipos y sistemas
- Acceso del personal para limpieza.

-Eventos de acciones correctivas y preventivas:

- Errores de Hardware.
- Errores de Software.

- **Frecuencia de procesado de logs**

Se llevan a cabo en cualquier momento que se realice una operación en la raíz de certificación de la ADSIB. El personal de operaciones notifica a su administrador de seguridad cuando un proceso o acción causa un evento crítico de seguridad o discrepancia.

- **Periodo de retención para los logs de auditoría**

Los periodos de retención de registros se mantienen por un período de dos (2) años.

El sistema de recolección de auditoría de la ADSIB es una combinación de procesos automáticos y procedimientos manuales desempeñados por la ATT además de los sistemas operativos y por el personal operacional.

Por lo tanto, el sistema es mantenido mediante mecanismos de control de acceso y separación de roles con relación al software y el hardware que manejan la recolecciones automáticas y mediante procedimientos operacionales confidencialmente documentados, conocidos y seguidos por el personal de la ADSIB.

Adicionalmente, la integridad de los eventos de auditoría se protege mediante la firma de cada evento con la clave privada de la persona que lleva acabo la acción, evitando cualquier vulnerabilidad.

La ADSIB tiene planes y procedimientos para el análisis de vulnerabilidades en el desempeño de sus funciones.

Archivo de registros

Todos los records de la ADSIB, referentes a la operación de sus servicios de certificación son archivados y retenidos por un período mínimo de diez (10) años.

El recurso de tiempo para la ATT es verificado periódicamente de manera independiente y todos los records automatizados de la raíz de certificación de la ADSIB, están asociados a la hora y fecha de su ocurrencia. Los archivos de records se mantienen bajo estricto control de acceso y están sujetos a la inspección de auditores.

Todos los archivos de records e información de identificación será archivada directamente por la ADSIB. La ADSIB tendrá en su custodia los records e información por un período de diez (10) años a partir de la fecha de expiración del certificado y hará sus mejores esfuerzos para que dicha entidad cumplan con sus obligaciones en esta materia.

El período de retención puede ser extendido con relación a algunos records e información en particular a solicitud de los servicios especiales de archivo. En todo caso los records pueden ser archivados en papel o en forma digitalizada.

Cambio de clave y cambio de claves del certificado

La ADSIB podrá cambiar su par de claves por los siguientes motivos:

a) De algún modo se ha visto comprometida la clave privada de la ADSIB.
b) Por la caducidad del certificado firmado por la ATT para las operaciones de la ADSIB.
c) Por falla o desastre de los equipos necesarios para la firma y que no sea posible habilitar los planes de recuperación.

Procedimientos para recuperación de desastres

La ADSIB cuenta con un plan de continuidad de negocio y recuperación de ante desastres, ante el evento de un eventual compromiso parcial o total de la construcción del Centro de Datos. El Plan de recuperación ante desastre es revisado periódicamente a la luz de los cambios riesgos en el ambiente.

El plan de recuperación ante desastre está orientado a:

- Fallas/corrupción de recursos de computación;

- Compromiso de la integridad de la clave; y

- Desastres naturales y terminación.

La Dirección Ejecutiva debe tomar los correctivos y emprender las actividades necesarias para restablecer el sistema de certificación en el momento de presentarse un escenario de desastre. En el plan de continuidad de negocio y recuperación ante desastre, se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre.

Procedimientos para concluir las operaciones de la Entidad Certificadora Pública.

La ADSIB tienen establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones. La ADSIB tiene elaborado un Plan de Cese de Actividades que está detallado en el Apéndice 1 de este documento.

6. Controles de Seguridad Técnica.

- **Instalación y generación del par de claves**

La ADSIB genera su par de claves (pública y privada) bajo el procedimiento establecido los procedimientos de la entidad y en cumplimiento de la normativa vigente con respecto a la firma digital y las regulaciones de la ATT

Esto incluye el desarrollo de una ceremonia de generación del par de claves en presencia de representantes de la Vicepresidencia del Estado (ente tutor de la ADSIB), la ATT y Notario de Fe Pública.

El resguardo de la clave privada se desarrolla conforme a la regulación establecida por la ATT.

- **Protección criptográfica de la clave privada**

La ADSIB posee una copia de seguridad de la clave privada bajo las mismas condiciones de seguridad que la original.

- **Controles**

Se utiliza un control multipersonal para la clave privada, según los roles asignados a los funcionarios de la ADSIB y que participan de las ceremonias de firma de certificados.

- **Otros aspectos de la gestión del par de claves.**

Archivo de la clave pública

La ADSIB publica su clave pública hasta el vencimiento del último certificado emitido por la misma.

Períodos operativos de los certificados y período de uso para el par de claves

El par de claves de la ADSIB tendrá la misma duración del certificado correspondiente emitido por la ATT. Para proseguir con sus operaciones la ADSIB emitirá un nuevo par de claves y solicitará el certificado correspondiente a la ATT, conforme a procedimiento.

- **Datos de activación**

La ADSIB tiene planes y procedimientos internos para los datos de activación.

- **Controles de seguridad informática**

La ADSIB ha definido una serie de controles de seguridad aplicables a los equipos informáticos, tales como el uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y pruebas de seguridad.

- **Controles de seguridad sobre el ciclo de vida de los sistemas**

El software de la ADSIB usado por la clave pública para la emisión de certificado y el manejo del ciclo de vida ha sido desarrollado de acuerdo con los requerimientos de la Resolución Administrativa de la ATT-DJ-RA TL LP 32/2015.

El HSM utilizado por la clave pública de la ADSIB cumple con los requerimientos FIPS 140-2. Los controles para el manejo de la seguridad se cumplen mediante una separación rígida de los roles del operador para cumplir los requerimientos de la política de seguridad establecida durante todo el ciclo

de vida de las claves se deben implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la ADSIB.

- **Seguridad de la red**

El hardware y software para la infraestructura de clave pública de la ADSIB son mantenidos "off-line" en una instalación de alta seguridad dentro de un exhaustivo control de seguridad y rigurosos controles de acceso interno.

Se mantiene sofisticados sistemas de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso. Adicionalmente, la raíz de certificación de la ADSIB se mantiene fuera de línea y no se relaciona con ningún componente externo.

- **Sincronización horaria.**

El Data Center de la ADSIB se mantiene "off-line", por lo que, la sincronización permanente en línea de la hora no se lleva acabo. La ADSIB tiene planes y procedimientos para darle mantenimiento a la hora y asegurar la calidad de su trabajo.

7. Perfiles de Certificado, CRL y OSCP.

7.1 Perfil del Certificado de la Entidad Certificadora Raíz (ECR)

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

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

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

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

7.2 Perfil del Certificado de la Entidad Certificadora Pública

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

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

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

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

7.3 Perfil de la CRL de la Entidad Certificadora Pública

El formato de las Listas de Certificados Revocados tendrán los siguientes contenidos y atributos mínimos:

a) Versión (versión): el valor del campo es 1 (corresponde a la versión 2 del estándar)
b) Algoritmo de firma (signatureAlgorithm): Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Pública para firmar la Lista de Certificados Revocados
c) Nombre del Emisor (Issuer): CN =”Entidad Certificadora ADSIB”; O = “ADSIB”; C = “BO”.
d) Día y Hora de Vigencia (This Update): Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
e) Próxima actualización (Next Update): Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
f) Certificados Revocados (Revoked Certificates): contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas

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

a) Identificador de la Clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey (clave pública correspondiente a la clave privada usada para firmar la Lista de Certificados Revocados)
b) Número de Lista de Certificados Revocados (CRL Number): número entero de secuencia incremental para una CRL y una Entidad Certificadora determinadas.
c) Extensiones de un elemento de la Lista de Certificados Revocados.
d) Código de motivo (Reason code): indica la razón de revocación de un elemento de la CRL

7.4 Perfil del OCSP de la Entidad Certificadora Pública

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

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

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

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

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

ii. Cuando se emite una respuesta OCSP, se sugiere requerir que se consideren los siguientes datos:

a) Versión.
b) Identificador de la Entidad Certificante Autorizada o de la entidad habilitada que emite la respuesta.
c) Fecha y hora correspondiente a la generación de la respuesta.
d) Respuesta sobre el estado del certificado.
e) Extensiones opcionales.
f) Identificador de objeto (OID) del algoritmo de firma.
g) Firma de respuesta.

iii. Una respuesta a una consulta OCSP debería contener:

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

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

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

7.5. Formato para el Certificado Digital de un Persona Natural o Física.

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

- Versión (version): El valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECA.
- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
- Nombre del Emisor (issuer): CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón social de la ECA;C=BO de acuerdo a ISO3166
- Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Nombres y Apellidos de la persona natural; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).
- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

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

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

7.6. Formato para el Certificado Digital de una Persona Jurídica

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

- Versión (version): El valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECA

- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA)..
- Nombre del Emisor (issuer): CN = "Entidad Certificadora"; y el nombre de la ECA; O= Razón social de la ECA; C = BO de acuerdo a ISO3166.
- Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón social de la empresa o institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).
- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

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

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

7.7. Formato para el Certificado Digital de Cargo Público

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

- Versión (version): El valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECA.
- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
- Nombre del Emisor (issuer): CN = "Entidad Certificadora"; y el nombre de la ECA; O = Razón

social de la ECA; C = BO de acuerdo a ISO3166.

- Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Nombres y Apellidos del servidor público; O = Nombre de la institución pública a la que pertenece; OU = Unidad Organizacional de la que depende el funcionario público (opcional); T = Cargo del servidor público; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).
- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 2048 bits.

ii. Las extensiones del Certificado Digital de Cargo Público serán las siguientes:

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

8. Administración Documental.

- **Procedimiento para cambio de especificaciones**

La ADSIB cuenta con procedimientos internos para la administración de los cambios sobre la presente Política de Certificación.

En caso de que la ADSIB desee una modificación en la presente política deberá realizar la solicitud a la ATT con la correspondiente justificación, la ATT evaluará la solicitud y en caso de aprobarla, realizará la modificación y posterior publicación de la nueva versión.

- **Procedimientos de Publicación y Notificación.**

La ATT publicará en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos remplazados junto con la publicación de la nueva versión.

La ADSIB deberá notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación. De la misma forma, la ADSIB deberá publicar en su sitio web cualquier modificación aprobadas por la ATT y notificar a los usuarios finales de los cambios realizados en caso de ser necesario

Apéndice 1.

Plan de Cese de actividades

1. Introducción

La Ley 164 de Telecomunicaciones, tecnologías de información y comunicación establece en su artículo 83 que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) prestará el servicio de certificación para el sector público y la población en general a nivel nacional.

En caso que la mencionada ley otorgue las atribuciones de Certificación Pública a otra entidad, la ADSIB deberá implementar el Plan de Cese de Actividades de Entidad Certificadora.

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) presentó la Resolución Administrativa RAR -DJ-RA TL LP 32/2015 que establece los requisitos, condiciones legales, económicas y técnicas para la autorización de la prestación de servicio de Firma y Certificación Digital. El artículo 12 de esta Resolución establece como requisito la presentación del Plan de Cese de actividades.

En este sentido, el presente documento tiene como objetivo delinear las estrategias para que la ADSIB culmine con las actividades como Entidad Certificadora Pública, en el supuesto que así disponga un cambio en la Ley 164.

2. Supuestos para el cese de actividades.

El cese de actividades de la ADSIB como Entidad Certificadora Pública se producirá siempre y cuando se modifique el artículo 83 de la Ley 164, que otorga a la institución la atribución del servicio de certificación digital.

La ADSIB tienen establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones.

3. Sujetos involucrados en el proceso de cese de actividades

El cese de actividades de la ADSIB como Entidad Certificadora Pública involucrará directamente a todos los y las titulares de los certificados digitales. La ADSIB tomará una serie de recaudos para minimizar el impacto de la finalización de sus servicios, que serán descritos en el procedimiento siguiente.

4. Procedimiento general

La función del Plan de Cese de actividades de la Entidad Certificadora Pública es asegurar que la transición de funciones a otra entidad se realice de manera ordenada, resguardando la información generada durante el período de actividad.

El período de implementación del Plan se realizará desde la declaración de Cese de Actividades hasta la inhabilitación lógica y física de la Autoridad Certificante, la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes. A partir del cese de actividades, la ADSIB ya no emitirá nuevos certificados, solo se remitirá a publicar la lista de certificados revocados.

La ADSIB en todo este período velará por minimizar el impacto de los titulares de los certificados digitales, a través del desarrollos de las estrategias y procedimientos delineados a continuación.

4.1. Publicación

Ante la declaración del cese de los servicios de certificación, la primera tarea será publicar la información en el sitio web: www.firmadigital.bo. Esta publicación deberá realizarse con dos meses de antelación. Si es que hubiese suscriptores a nivel nacional, también se deberá publicar en un medio de difusión nacional.

4.2. Notificación

La ADSIB notificará a todos los y las suscriptores de los certificados digitales del cese de actividades cuyos certificados permanezcan en vigencia. La misma se llevará a cabo con una antelación mínima de dos (2) meses.

La notificación se realizará mediante correo electrónico firmado digitalmente y la página web de la institución, por el transcurso del tiempo que dure la transición del servicio a otra entidad. Las mismas indicarán la fecha precisa del cese de actividades, señalando además que de no existir objeción a la transferencia de los certificados digitales, dentro del plazo de quince (15) días hábiles, contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido la transferencia de los mismos.

Si se hubiese emitido certificados a nivel nacional, deberá publicarse en un medio de prensa.

4.3. Solicitudes del certificado

Una vez anunciado el cese de actividades de la ADSIB como Entidad Certificadora Pública, se rechazará la solicitud de emisión de un nuevo certificado, de cualquier tipo, por parte de un suscriptor dentro de los sesenta (60) sesenta días calendarios anteriores a la fecha prevista para el cese.

La ADSIB también rechazará toda solicitud de renovación de un certificado por parte de un suscriptor de los sesenta (60) días corridos anteriores a la fecha prevista para el cese.

4.4. Revocación de Certificados y Lista de Certificados Revocados

La ADSIB deberá proceder de la siguiente manera para la revocación de los certificados.

a) Se podrá revocar certificados de suscriptores hasta el mismo día y hora del cese de actividades. Solamente podrá efectuar revocaciones a solicitud de sus suscriptores. Si los suscriptores, después de haber sido notificados del cese de actividades de la Entidad Certificadora, dentro del plazo de quince (15) días contados de la fecha de la notificación, se entenderá que el usuario ha consentido la transferencia del certificado digital.

b) Colorará a disposición de la ATT los certificados que se encuentre vigentes, hasta tanto se produzca el vencimiento de la totalidad de los certificados emitidos por la ADSIB.

c) Actualizará la lista del repositorio de los certificados digitales.

d) Emitirá una lista de certificados revocados (LCR) hasta la fecha prevista de cese de actividades.

e) Inmediatamente de revocados los certificados, la ADSIB emitirá una última lista de certificados revocados.

f) La última lista LCR estará disponible para consultas, como mínimo hasta el último día del cese de funciones.

4.5. Desactivación y custodia de los equipos

A partir del cese de actividades, los equipos de la ADSIB, incluidos los que soporta a la clave privada, quedarán desafectados de la emisión y revocación de certificados. No obstante, permanecerán en custodia de la ADSIB, para:

a) Satisfacer eventuales requerimientos de información, en caso de que suscitaren conflictos.

b) La posible necesidad de rehacer la última lista de certificados revocados.

Después, del periodo de custodia, la ADSIB podrá disponer libremente de los equipos que hubiese dispuesto para el servicio de la certificación digital.

En forma previa a la desactivación se generarán copias de respaldo de toda la información disponible.

Los equipos de publicación de CRL continuarán prestando el servicio hasta la finalización del último día de la fecha del cese de actividades de la ADSIB como Entidad Certificadora, según lo mencionado en el punto “4.4.- Revocación de Certificados y Lista de Certificados Revocados”.

4.6. Transferencia de certificados

Al producirse el cese de sus actividades, se admitirá que la ADSIB realice una transferencia de los certificados emitidos a sus suscriptores a favor de otra entidad certificadora, establecido en la Ley 164. Para ello se requerirá un acuerdo previo entre ambas entidad certificadora, con aprobación de la ATT, Certificadora Raíz, que deberá ser firmado por las máximas autoridades respectivas.

Dicho acuerdo debe indicar que la Autoridad Certificante continuadora toma a su cargo la administración de la totalidad de los certificados emitidos por la ADSIB que cesa sus actividades, que no hubieran sido revocados a la fecha de la transferencia. Se enviará copias del mencionado acuerdo a la ATT para su archivo.

Asimismo, la ADSIB transferirá a la Autoridad Certificante continuadora toda la documentación que obre en su poder y que hubiera generado en el proceso de emisión y administración de certificados, así como la totalidad de los archivos y copias de resguardo, en cualquier formato y toda otra documentación referida a su operatoria.

La ADSIB informará acerca de la transferencia en las publicaciones y notificaciones que efectúe referidas al cese de sus actividades mencionadas en los apartados 4.1 y 4.2. Además, cumplirá con la totalidad de los procedimientos indicados en el mismo.

4.7. Procedimientos

Una vez anunciada la fecha del cese de funciones de la ADSIB como Entidad Certificadora Pública, se lo comunicará a todo el personal y cada cada uno de los roles deberá proceder de acuerdo a los descrito en este Plan. Para este efecto, se distribuirá una copia de este documento a todo el personal directamente o indirectamente involucrado.

El Comité de Gestión de Calidad de la Entidad Certificadora ejercerá la supervisión de las operaciones relacionadas, tomando en cuenta el resguardo de la información generada, y velando por la minimizar el impacto del servicio a los suscriptores.

4.8. Resguardo de información histórica

Al finalizar la ADSIB el cese de actividades, deberá resguardar una importante cantidad de información. Los plazos para la conservación de documentos están detallados en el documento de Procedimientos y Condiciones para la conservación de documentos de la Entidad Certificadora.

Asimismo, ADSIB conservará toda la información relacionada con su servicio de certificación digital, detalladas a continuación:

- Los archivos de documentación presentada por solicitantes y suscriptores;
- La documentación relacionada con pedidos de revocación;
- La documentación generada en las ceremonias digitales.

También guardará una copia de la información generada mientras la ADSIB estuvo activa:

- La última lista de certificados revocados;
- El backup de los servidores y de su configuración;
- Los libros de Actas.

5. Modificaciones al Plan de Cese de Actividades

Toda modificación a las previsiones de este plan se hará con intervención del Comité de Gestión de Calidad de la Firma digital. Antes de su puesta en vigencia, el documento modificado será sometido a la aprobación de la Autoridad Certificadora Raíz, la ATT.

Apéndice 2
Política de Protección de Datos Personales

1. Introducción

1.1. Descripción general.

Descripción del servicio

Un certificado digital emitido por ADSIB le permite al cliente realizar firmas digitales avanzadas y autenticar su identidad con la validez legal, vincula un documento digital o mensaje electrónico de datos y garantiza la integridad del documento digital o mensaje electrónico con firma digital .La certificación que emite ADSIB, contempla tres destinatarios: cargos públicos, personas jurídicas y personas naturales.

A nivel conceptual, la Firma Digital consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos digitales. La clave privada siempre se encuentra en posesión del firmante y es la utilizada para realizar firmas. La pública se divulga y es la utilizada para verificar una firma de otro sujeto.

Todo lo descrito se encuentra validado por la Resolución Administrativa Regulatoria RAR -DJ-RA TL LP 32/2015 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

1.2. Identificación y nombre del documento.

Políticas de Protección de Datos

La Entidad Certificadora Pública considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que cursan a través de las TIC's, para otorgar seguridad y protección a la intimidad del usuario que navega en la red .

- **Nombre**

El presente documento lleva como titulo "Contenido mínimo de las políticas de certificación para una entidad certificadora. Políticas de certificación. Apéndice 2. Política de Protección de Datos Personales". Se constituye en su versión final, sin revisiones.

- **Versión fecha de elaboración**

El documento fue elaborado desde el 21 de noviembre hasta el 21 de diciembre del año 2014.

- **Fecha de actualización**

A ser acordado una vez se realicen las revisiones necesarias.

- **Sitio web de consulta.**

El sitio web de consulta es: www.firmadigital.bo.

2.-Conceptos fundamentales:

a) Archivo o Banco de Datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento físico, electrónico, magnético o informático, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

b) Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada .

c) Cesión de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.

d) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.

e) Datos personales: toda información de cualquier tipo referida a personas individuales o colectivas determinadas o determinables.

f) Datos sensibles: datos personales que revelen filiación política o filosófica, credo religioso, ideología, afiliación sindical e informaciones referentes a origen racial y étnico, salud u orientación sexual.

g) Destinatario: persona individual o colectiva, pública o privada, que reciba cesión de datos, se trate o no de un tercero.

h) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.

i) Encargado del tratamiento: persona individual o colectiva, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable del archivo o banco de datos o del tratamiento.

j) Tercero: la persona individual o colectiva, pública o privada, distinta del titular del dato, del responsable del archivo o banco de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

k) Responsable del tratamiento: persona individual o colectiva, pública o privada, propietaria del archivo o banco de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

l) Titular de los datos: es la persona natural o jurídica a quien se refiere la información que reposa en un archivo o banco de datos.

m) Tratamiento de datos personales: Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión .

n) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en un archivo o banco de datos propio o a través de conexión con los mismos.

o) Fuentes accesibles al público: aquellos archivos o banco de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

p) Firma Digital: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

q) Protección de datos personales: Toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable.

r) Servicio de certificación digital: Consiste en emitir, revocar y administrar los certificados digitales utilizados para generar firmas digitales.

s) Servicio de registro: Consiste en comprobar y validar la identidad del solicitante de un certificado digital, y otras funciones relacionadas al proceso de expedición y manejo de los certificados digitales.

3.- Principios:

Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios:

Principio de Finalidad.-

La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;

Principio de Veracidad.-

La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;

Principio de Transparencia.-

Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;

Principio de Seguridad.-

Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;

Principio de Confidencialidad.-

Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

4.- Derechos de los Titulares de Datos:

Los titulares de los datos, tendrán los siguientes derechos:

- Derecho de información y contenido de la información.
- Derecho de conocer los datos registrados.
- Derecho de rectificación, actualización, inclusión o eliminación.
- Datos sensibles: Ninguna persona puede ser obligada a proporcionar datos sensibles, como ser: ideología, religión, salud, origen racial o étnico y otros. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular y/o cuando medien razones de interés general autorizadas por ley, o cuando la Entidad Certificadora tenga mandato legal para hacerlo.

5.- Marco legal nacional para el tratamiento de los datos personales en materia de telecomunicaciones:

La Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información Y Comunicación, en su Art. 56 (Inviolabilidad y Secreto de las Telecomunicaciones) señala*:* "*En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma"*.

Por otro lado, el Art. 56 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, a fin de garantizar los datos personales y la seguridad informática de los mismos, adopta 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 y privado 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 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.

El Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, en el Art. 176 establece:

Artículo 176.- (Protección de los Datos Personales).

I. El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

II. Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los

usuarios del servicio, salvo en los siguientes casos:

a) De existir una orden judicial específica;

b) Con consentimiento previo, expreso y por escrito del usuario titular;

c) En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo.

III. El operador o proveedor de servicios deberá coadyuvar en la identificación de los presuntos responsables de vulneraciones a la inviolabilidad, secreto de las comunicaciones, protección de los datos personales y la intimidad de los usuarios, que su personal pudiera cometer en las instalaciones del operador o proveedor.

IV. La ATT aprobará los procedimientos y medidas utilizadas por los operadores y proveedores para salvaguardar la inviolabilidad y secreto de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

V. Queda prohibido que los operadores y proveedores de servicios permitan el acceso a registros o bases de datos de sus usuarios, ya sea de manera individual o a través de listas de usuarias, usuarios o números, con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita de la usuaria o usuario que desee recibir dicha publicidad .

Asimismo de conformidad a lo establecido en el artículo 43 inciso i) del D.S 1793, la Entidad Certificadora mantendrá 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.

Finalmente, el Art. 43 inciso b) del Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013, señala: "*Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT* ".

6.- Marco jurídico aplicable:

Asimismo, las disposiciones legales y reglamentarias que regulan la protección de datos, son:

- Constitución Política del Estado
- Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación, de fecha 08 de agosto de 2011.
- Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013.
- Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, de fecha 24 de octubre de 2012.
- Decreto Supremo N° 28168, que garantiza el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo, de fecha 17 de mayo de 2005.
- Estándares Técnicos emitidos por la ATT.

Calle Ayacucho esq. Mercado No. 308
Edif. Vicepresidencia del Estado, piso 3
Geo#: 6mpd1sdnm / La Paz - Bolivia

Telf. (591-2) 2 200720 /30 /40
contacto@adsib.gob.bo
www.adsib.gob.bo

VERSIONES:

Versión: 4
Fecha: 2 de febrero de 2016
Cambios:

- Incorporación de la mención a la RAR ATT-DJ-RA TL 1538/2015.
- Cambio de la fecha de actualización del documento.
- Cambio de los formatos autorizados de certificados digitales según la RAR ATT-DJ-RA TL 1538/2015.
- Supresión de la mención de verificación de los datos de servidores públicos con la Contraloría.
- Nueva redacción sobre la generación del par de claves.
- Corrección de la URL: www.firmadigital.bo
- Errores de ortografía.