T ÉRMINOS Y CONDICIONES DEL SERVICIO DE CERTIFICACIÓN DIGITAL

ADSIB-FD- RINT-002 Unidad de Gestión de Servicios

	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre:	Cesar Orlando Guerrero Carrillo	Rosario del Carmen Mamani Alegria Odelis Sheily Mendizabal Bazan	Bladimir Magne Molina
Cargo:	Profesional en Calidad de Servicios	Jefe de la Unidad de Gestión de Servicios Asesor Legal	Director Ejecutivo
Firma:	Firmado Digitalmente	Firmado Digitalmente	Firmado Digitalmente
Fecha:	11/01/2020	11/01/2020	11/01/2020

T ÉRMINOS Y CONDICIONES DEL SERVICIO DE CERTIFICACIÓN DIGITAL

Contenido

TÉRMINOS Y CONDICIONES DEL SERVICIO DE CERTIFICACIÓN DIGITAL

1 Introducción

Los Términos y Condiciones para la Provisión de la Certificación Digital contemplan 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 Descripción 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.

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.

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 dos destinatarios: 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 custodia del firmante y es la utilizada para realizar firmas. La clave pública es la que se divulga y es utilizada por los terceros aceptantes para verificar la validez de una firma digital.

3 Alcance o cobertura de la prestación del servicio.-

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

- Personas naturales
- Personas jurídicas

La Ley N° 164, Ley General de Telecomunicaciones, 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 medios electrónicos:

- Los actos propios del derecho de familia.
- Los actos en que la ley requiera la concurrencia personal física de alguna de las partes.
- 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 expreso de partes.

4 Modalidades de prestación del servicio

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 dos tipos de certificados conforme a lo establecido en la normativa técnica de la ATT. Los tipos de certificados son:

a) Persona jurídica.- certificado expedido únicamente a personas bajo relación jurídica con una persona jurídica, a solicitud expresa del representante legal de dicha persona.
b) Persona natural.- certificado expedido a cualquier ciudadana o ciudadano mayor de edad y hábil por derecho para realizar actos jurídicamente válidos.

Independientemente del tipo, se pueden emitir certificados por tipo de uso:

a) Firma Digital Simple
b) Firma Digital Automática

Así mismo, según el medio donde se genere el par de claves, el certificado podrá tener alguno de los siguientes niveles de seguridad:

a) Nivel de seguridad alto: el par de claves se genera en un dispositivo criptográfico por hardware
b) Nivel de seguridad normal: el par de claves se genera en un dispositivo criptográfico por software

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) con un máximo de tres reemisiones de certificado digital, 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 revocatoria de un certificado**
    3. Solicitar la renovación de un certificado sin cambio de clave privada**
    4. Reportar incidentes con respecto a sus certificados
    5. Acceder al servicio de soporte técnico en línea, en los horarios establecidos por la ECP y según sus procedimientos
    6. Solicitar la reemisión de certificados por pérdida o cambio del dispositivo criptográfico (HSM, token o smartcard) 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 renovación, revocatoria o reemisión 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, 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 criptográfico (token o HSM) para la preservación de las claves pública y privada y certificado del usuario.

**La renovación, revocación y/o reemisión de certificados se realizarán conforme a los procedimientos establecidos por la ECP.

El usuario es responsable de la generación del par de claves en dispositivos criptográficos seguros. En caso de usarse dispositivos criptográficos basados en hardware, los mismos deben estar homologados por la ATT, que dispone de la lista de todos los dispositivos homologados en su sitio web.

5 Definiciones

Definiciones aplicadas para el presente el documento:

- **Certificado digital:** Es un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.
- **Par de claves:** Es el conjunto de la clave privada y la clave pública. Las dos claves se generan 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

- **Clave privada:** Conjunto de caracteres alfanuméricos generados mediante un sistema de cifrado que contiene datos únicos que el signatario emplea en la generación de una firma electrónica o digital sobre un mensaje electrónico de datos o documento digital.
- **Clave pública:** Conjunto de caracteres de conocimiento público, generados mediante el mismo sistema de cifrado de la clave privada; contiene datos únicos que permiten verificar la firma digital del signatario en el Certificado Digital.
- **Firma digital:** Es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital.
- **Firma Digital Automática:** Firma digital generada por un sistema informático, donde el titular del certificado digital delega su uso para tareas definidas en éste.
- **Nivel de seguridad:** En caso de que el par de claves sea generado por un dispositivo criptográfico basado en hardware, el certificado tendrá nivel de seguridad alto, en caso de que el par de claves sea generado por software tendrá nivel de seguridad normal.
- **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 los datos 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.
- **Módulo criptográfico basado en token:** Es un dispositivo de seguridad basado en hardware (Por ejemplo HSM, token o smartcard) que genera, almacena y protege claves criptográficas. Los dispositivos criptográficos deberán estar homologados por la ATT.
- **Usuario titular:** El usuario titular para el servicio de certificación digital de la ADSIB es la persona física poseedora del certificado digital y en consecuencia, tendrá los derechos de revocación, reemisión y renovación sobre el certificado. El certificado puede ser de persona natural o persona jurídica.
- **Usuario corporativo:** Las cuentas corporativas son las entidades que establecen un vínculo contractual o de convenio con la ECP para adquirir certificados digitales para su personal interno.
- **Lista de certificados revocados:** Una lista de revocatoria de certificados (en inglés Certificate Revocation List - CRL) es un archivo digital que contiene una lista de certificados revocados. La revocatoria de un certificado corresponde a revocar su validez, por algún motivo, antes de su fecha de expiración. La lista de revocatoria de certificados está firmada por una autoridad reconocida dentro de la infraestructura de clave pública. En el caso de la Entidad Certificadora Pública -

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

6 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:

- El usuario deberá generar una cuenta de usuario y una contraseña para acceder y llenar el formulario de solicitud.
- En función al nivel de seguridad del certificado a solicitar contar con:
  - Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smart cards que cumplan con el estándar FIPS 140-2). Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web. En el dispositivo de seguridad es donde se generarán el par de claves para realizar la solicitud.
  - Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 845/2018, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos.
- El usuario deberá crear su par de claves y enviar su clave pública a través de mecanismos que garanticen que el procedimiento es seguro. Si el usuario no supiera realizar la operación, los Oficiales de Registro le proporcionarán el soporte necesario, mismo que podrá ser realizado en cualquier Agencia de Registro autorizada siempre y cuando se utilice un Token o SmartCard como medio de almacenamiento del Certificado; en caso de Certificados almacenados en un contenedor de Software o en un HSM, la responsabilidad de la generación del par de claves es del usuario solicitante.

La ADSIB como ECP, las Agencias de Registro y los Oficiales de Registro autorizados harán 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 esté 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 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 la Lista de Certificados Revocados (CRL), el servicio OCSP, así como brindar los mecanismos necesarios para la renovación, reemisión y revocación de los certificados firmados. 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.

7 Habilitación y plazo para la provisión del servicio

Las Agencias de Registro, una vez haya validado y verificado los requisitos sean los correctos y que el usuario haya registrado en el sistema el comprobante de pago, procederá a enviar la solicitud de firma de Certificado a la ADSIB – ECP, quien tendrá un plazo máximo de 72 horas para la emisión de los certificados una vez recibida la solicitud CSR de la agencia de registro, y enviará a la respectiva Agencia de Registro el certificado digital firmado, salvo en caso fortuito, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante.

8 Tarifas

La estructura tarifaría del servicio de certificación digital se encuentra publicada en la página: https://firmdigital.bo/

8.1 Obtención, revocación, vigencia y conservación del certificado digital De conformidad a lo señalado en el Artículos 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:

8.2 Obtención del certificado digital

Los certificados emitidos por la Entidad Certificadora Pública - ADSIB tienen periodos de vigencia según el tipo de Certificado, dicho periodo está especificado en el propio certificado y está definido en los documentos de Políticas de Certificación de cada tipo de certificado.

Independientemente del tipo, se pueden emitir certificados por tipo de uso:

- **Firma Digital Simple:** cuando el usuario titular administra el certificado para cada una de las firmas a realizar

Así mismo, según el medio donde se genere el par de claves, el certificado podrá tener alguno de los siguientes niveles de seguridad:

- **Nivel de seguridad alto:** el par de claves se genera en un dispositivo criptográfico por hardware
- **Nivel de seguridad normal:** el par de claves se genera en un dispositivo criptográfico por software

La solicitud de un certificado digital puede ser realizado por cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

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.

8.2.1 Los requisitos para personas naturales son:

a) Documento de Identidad vigente (Carnet de identidad o extranjero, según corresponda).
b) Última factura de un servicio básico (Luz o agua) que permita verificar su dirección actual.
c) Registro y solicitud de un certificado digital de tipo persona natural en el sistema de la Agencia de registro.
d) En función al nivel de seguridad del certificado a solicitar contar con:
   - Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smart cards que cumplan con el estándar FIPS 140-2). Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web. En el dispositivo de seguridad es donde se generarán el par de claves para realizar la solicitud.
   - Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 845/2018, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos.

8.2.2 Los requisitos para personas jurídicas son:

a) Documento de Identidad vigente (carnet de identidad o de Extranjero, según corresponda).
b) Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición del NIT (Número de Identificación Tributaria) del solicitante vigente.
c) Nota de Autorización original para el solicitante por la Máxima Autoridad Ejecutiva o el Representante Legal de la Empresa.
d) Registro y solicitud de un certificado digital de tipo persona jurídica en el sistema de la Agencia de registro.
e) En función al nivel de seguridad del certificado a solicitar contar con:
   1. Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smart cards que cumplan con el estándar FIPS 140-2). Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web. En el dispositivo de seguridad es donde se generarán el par de claves para realizar la solicitud.
   2. Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 845/2018, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en el contenedor de software donde realiza la solicitud, y el

8.3 Renovación de un certificado digital

Para ese procedimiento el usuario titular deberá acceder al Sistema de la Agencia de Registro con las credenciales de usuario que obtuvo al momento de crear la cuenta y decidir si desea generar un nuevo par de claves o conservar el par de claves para la renovación del Certificado. Se puede realizar la solicitud de renovación hasta en tres (3) oportunidades, siempre y cuando el certificado este vigente. Si se ha excedido el periodo de vigencia del certificado, se debe realizar una solicitud de un nuevo certificado. La cuarta renovación consecutiva también será tratada como una solicitud nueva, necesitando cumplir todos los procedimientos establecidos por la ECP.

8.4 Reemisión de un certificado digital

La solicitud de reemisión de certificado digital debe aplicarse a un certificado revocado, y podrá generarse un nuevo par de claves para el nuevo certificado digital.

Al enviar el archivo CSR de reemisión a la Entidad Certificadora Pública, el Sistema de Agencia de Registro especificará el periodo de validez correspondiente en base al tiempo restante del certificado digital inicial.

Cuando un usuario con Certificado Digital con Token solicite una reemisión, puede solicitar también la reposición del token. Para ello debe apersonarse a una Agencia de registro para la entrega del dispositivo, previa cancelación del costo de reposición del dispositivo y proceder según lo establecido para una reemisión de certificado digital.

Se podrá realizar una reemisión con cambio de titular; para ello, es necesario que el nuevo titular presente todos los requisitos necesarios y siga los procedimientos como si de una nueva solicitud se tratase, incluyendo la presentación de los requisitos y firma de un nuevo **contrato de adhesión**.

En caso que se solicite una reemisión sin cambio de titular también será necesario firmar un nuevo contrato de adhesión.

8.5 Revocación de un certificado digital

I. Un certificado digital podrá ser revocado debido a las siguientes causas:
   a) A solicitud del titular debido a robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
   b) Emisión defectuosa de un certificado debido a que:
      1. No se ha cumplido un requisito material para la emisión del certificado

3. Identificación de un error de entrada de datos u otro error de proceso.

c) No se firme el contrato de adhesión al servicio en el plazo establecido posterior a su emisión.
d) La información contenida en el certificado o utilizada para realizar la solicitud cambió.
e) El certificado de la Entidad Certificadora Pública ADSIB o Entidad Certificadora Raíz ATT es revocado.
f) Otros fundamentos técnicos y/o legales, de interés nacional, por resguardo de la seguridad del Estado Plurinacional de Bolivia o de interés del pueblo boliviano, mediante Resolución Administrativa de su Máxima Autoridad Ejecutiva.

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

8.6 Vigencia de los certificados

La vigencia de los certificados digitales emitidos no será superior a un (1) año.

8.7 Conservación del certificado digital

La conservación del certificado digital es de entera responsabilidad del usuario titular, y debe ser almacenado adecuadamente en el dispositivo criptográfico para el que fue emitido según la generación de su par de claves (hardware o software).

9 Derechos y obligaciones de las usuarias y usuarios en relación al servicio

9.1 Titular del certificado digital

De acuerdo a lo establecido en el Artículo 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 Artículo 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

c) El documento con firma digital le otorga al titular del certificado 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 o a alguna Agencia de Registro autorizada 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 del certificado y su revocatoria, son de exclusiva responsabilidad del usuario.

9.3 Derechos del titular del certificado

De conformidad a lo señalado en el Artículo 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 Artículo 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:

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 revocación del certificado.

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 Artículo 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 Artículo 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 Artículos 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 Artículo 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

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 Artículo 59 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, la 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.
d) 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.
e) 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.
f) 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.
g) Atender las solicitudes y las reclamaciones realizadas por las usuarias o los usuarios.
h) Informar oportunamente la desconexión o cortes programados de los servicios.
i) 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.
j) 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.
k) Proveer servicios que no causen daños a la salud y al medio ambiente.
l) Cumplir las instrucciones y planes que se emitan en casos de emergencia y seguridad del Estado.
m) Actualizar periódicamente su plataforma tecnológica y los procesos de atención a las usuarias y los usuarios.
n) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

11.3 Obligaciones de la entidad certificadora publica

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 Artículo 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, revocación, 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 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 administre

12 Derechos y obligaciones de la entidad certificadora pública y ante terceros que confían

De conformidad a lo establecido en el Artículo 44 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, la Responsabilidad 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 Atención de consultas, reclamaciones y emergencias y/o servicios de información y asistencia

13.1 Atención de consultas y emergencias y/o servicios de información

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 https://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

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 Artículo 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 protección de la información

De conformidad a lo señalado en el Artículo 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.

16 VERSIONES

Versión	Fecha de Revisión	Descripción del cambio	Revisado por	Aprobado por	RES. ADM.	Fecha de aprobación
1.0	12/01/2015	Elaboración del documento considerando la elaboración de Políticas separadas por tipo de certificado	Sylvain Lesage	Nicolas Laguna	RA ADSIB No. 04/2015	12/01/2015
2	08/11/2018	Elaboración del documento considerando la elaboración de Políticas separadas por tipo de certificado	Reynaldo Alonzo Vera Arias	María Jannett Ibañez	ADSIB/RA/0074/2018	31/12/2018

		Persona Natural)				
2.1	30/05/2019	Ajustes al documento en base a la nueva reglamentación según Resolución ATT-DJ-RA TL LP 209/2019 emitida por la ATT	Reynaldo Alonzo Vera Arias	José Luis Machicado	ADSIB/RA/0026/2019	24/06/2019
2.2	10/2020	Ajustes al documento en el marco de reglamentación aprobada mediante Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 209/2019, y las recomendaciones realizadas por la ATT	Reynaldo Alonzo Vera Arias	José Luis Machicado		