Términos y Condiciones para la provisión de servicios de Certificación Digital

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

La Paz - Bolivia

1.- INTRODUCCIÓN

Los Términos y Condiciones para la Provisión de la Certificación Digital contempla la descripción del servicio que implementará la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) en tanto tenga la calidad de Entidad Certificadora Pública.

Como establece la Ley N°164 de Telecomunicaciones, la Entidad Certificadora Pública (en adelante ECP) prestará el servicio de Certificación Digital otorgando validez a los documentos firmados digitalmente.

La implementación del uso de la firma digital en Bolivia contribuirá a reducir los procesos burocráticos y los consiguientes tiempos necesarios para cumplirlos, como también facilitar el intercambio de información entre instancias, entidades, personas y empresas. De este modo la ADSIB se consolida como líder en la prestación de servicios en tecnologías de la información y comunicación. Para alcanzar este objetivo es necesario desarrollar la confianza de los usuarios en el servicio, en cuanto a su calidad, idoneidad y seguridad.

El presente documento ofrece una descripción detallada del servicio que ofertará la ADSIB, velando por el interés del pueblo boliviano, la calidad y confianza que requieren los usuarios.

2.- DESCRIPCION DEL SERVICIO Y ASPECTOS ASOCIADOS

La Agencia para el Desarrollo de la Información en Bolivia (ADSIB) se constituye como una Entidad Descentralizada bajo tuición de la Vicepresidencia del Estado Plurinacional de Bolivia. 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.

De acuerdo a la Ley N° 164 Ley General de Telecomunicaciones y sus Reglamentos vigentes, establecen que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB, se constituye en la Entidad Certificadora Pública debiendo prestar el servicio de certificación digital para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la presente Ley y velará por la autenticidad, integridad y no repudio entre las partes.

Un certificado digital emitido por la ADSIB le permite al signatario o usuario 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 digital que emite la ADSIB, contempla tres destinatarios: cargos públicos, personas jurídicas y personas naturales.

Asimismo, el servicio de Certificado Digital responde a formatos y procedimientos de calidad y estándares reconocidos internacionalmente y fijados por la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transporte (ATT), conteniendo la información necesaria para la identificación, vigencia y verificación de la firma digital.

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.

3.- ALCANCE O COBERTURA DE LA PRESTACIÓN DEL SERVICIO.-

La ADSIB en tanto se constituya en Entidad Certificadora Pública podra emitir certificados a:

- Personas naturales
- Personas jurídicas
- Cargos Públicos

La Ley N° 164, Ley General de Telecomcunicaciones, establece la validez jurídica y probatoria de:

1. El acto o negocio jurídico realizado por persona natural o jurídica en documento digital y aprobado por las partes a través de firma digital, celebrado por medio electrónico u otro de mayor avance tecnológico.
2. El mensaje electrónico de datos.
3. La firma digital.

La misma ley realiza excepciones en los siguientes actos y hechos jurídicos de su celebración por medio electrónicos:

1. Los actos propios del derecho de familia.
2. Los actos en que la ley requiera la concurrencia personal física de alguna de las partes.
3. Los actos o negocios jurídicos señalados en la ley que, para su validez o producción de determinados efectos, requieran de documento físico o por acuerdo expeso de partes.

4.- MODALIDADES DE PRESTACIÓN DEL SERVICIO Y DEFINICIONES.

La ADSIB en tanto Entidad Certificadora Pública ofertará el siguiente servicio:

- Contratación por la emisión del Certificado Digital.

El servicio de certificación digital que presta la ADSIB comprende tres tipos de certificados conforme a lo establecido en la normativa técnica de la ATT. Los tipos de certificados son:

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.

Por cada certificado emitido y por el que se cobre la tarifa determinada según el acápite anterior el usuario se hace beneficiario del servicio de certificación por el lapso de un año (365 días calendario) o un máximo de tres remisiones de certificado digital, lo que suceda primero, que incluye:

a) Emisión del certificado digital correspondiente, incluyendo la información establecida en la

reglamentación técnica de la ATT*

b) Derecho a mantener una cuenta de usuario en el sistema de solicitud de certificados digitales de la ECP, que le permitirá al usuario:

1) Acceder a cualquiera de los certificados emitidos a su nombre y la información correspondiente a su validez, estado y vigencia.

2) Solicitar la suspensión o re activación de la validez de un certificado**

3) Solicitar la revocatoria de un certificado**

4) Solicitar la renovación de un certificado sin cambio de clave privada**

5**)** Reportar incidentes con respecto a sus certificados

6**)** Acceder al servicio de soporte técnico en línea, en los horarios establecidos por la ECP y según sus procedimientos

7**)** Solicitar la remisión de certificados por pérdida de token (hsm) 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**

c) Acceso al servicio de soporte técnico presencial en oficinas de la ECP, en los horarios y bajo los procedimientos establecidos por la misma.

d) Derecho a solicitar la suspensión, re activación, renovación, revocatoria o remisión de sus certificados en oficinas de la ECP, en los horarios y bajo los procedimientos establecidos por la misma**

e) Derecho a que cualquier persona pueda establecer el estado actual de sus certificados (válido, suspendido, revocado) a través de los servicios de Listas de Revocatoria de Certificados (CRL) o servicio OCSP, conforme a lo dispuesto por la ECP.

f) Derecho a participar de las promociones o beneficios adicionales que pueda establecer la ECP.

* La emisión del certificado no incluye el dispositivo token (hsm) para la preservación de las claves pública y privada y certificado del usuario.

**La suspensión, reactivación, renovación, revocatoria y/o remisión de certificados se realizarán conforme a los procedimientos establecidos por la ECP.

El servicio no contempla la provisión del token para la generación de la clave privada del usuario. En la página www.firmadigital.bo se publicará una lista de proveedores de token que cumplan con los estándares solicitados.

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.

Par de claves:
Es el conjunto de la clave privada y la clave pública. Las dos claves están generadas al mismo tiempo por el mismo mecanismo criptográfico. Estas dos claves son complementarias, y para cualquier operación que implique el uso de una de las dos claves, se necesita la segunda clave para cumplir la operación.

Solicitud de firma de certificado:
Una solicitud de firma de certificado (en inglés *Certificate Signing Request* - CSR) es un archivo digital que un solicitante transmite a una Entidad Certificadora para obtener la firma de su certificado. La solicitud de firma de certificado contiene las informaciones de identidad y la clave pública del solicitante, y esta firmada con la clave privada del solicitante para certificar que la solicitud es autentica.

Infraestructura de clave pública
La infraestructura de clave pública es el conjunto de todas las entidades certificadoras y usuarios de los certificados digitales y de las relaciones entre estos actores. Una infraestructura de clave pública es organizada de manera jerárquica, encabezada por una entidad certificadora raíz con certificado auto-firmado, y por debajo entidades certificadoras que emiten certificados para los usuarios. Todos los certificados emitidos en una infraestructura de clave pública pueden ser validados siguiendo un camino lógico hasta la entidad certificadora raíz, en la cual esta depositada la confianza en la infraestructura de clave pública. En el caso de la infraestructura de clave pública de Bolivia, la **Entidad Certificadora Raíz es la ATT**, y la **Entidad Certificadora Pública es la ADSIB**.

Lista de revocatoria de certificados
Una lista de revocatoria de certificados (en inglés *Certificate Revocation List* - CRL) es un archivo digital que contiene una lista de certificados revocados o suspendidos. La revocatoria o la suspensión de un certificado corresponde a revocar o suspender su validez, por algún motivo, antes de su fecha de expiración. La lista de revocatoria de certificados esta firmada por una autoridad reconocida dentro de la infraestructura de clave pública. En el caso de la Entidad Certificadora Pública - ADSIB, la lista de revocatoria esta firmada con un par de claves y un certificado dedicados de la ADSIB.

Emisión de Certificados :
La ECP emitirá los certificados que se le soliciten, una vez que se hayan aprobado dichas solicitudes mediante la comprobación del cumplimiento de los correspondientes requisitos.

Administración de Claves:
Generación de las claves públicas y privadas generadas automáticamente por el sistema, siendo su generación, administración, uso, gestión y custodia son de exclusiva responsabilidad del SIGNATARIO (A) / USUARIO (A).

Directorios de Listas de Certificados Revocados:
La ECP cuenta con repositorios o directorios de datos en los que son almacenados tanto los certificados emitidos así como los certificados revocados.

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, indicando en el certificado digital.

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 pérdida posibilita la usurpación de identidad del signatario.

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 digitial, junto a los datos de identidad del signatario.

Tiene vocación a ser de conocimiento público, y permite verificar la firma digital de un documento.

5.- REQUISITOS TÉCNICOS NECESARIOS 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 un 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.

- 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.

- 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.

La ADSIB hará todos los esfuerzos por brindar un servicio de calidad a los usuarios, tanto en los aspectos técnicos como humanos, enmarcada en una política de satisfacción de sus suscriptores. En ese contexto, la ADSIB como Entidad Certificadora Pública no se hará responsable de la suspensión del servicio por cualquier causa que no este bajo control directo de la entidad, como eventos de fuerza mayor o caso fortuito, cortes de energía prolongados, desastres naturales, interrupción en el servicio de internet por parte del proveedor del servicio, orden de suspensión o revocatoria por autoridad competente u otros.

La ADSIB tampoco se hace responsable por fallas o pérdidas de datos fruto de ataques informáticos u otros que logren sobrepasar las medidas de seguridad y procedimientos establecidos y aprobados por la Entidad Certificadora Raíz.

Los servicios de la ECP en favor del usuario, en cuanto a la certificación digital, se limitan a la firma de los certificados y publicación de las listas de revocatoria, salvo caso fortuito o fuerza mayor, y a brindar los mecanismos necesarios para la renovación, suspensión y revocatoria de los certificados firmados por la ECP. De ser posible y a criterio de la ECP, la misma ofrecerá soporte técnico a los usuarios, en el marco de lo que considere pertinente y bajo los alcances que establezca. La atención de reclamos se realizará conforme a la normativa vigente y el procedimiento establecido.

6.- HABILITACION Y PLAZO PARA LA PROVISION DEL SERVICIO.-

La ADSIB una vez que haya validado y verificado que los requisitos técnicos estén correctos y que el usuario haya registrado en el sistema el comprobante de pago, procederá a habilitar el certificado digital en un máximo de tres (3) días hábiles.

7.- TARIFAS.-

La estructura tarifaria del servicio de certificación digital es la siguiente:

Tipo de Certificado	Tarifa en Bs.
Persona Natural	195
Persona Jurídica	370
Cargo Público	450

7.1.- POLITICA TARIFARIA

A las tarifas señaladas anteriormente se aplicará la siguiente Escala Tarifara por la adquisición a escala de certificados digitales para el sector público:

Promoción por número de certificados digitales:

Sector Público

Número de certificaciones digitales	Precio por certificación digital
>30	370
>100	320
>200	245
>500	195

8.- OBTENCION, SUSPENSION, REVOCACION, VIGENCIA Y CONSERVACION DEL CERTIFICADO DIGITAL.-

De conformidad a lo señalado en el Art.28, 29, 30 y 31 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, se establecen los siguientes requisitos:

8.1.- OBTENCIÓN DEL CERTIFICADO DIGITAL.-

Para la obtención del Certificado Digital el SIGNATARIO (A) o USUARIO (A) deberá acreditar su identidad, siendo la solicitud personal y presencial; debiendo cumplir con los siguientes requisitos:

8.1.2.- Los requisitos para **personas naturales** son:

a) Fotocopia simple de su Cédula de Identidad o en el caso de ser extranjero (a) Carnet de extranjero (a).

b) Fotocopia de la última factura de pago de luz, agua o teléfono que permita verificar su dirección actual.
c) La documentación debe ser validada por la Entidad Certificadora Pública con la presentación de la documentación original por parte del solicitante.
d) Dispositivo que permita firmar un documento, donde será almacenado el Certificado Digital y custodiado (*Token o tarjetas inteligentes -smart cards-*) que cumpla con el estándar FIPS 140-2.

8.1.3.- Los requisitos para **personas jurídicas** son:
a) 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).
b) Fotocopia simple de Cédula de Identidad o en el caso de ser extranjero (a) Carnet de extranjero (a).
c) Fotocopia del nombramiento o Certificado laboral firmado por el Representante Legal.
d) Autorización original de la persona jurídica firmada por el Representante Legal.
e) En función al tipo de información que utiliza una organización/entidad las claves públicas y privada podrán ser emitidas a:

- 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 uno o varios documentos y que cumpla con los sistemas de seguridad reconocidos internacionalmente, garantizando la confiabilidad del mismo a sus usuarios o signatarios.

f) La documentación debe ser validada por la Entidad Certificadora Pública con la presentación de la documentación original por parte del solicitante.

8.1.4.- Los requisitos para los **Cargos Públicos** son:
a) Fotocopia simple de Cédula de Identidad o en el caso de ser extranjero (a) Carnet de extranjero (a).
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 será validada por la Entidad Certificadora Pública 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.
f) La documentación debe ser validada por la Entidad Certificadora Pública con la presentación de la documentación original por parte del solicitante.

8.2.- SUSPENSION DE LA VIGENCIA.-

I. La vigencia de un Certificado Digital será suspendida por la Entidad Certificadora Pública, cuando se verifique alguna de las siguientes circunstancias:
a) A solicitud del titular del certificado, debidamente comunicada a la entidad certificadora;
b) Decisión de la entidad certificadora en virtud de razones técnicas, que será previamente comunicada a los signatarios;
c) Por orden o decisión judicial debidamente fundamentada que determine la suspensión provisional de la vigencia del certificado digital.

II. En mérito a la suspensión de la vigencia, cesan de forma temporal los efectos jurídicos del Certificado Digital conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.
III. La suspensión de la vigencia del Certificado Digital será levantada por cualquiera de las siguientes causas:

a) A requerimiento del titular del certificado digital, cuando la suspensión haya sido solicitada por éste;
b) Cesación de las causas técnicas que motivaron la suspensión a criterio de la entidad certificadora;
c) Por orden o decisión judicial debidamente fundamentada que determine el cese de la suspensión de la vigencia del certificado digital.

IV. En las situaciones descritas en el parágrafo anterior, la Entidad Certificadora Pública habilitará de manera inmediata el certificado digital.
V.- La suspensión de un certificado digital, no producirá, por si sola, la invalidez jurídica de los actos que al amparo de dicho certificado se hayan realizado con anterioridad.

8.3.- REVOCACION DE UN CERTIFICADO DIGITAL.-
I. Un certificado digital será revocado en los siguientes casos:

a) A solicitud de su titular, debidamente comunicada a la entidad certificadora;
b) Por fallecimiento del titular del certificado;
c) Por disolución o quiebra de la persona jurídica titular del certificado digital, a partir de la comunicación oficial recibida por la entidad certificadora;
d) Sentencia condenatoria ejecutoriada en contra del titular del certificado digital, por la comisión de delitos en los que se haya utilizado como instrumento la firma digital;
e) Sentencia judicial que declare la ausencia o interdicción del titular del certificado digital;
f) Por requerimiento de autoridad competente conforme a Ley;
g) Cuando se corrobore que el titular del certificado digital no ha custodiado adecuadamente los mecanismos de seguridad, propios del funcionamiento del sistema de certificación, que le proporcione la entidad certificadora ;
h) De comprobarse por parte de la ATT, que se han producido vulneraciones técnicas del sistema de seguridad de la entidad certificadora que afecte la prestación de servicios de certificación digital.
i) Por incumplimiento de las causas pactadas entre la entidad certificadora con el titular del certificado digital.
j) Por proporcionar información y/o datos falsos y/o que los mismos no concuerden con el registro de identidad personal del Servicio General de Identificación Personal (SEGIP).

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

8.4.- VIGENCIA DE LOS CERTIFICADOS PARA CARGOS PÚBLICOS.-
La vigencia de los certificados digitales emitidos con relación al ejercicio de cargos públicos no será superior a un (1) año y no deberá exceder el tiempo de duración de dicho cargo público a menos que exista prórrogas de funciones en las instituciones, debiendo todo cambio en el cargo, ser comunicado a la entidad certificadora pública inmediatamente.

8.5.- CONSERVACION DEL CERTIFICADO DIGITAL.-
I. La conservación de la información contenida en un mensaje electrónico de datos o documento digital ambos con firma digital, deberá cumplir las siguientes condiciones:

a) Estar en el formato original con el que haya sido generado, enviado o recibido, demostrando su integridad, la identidad del generador del mensaje electrónico de datos o documento digital, su origen, fecha, hora de creación, destino y otros;

b) Ser accesible y disponible para posteriores consultas a requerimiento de autoridad competente;
c) Ser conservada de acuerdo a la naturaleza del mensaje electrónico de datos o documento digital y la normativa vigente.

II. Para la conservación de la información contenida en mensajes electrónicos de datos o documentos digitales, la entidad certificadora podrá utilizar el servicio de terceros, garantizando la integridad de los mismos.

III. La información que tenga por única finalidad hacer conocer el envío o recepción de un mensaje electrónico de datos o documento digital está exenta de la obligación de conservarse.

IV. Por otro lado, la Entidad Certificadora Pública aplicará sus respectivos procedimientos y condiciones para la conservación de los documentos físicos y digitalizados, respaldados en normas legales vigentes, procesos institucionales, procesos archivísticos y basados en los requerimientos de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

9.- DERECHOS Y OBLIGACIONES DE LAS USUARIAS Y USUARIOS EN RELACION AL SERVICIO.-

9.1.- 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.

9.2.- 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.

9.3.- 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, el 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.

9.4.- 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.

10.- DERECHOS Y OBLIGACIONES DE LOS SIGNATARIOS (AS) Y/O USUARIOS (AS).-

10.1.- DERECHOS DE LOS SIGNATARIOS (AS) Y/O USUARIOS (AS).-

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.

10.2.- OBLIGACIONES DE LOS SIGNATARIOS (AS) Y/O USUARIOS (AS).-
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.

11.- DERECHOS Y OBLIGACIONES DE LA ENTIDAD CERTIFICADORA PUBLICA.

11.1.- 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.

11.2.- 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 .

11.3.- 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.

12.- DERECHOS Y OBLIGACIONES DE LA ENTIDAD CERTIFICADORA PUBLICA Y ANTE TERCEROS QUE CONFIAN.-

De conformidad a lo establecido en el Art. 44 del Decreto Supremo N° 1793 Reglamento para el

Desarrollo de Tecnologías de Información y Comunicación, 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 terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

13.- ATENCION DE CONSULTAS, RECLAMACIONES Y EMERGENCIAS Y/O SERVICIOS DE INFORMACION Y ASISTENCIA.-

13.1.- ATENCION DE CONSULTAS Y EMERGENCIAS Y/O SERVICIOS DE INFORMACION.-

La Entidad Certificadora Pública – ADSIB atenderá las consultas referentes a los servicios que presta en la cuenta de correo electrónico soporte@firmadigital.bo, a los números de teléfono 2200720 – 2200730 y sistema de consultas establecidos en el sitio web www.firmadigital.bo.
Las consultas serán atendidas de Lunes a Viernes, de 08:30 a 12:00 y de 14:30 a 19:00 (GMT -4), o en los horarios de trabajo establecidos por las autoridades competentes en el territorio del Estado Plurinacional de Bolivia para la administración pública.

13.2.- PROCEDIMIENTO DE RECLAMACIONES.-

El procedimiento de Reclamaciones se regirá de conformidad a lo establecido en el Decreto Supremo 27172 Reglamento de la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial (vigente a la fecha):

13.2.1.- RECLAMACIÓN DIRECTA.-

El usuario tiene el derecho de recibir por parte de la Entidad Certificadora Pública, a través de su Oficina de Atención al Consumidor – ODECO, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación del servicio. Asimismo puede solicitar la devolución de los importes indebidamente pagados.
Asimismo, el usuario o un tercero por él, previa identificación, presentará su reclamación, en una primera instancia ante la Entidad Certificadora Pública.
Por otro lado, la reclamación será presentada en forma escrita o verbal, gratuita, por cualquier medio de comunicación, dentro de los veinte (20) días del conocimiento del hecho, acto u omisión que la motiva.
El plazo que la Entidad Certificadora Pública tiene para resolver la reclamación se regirá de acuerdo a lo establecido en el Art. 57 del Decreto Supremo 27172:
a) A los tres (3) días de su recepción, en casos de interrupción del servicio o de alteraciones graves derivadas de su prestación; o
b) A los quince (15) días en los demás casos.
La Entidad Certificadora Pública se pronunciará por la procedencia o improcedencia de la reclamación, dejando constancia escrita de su decisión. Si decide la procedencia de la reclamación adoptará todas las medidas necesarias para devolver los importes indebidamente cobrados, reparar o reponer cuando corresponda, y en general asumirá toda medida destinada a evitar perjuicios a los usuarios. La decisión deberá cumplirse en un plazo máximo de veinte (20) días.
La Entidad Certificadora Pública comunicará al reclamante/usuario la resolución que decide la reclamación dentro de los cinco (5) días siguientes a su pronunciamiento, informando al reclamante, en caso de ser improcedente su reclamación, sobre su derecho a presentarla en la correspondiente instancia.

Por otro lado, se establece que la carga de la prueba será de la Entidad Certificadora Pública.

13.2.2.- RECLAMACIÓN ADMINISTRATIVA.-

Por otro lado, en cuanto al procedimiento de la Reclamación Administrativa se establece que si la Entidad Certificadora Pública declara improcedente la reclamación o no la resuelve dentro del plazo establecido al efecto, el usuario o un tercero por él, podrán presentarlo a la Autoridad competente en el plazo de quince (15) días.

El usuario presentará su reclamación de manera escrita o verbal, por cualquier medio de comunicación, acreditando que con anterioridad realizó la reclamación directa en la entidad o, en su defecto, expresando las razones por las que realiza su reclamación en esta instancia.

Asimismo, en esta etapa el usuario podrá acompañar las pruebas documentales de que intentare valerse y ofrecer las restantes; y la ATT registrará su Reclamación Administrativa.

14.- MEDIDAS PARA SALVAGUARDAR LA INVIOLABILIDAD DE LAS TELECOMUNICACIONES Y PROTECCION DE LA INFORMACION.-

De conformidad a lo señalado en el Art.56 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación y en el marco de lo establecido en la Constitución Política del Estado, la Entidad Certificadora Pública garantizará 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.

15.- CAMBIO O MODIFICACIONES EN LA LEY O REGLAMENTOS DE TELECOMUNICACIONES.-

Los presentes Términos y Condiciones se encuentran enmarcados en la Ley General de Telecomunicaciones y sus Reglamentos vigentes. Cualquier modificación futura a estas disposiciones legales será de aplicación inmediata en lo concerniente a los Términos y Condiciones.

VERSIONES

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

- nueva redacción sobre la generación del par de claves, en sección 5. REQUISITOS TÉCNICOS
- corrección de un error en el precio para persona jurídica (370 Bs) conforme a la escala tarifaria vigente
- corrección de un error en la promoción por número de certificados digitales en el sector público, conforme a la escala tarifaria vigente.
- Remplazo del término “hsm” por el término “token (hsm)”.
- ortografía: “prolongados”