POLÍTICAS DE CERTIFICACIÓN

ADSIB-FD-POLT-015 Unidad de Gestión de Servicios

	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre:	Miguel Ángel Choque Quispe	Reynaldo Alonzo Vera Arias	José Luis Machicado Moya
Cargo:	Profesional en Calidad de Servicios	Jefe de la Unidad de Gestión de Servicios	Director Ejecutivo a.i.
Firma:	Firmado Digitalmente	Firmado Digitalmente	Firmado Digitalmente
Fecha:			

POLÍTICAS DE CERTIFICACIÓN

Contenido

POLÍTICAS DE CERTIFICACIÓN

1. Introducción.

1.1. Descripción General.

El presente documento presenta la Política de Certificación Digital para los Certificados Digitales emitidos por la Entidad Certificadora Pública ADSIB, y define los términos que rigen el servicio en el marco de la Ley N.º 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, Decretos Supremos Nº 1793 y Decreto Supremo Nº 3527 que aprueban el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación y modificaciones, respectivamente.

La Política de Certificación es un instrumento que establece las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, renovación y revocación de los certificados.

En este documento está sujeto al cumplimiento de la Declaración de Prácticas de Certificación de la Entidad Certificadora Pública - ADSIB.

Las Políticas de certificación son desarrolladas y aprobadas por la Entidad Certificadora Pública - ADSIB, y posteriormente presentadas a la ATT.

Este documento fue desarrollado de acuerdo con las Resoluciones Administrativas Regulatorias RAR ATT-DJ-RAR-TL LP 202/2019, RAR ATT-DJ-RAR-TL LP 209/2019, RAR ATT-DJ-RAR-TL LP 272/2017, emitidas por el ente regulador ATT.

1.1.1. Propósito.

El certificado digital cumple los siguientes propósitos:

a) Acredita la identidad del titular del Certificado Digital
b) Proporciona legitimidad del Certificado en base a los servicios de verificación del estado de certificados.
c) Vincula un documento digital o mensaje electrónico de datos firmado digitalmente con el usuario titular.
d) Garantiza la integridad del documento digital o mensaje electrónico con firma digital.

1.1.2. Descripción de la Entidad Certificadora.

La Entidad Certificadora Pública ADSIB se encuentra autorizada por la ATT para brindar el servicio de certificación digital y para ello tiene instalada una infraestructura que brinda seguridad y garantiza la calidad del servicio.

Las oficinas de la Entidad Certificadora Pública ADSIB se encuentran ubicadas en la Calle Jaime Mendoza No 981 Zona San Miguel - La Paz Bolivia, así mismo, las dependencias de su Centro de Procesamiento de Datos se encuentran en instalaciones del Edifico de la Vicepresidencia, en la parte del subsuelo.

La ADSIB como Entidad Certificadora Pública tiene las siguientes funciones:

- Emitir, validar, renovar, revocar, denegar o reemitir los certificados digitales.
- Facilitar servicios de generación de firmas digitales.
- Validar la firma digital realizada con certificados digitales y la identidad del usuario titular.
- Validar y comprobar, cuando corresponda, la identidad y existencia real del usuario titular.
- Reconocer y validar los certificados digitales emitidos en el exterior, siempre y cuando se establezcan los convenios respectivos para tal fin.
- Otras funciones relacionadas con la prestación del servicio de Certificación Digital.

1.2. Identificación del documento.

1.2.1. Nombre.

El presente documento lleva como título “Políticas de Certificación”.

1.2.2. Versión.

El documento se encuentra en su versión 2.1.

1.2.3. Fecha de elaboración.

El documento fue actualizado en octubre de 2020.

1.2.4. Fecha de actualización.

Se considera como fecha de actualización a la fecha en la que el documento entre en vigencia a partir de su respectiva aprobación.

1.2.5. Localización.

La presente política se la puede localizar en: https://www.firmadigital.bo/politica.pdf

1.2.6. Identificador de Objeto.

Este documento tiene el siguiente Identificador de Objeto (OID): 2.16.68.0.0.0.1.14.1.2.0.1.0.0

1.3. Infraestructura Nacional de Certificación Digital del Estado.

La Infraestructura Nacional de Certificación Digital, está establecida en el Decreto Supremo N.º 1793, el cual menciona los siguientes niveles:

- Primer Nivel: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes: Entidad Certificadora Raíz.
- Segundo Nivel: Entidades Certificadoras.
- Tercer Nivel: Agencia de Registro.
- Cuarto nivel: Signatarios.

En el documento "Declaración de Prácticas de Certificación" se detalla más información sobre cada nivel de la INCD.

1.4. Uso de los certificados.

1.4.1. Usos apropiados de los certificados

Los certificados digitales emitidos por la ADSIB en calidad de Entidad Certificadora Pública podrán usarse en los términos establecidos en la normativa vigente relacionado a la Certificación Digital, con las condiciones adicionales establecidas en la Declaración de Prácticas de Certificación, la presente Política de Certificación y cualquier otra normativa vigente que así lo indique.

Los certificados digitales emitidos bajo esta Política de Certificación, pueden ser utilizados bajo los siguientes propósitos:

- Firma de documentos digitales.
- Protección de Correo Electrónico.
- Autenticación en sitio web.
- Firma de código informático.

Nota: Se puede encontrar más información sobre este aspecto en los Anexos del presente documento.

1.4.2. Usos no autorizados de los certificados.

No se permite el uso de certificados digitales en los siguientes casos: Que vaya en contra a la legislación vigente, resoluciones establecidas por la ATT como ente regulador, las que no estén establecidas en la "Declaración de Prácticas de Certificación", la "Política de Certificación" y cualquier otra restricción establecida por normativa vigente.

No se autoriza el uso de certificados digitales para firma de CRL u OCSP.

Nota: Se puede encontrar más información sobre este aspecto en los Anexos del presente documento.

Todo uso no autorizado o malintencionado que concluya en un proceso por daños y perjuicios, solamente surten efecto entre los usuarios intervinientes del acto o negocio jurídico. La Entidad Certificadora Pública ADSIB no opera como mediadora, ni entidad sancionadora en ningún caso; únicamente será la entidad encargada de facilitar información y ofrecer servicios que permitan validar la información de los certificados y la integridad de los documentos firmados digitalmente.

1.5. Administración de la Política de Certificación.

La responsabilidad de la administración de esta "Política de Certificación" corresponde a la ADSIB como Entidad Certificadora Pública.

Las revisiones de esta Política de Certificación deberán ser enviadas a la ATT.

1.6. Definiciones y abreviaturas.

1.1.1. Abreviaturas

- **ADSIB:** Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- **AR:** Agencia de Registro.
- **ATT:** Autoridad de Regulación y Fiscalización de Transportes y Telecomunicaciones.
- **CP:** (Certificate Policy) Política de Certificación.
- **CPS:** (Certification Practice Statement) Declaración de Prácticas de Certificación.
- **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
- **CSR:** (Solicitud de Firma de Certificado) Es una petición de certificado digital que se envía a la ECA conteniendo la información para la emisión del certificado digital una vez realizadas las comprobaciones que correspondan.
- **DPC:** Declaración de Prácticas de Certificación.
- **EC:** Entidad Certificadora.
- **ECA:** Entidad Certificadora Autorizada.
- **ECR:** Entidad Certificadora Raíz.
- **ECP:** Entidad Certificadora Pública
- **HSM:** (Hardware Security Module) Modulo de Hardware de Seguridad[1].
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **INCD:** Infraestructura Nacional de Certificación Digital.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.
- **NIT:** Número de Identificación Tributaria emitido por el Servicio de Impuestos Nacionales.
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RFC:** (Request For Comments[2]) Requerimiento de Comentarios.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **SEGIP:** Servicio General de Identificación Personal
- **SERECI:** Servicio de Registro Cívico
- **SHA:** (Secure Hash Algorithm) Algoritmo de Hash Seguro.
- **TIC:** Tecnologías de Información y Comunicación.

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

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

- **URI:** Identificador Uniforme de Recursos
- **UTF:** (Unicode Transformation Format) Formato de codificación de caracteres.

1.1.2. Definiciones

- **Autenticación:** Proceso técnico de verificación por el cual se garantiza la identidad del signatario en un mensaje electrónico de datos o documento digital, que contenga firma digital.
- **Certificado Digital:** Es un archivo digital firmado digitalmente por una entidad certificadora autorizada que incluye datos que permiten identificar al titular del certificado, a la entidad certificadora que lo emitió, el periodo de vigencia e información necesaria para verificar la firma 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 para cumplir la operación.
- **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 la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración. Este tipo de Firma tiene validez legal desde el año 2011.
- **Firma Digital Automática:** Firma digital generada en forma desatendida o automática por un sistema informático, el titular del certificado digital delega el uso de su certificado para tareas definidas.
- **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 está firmada con la clave privada del solicitante para certificar que la solicitud es auténtica.
- **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 está 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 hardware:** 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 Entidad Certificadora Pública 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:** Entidades públicas o privadas que establecen un vínculo contractual o de convenio con la Entidad Certificadora Pública ADSIB, para las operaciones sobre certificados digitales de su personal interno se les habilitará cuentas corporativas.
- **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 ADSIB, la lista de revocatoria está firmada con un par de claves y un certificado dedicados de la ADSIB.
- **Emisión de Certificados:** La Entidad Certificadora Pública ADSIB emitirá los certificados que se soliciten a través de una Agencia de Registro autorizada mediante un CSR; las solicitudes son remitidas una vez que el Oficial de Registro de la Agencia de Registro haya comprobado el cumplimiento de los requisitos.
- **Repositorio:** Es el lugar en el sitio web donde se publican los documentos relacionados al servicio de certificación digital, así como los servicios relacionados que se encargan de comprobar el estado de los certificados

2. Publicación de información y del repositorio.

2.1. Repositorio.

La Entidad Certificadora Pública ADSIB mantiene un repositorio de la documentación en el sitio web:

https://firmadigital.bo/

La Entidad Certificadora Pública - ADSIB es responsable de mantener su repositorio actualizado y con todos los criterios de seguridad establecidos en las políticas de seguridad, así mismo, dicho repositorio es de acceso público y no contiene información confidencial o privada. El repositorio está disponible durante las 24 horas los 7 días de la semana y en caso de presentarse algún incidente en el sitio web, la ADSIB, aplicará el plan de contingencias, gestión de incidentes y continuidad del servicio para restablecer nuevamente el sitio web y se encuentre disponible.

Las listas de los certificados emitidos a usuarios finales no se hacen públicas en ningún repositorio.

2.2. Repositorio CRL.

El Repositorio CRL se encuentra en:

https://firmadigital.bo/firmadigital_bo.crl

2.3. Servicio OCSP.

El servicio de consulta OCSP se encuentra en:

https://www.firmadigital.bo/ocsp

2.4. Términos y condiciones.

La prestación del servicio de Certificación Digital, se encuentra sujeto y sometido al cumplimiento de las Políticas de Certificación de la Entidad Certificadora Pública ADSIB que para fines del servicio se constituyen como sus Términos y Condiciones.

2.5. Políticas de Certificación.

El presente documento “Política de Certificación” se encuentra en:

https://firmadigital.bo/cpadsib.pdf

2.6. Declaración de prácticas.

La Declaración de Prácticas de Certificación se encuentran en:

https://firmadigital.bo/ecpadsib.pdf

2.7. Publicación.

La Entidad Certificadora Pública ADSIB proporciona acceso público a la siguiente información:

- Los certificados digitales de la Entidad Certificadora Pública (ADSIB) y de la Entidad Certificadora Raíz (ATT) que constituyen la cadena de confianza de la INCD.
- La Lista de Certificados Revocados (CRL) y los servicios de validación de certificados en línea (OCSP).
- Los documentos públicos de la Entidad Certificadora Pública – ADSIB, que están compuestos por el presente documento y la Declaración de Prácticas de Certificación. La Entidad Certificadora Pública ADSIB mantiene un histórico de las versiones publicadas.
- Cualquier otra información relacionada con el servicio de Certificación Digital (Precios de cada tipo de certificado, manuales de usuario y otra información de interés).

2.8. Frecuencia de actualización.

La Entidad Certificadora Pública ADSIB realiza una constante actualización de los repositorios públicos. Por otra parte, y por ser una información crítica, la actualización del repositorio CRL se realiza cada 15 minutos y el servicio OCSP se mantiene en línea.

2.9. Controles de acceso al repositorio.

La Entidad Certificadora Pública ADSIB no restringe el acceso a las consultas del repositorio, sin embargo, para proteger la integridad y autenticidad de la información publicada se cuenta con controles que impiden a personas no autorizadas modificar la información (incluir, actualizar o eliminar datos).

3. Identificación y Autenticación.

Conforme al estándar X.500, todos los Certificados Digitales requieren un nombre distinguido único. Por lo mismo, no serán admitidos o procesados por la Entidad Certificadora Pública ADSIB los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el usuario titular. En caso de que el titular pertenezca a una población indígena serán considerados los nombres que figuran en la cédula de identidad.

Se garantiza que los nombres de los Certificados Digitales son únicos para cada titular porque contienen el atributo de número de documento de identidad y número de complemento asignados por el SEGIP, y que permiten distinguir entre 2 identidades cuando existan problemas de duplicidad de nombres (homónimos).

Para demostrar la identidad del usuario solicitante se solicitará lo siguiente:

- Documento de identidad original y vigente para contrastar los datos con el SEGIP.
- Toma de Fotografía para verificación visual con documento de identidad.
- Captura de huella dactilar, para verificar identidad del usuario solicitante.

En el documento “Declaración de Prácticas de Certificación” se detalla información sobre la identificación y autenticación de los titulares de los certificados.

3.1. Formato del Nombre distinguido.

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos por la ADSIB utilizan codificación UTF-8 para todos los atributos, según la RFC 5280 (“Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile”).

3.2. Validación de la identidad inicial.

Las agencias de registro realizan la validación y autenticación de la identidad de los usuarios solicitantes de Certificados Digitales mediante servicios de interoperabilidad establecidos con el SEGIP. Se pueden

adicionar validaciones adicionales a través de cualquier otro mecanismo que se vea por conveniente.

3.3. Identificación y autenticación para solicitudes de revocación.

Se realizará la verificación de la identidad del titular cuando la solicitud de revocación se realice a través de un correo electrónico, una llamada telefónica o presencialmente en alguna Agencia de Registro. Se deberá seguir los siguientes procedimientos en cada caso:

a) En caso de recibir solicitudes de revocación vía correo electrónico o llamada telefónica, se confirmará la identidad de la persona con algunas preguntas y además se realizará una llamada telefónica para verificar la autenticidad de la solicitud; en caso que el usuario no conteste, se intentará hasta tres veces. Si no se obtiene respuesta al tercer intento, se realizará la revocación y se registrará este hecho junto a la solicitud.
b) En caso de recibir una solicitud de revocación presencial, los Oficiales de Registro podrán colaborar en el proceso de solicitud de revocación desde la cuenta del usuario titular, y una vez registrada la solicitud, el Oficial procederá a validarla sin necesidad de realizar la verificación vía llamada telefónica.

Los usuarios corporativos pueden realizar la revocación de los certificados emitidos para los usuarios titulares registrados desde su propia cuenta corporativa, sin realizar verificación alguna.

3.4. Identificación y autenticación de las solicitudes de renovación de certificado.

Las solicitudes de renovación son autenticadas por el sistema de Agencia de Registro. Se podrá autenticar una solicitud de renovación de acuerdo a las siguientes formas:

a) El usuario titular debe acceder al Sistema de Agencia de Registro con las credenciales de usuario que obtuvo al momento de crear la cuenta.
b) Las renovaciones se podrán realizar únicamente mientras el certificado inicial se encuentre vigente. Si el certificado inicial ha superado su tiempo de vigencia, se deberá realizar la solicitud como una nueva emisión de Certificado Digital.
c) Los Oficiales de Registro autorizados de las agencias de registro de la Entidad Certificadora Pública ADSIB pueden solicitar la renovación del certificado digital de un usuario titular, autenticando la respectiva identidad de la persona a la presentación de los respectivos requisitos según Perfil de Certificado.

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

4.1. Requisitos para la obtención de certificado digital.

Los requisitos para la obtención de un Certificado Digital son:

- Documento de Identidad vigente (carnet de identidad o de Extranjero, según corresponda).
- Registro y solicitud de un certificado digital en el sistema de la Agencia de registro.

Nota: Según el tipo de Certificado digital solicitado, existen requisitos adicionales que se encuentran descritos en los Anexos del presente documento.

4.2. Solicitud del certificado.

Para solicitar un certificado digital, el usuario solicitante debe ser mayor de 18 años. Los titulares pueden obtener más de un Certificado Digital al mismo tiempo.

La solicitud de un Certificado Digital, se inicia desde el sistema de Agencia de Registro, siguiendo los pasos indicados en el mismo. Para completar la solicitud, el usuario solicitante debe presentar los requisitos establecidos según el Perfil de Certificado solicitado; y finalmente se procederá a realizar la captura de la foto. En caso de ser necesario, el usuario solicitante podrá apersonarse a alguna Agencia de Registro para asesoramiento.

4.3. Generación del par de claves

Al momento de solicitar un Certificado Digital, se podrá definir el nivel de seguridad de acuerdo a la normativa vigente. Según el nivel de seguridad seleccionado, el solicitante podrá generar el par de claves de la siguiente forma:

- **Certificados digitales emitidos por dispositivo criptográfico basado en hardware:** El solicitante deberá generar el par de claves en un dispositivo basado en hardware que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente.
- **Certificados digitales emitidos por dispositivo criptográfico basado en software:** El solicitante deberá generar el par de claves, en un dispositivo criptográfico basado en Software que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente. La Entidad Certificadora Pública ADSIB pone a disposición de los solicitantes un software homologado por la ATT para la generación del par de claves, garantizando la confidencialidad de la información y proporcionando al usuario titular el contenedor PKCS#12.

Es obligatorio que la generación del par de claves sea realizada por el titular, de todas formas, de ser necesario, los Oficiales de Registro brindarán el apoyo necesario para la generación del par de claves a requerimiento del solicitante, no debiendo participar de manera directa por tratarse de una acción privada.

4.4. Procesamiento de la solicitud del Certificado.

La Agencia de Registro, debe realizar un proceso de validación de la identidad del solicitante, verificación de cumplimiento de requisitos y verificación del pago correspondiente. Una vez verificada la solicitud de emisión de certificado digital (CSR), debe ser firmada digitalmente y remitida a la Entidad Certificadora Pública ADSIB a través del Sistema de Agencia de Registro.

Cuando la Agencia de Registro, mediante algún Oficial de Registro, detecte que el usuario solicitante tiene algún impedimento para obtener su certificado digital, no deberá continuar con el proceso y deberá proceder a explicar al solicitante la causa del impedimento y las posibles soluciones.

Las solicitudes creadas se mantendrán en el sistema durante 15 días a la espera de pago o registro de foto y huella antes de pasar al estado EXPIRADO. Este estado indica que la solicitud será desestimada y será necesario comunicarse con la Agencia de Registro para volver a habilitarla. La habilitación implica que se generará un nuevo Código de Pago CPT si fuera necesario.

4.5. Emisión de certificados.

La Entidad Certificadora Pública ADSIB dispone de procedimientos internos para la ceremonia de Firma Digital de los certificados que son estrictamente aplicados a las solicitudes CSR aprobadas y enviadas por cada Agencia de Registro.

La ADSIB, dando cumplimiento a la normativa vigente, tendrá un plazo máximo de 72 horas para la emisión de los certificados una vez recibida la solicitud CSR de la Agencia de Registro, salvo en caso fortuito, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante.

Una vez emitido un Certificado Digital, se lo remitirá al sistema de la respectiva Agencia de Registro donde se realizó el registro de la solicitud. El sistema de Agencia de Registro notificará al usuario titular poseedor de la clave privada que ya puede descargar su certificado correspondiente.

4.6. Aceptación del certificado.

Luego de descargar el certificado digital, el usuario titular debe firmar digitalmente el contrato de adhesión al servicio. Para ello tiene un plazo máximo de 120 horas a partir de la emisión del certificado; en caso de no firmar el contrato de adhesión en ese plazo el certificado digital será revocado de manera automática.

Es obligación del usuario titular realizar la importación del certificado digital a su respectivo medio de almacenamiento y proceder a firmar el contrato de adhesión; la no realización de estas acciones no afecta el cumplimiento del servicio.

Si un Certificado Digital es revocado por no firma de Contrato de Adhesión, la Entidad Certificadora Pública ADSIB podrá emitir un nuevo certificado sin costo alguno y sin afectar el conteo de reemisiones del certificado; siempre y cuando se realice la solicitud por parte del usuario titular. El nuevo certificado reemitido tendrá la vigencia del certificado inicial revocado y no se aplicará ningún tipo de costo adicional.

4.7. Usos del certificado.

Los certificados digitales podrán ser utilizados según lo estipulado en el documento “Declaración de Practicas de Certificación”, en la presente Política de Certificación y en cualquier otro documento complementario emitido por la Entidad Certificadora Pública ADSIB y o por la ATT.

Para determinar el uso del certificado es necesario comprobar el valor de la extensión “Key Usage” del certificado en cuestión.

4.8. Solicitud de renovación de certificados.

La renovación de certificados se la puede realizar **hasta en tres oportunidades consecutivas**, siempre y cuando dicha solicitud se realice mientras el certificado a ser renovado se encuentre vigente. En estos casos, la presencia física del usuario titular no es necesaria; pudiendo realizar todo el procedimiento en línea.

La vigencia del Certificado Digital obtenido a partir de una renovación, será de un (1) año computable a partir de la expiración del certificado digital inicial.

La solicitud de renovación del certificado digital será responsabilidad del usuario titular o usuario corporativo. La solicitud se podrá realizar a través del sistema de Agencia de Registro o desde la cuenta corporativa activa y vigente.

La renovación del Certificado Digital puede ser realizada únicamente durante los últimos treinta (30) días calendario del periodo de vigencia del certificado digital a renovarse. El titular del certificado digital tendrá conocimiento de las fechas disponibles para la renovación de su certificado digital, éstas serán notificadas al titular del certificado digital según el siguiente cronograma:

- Quince (15) días antes de la expiración del Certificado Digital
- Diez (10) días antes de la expiración del Certificado Digital
- Cinco (5) días antes de la expiración del Certificado Digital

En caso que la vigencia del certificado haya finalizado o el usuario titular haya realizado tres (3) renovaciones consecutivas, la solicitud de la 4ta renovación del certificado digital deberá ser procesada como una nueva solicitud.

Toda solicitud de renovación será validada por un Oficial de Registro antes de la emisión del Certificado Digital.

4.9. Solicitud de revocación de certificados.

El titular del certificado digital podrá realizar la solicitud de revocación de su certificado digital, mediante el sistema de Agencia de Registro. Para usuarios con cuentas corporativas la solicitud de revocación podrá ser realizada a través de su respectivo usuario administrador.

Se podrá solicitar la revocación de un certificado mientras se encuentre vigente, bajo las consideraciones establecidas en la Declaración de Prácticas de Certificación.

La revocación del certificado se hará efectiva en alguno de los siguientes casos:

- Después de realizar la verificación de la solicitud realizada mediante el sistema de la Agencia de Registro y/o por correo electrónico o llamada telefónica.
- Inmediatamente cuando se realice la solicitud ante un oficial de registro o mediante la cuenta corporativa.

4.10. Solicitud de reemisión de certificados.

La reemisión de un certificado digital al mismo usuario titular es un procedimiento que no requiere su presencia física, y las condiciones para realizarla son:

- El certificado del titular se encuentre revocado.
- La solicitud se realice en el periodo de vigencia del certificado digital inicial.

Se puede solicitar la reemisión de un certificado en los siguientes casos:

- No supere la tercera solicitud de reemisión en el periodo de vigencia del certificado, ya sea realizada por el titular o por la cuenta corporativa asociada al Certificado Digital.
- En caso de que se requiera el cambio de alguno de los datos del certificado (Ej. Cambio de usuario titular o cambio de razón social de la entidad).
- En caso de requerir el cambio de modo de uso del Certificado Digital: de firma automática a firma simple, o viceversa.
- En caso de requerir el cambio de nivel de seguridad del Certificado Digital: de nivel normal a nivel alto, o viceversa.
- Cuando se comprueba que alguno de los datos del certificado es incorrecto.
- Cuando se quiera reutilizar un certificado digital revocado que aún se encuentre en un periodo de vigencia válido, y el mismo no se haya reemitido previamente.

El usuario solicitante podrá generar un nuevo par de claves con la nueva solicitud. El periodo de validez del nuevo Certificado será por el lapso restante del periodo de validez del certificado inicial.

El titular del certificado digital puede solicitar la reemisión de su certificado desde el sistema de la Agencia de Registro. Los usuarios corporativos podrán solicitar la reemisión de certificados mediante la cuenta corporativa.

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**.

Así mismo, en caso de Certificados de Tipo Persona Natural que requieran de una reemisión con cambio de titular, se deberá presentar una nota formal firmada por el actual titular del Certificado o por algún funcionario con algún nivel superior al beneficiario, especificando la nueva persona beneficiaria por la reemisión.

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

4.11. Servicio de estado de los certificados.

La Entidad Certificadora Pública ADSIB posee dos (2) servicios de comprobación del estado de los certificados digitales.

Un método de comprobación es la lista de certificados digitales revocados (CRL), que tiene la finalidad de comprobar si un certificado ha sido revocado. Esta lista se actualiza periódicamente cada 15 minutos.

El segundo servicio de comprobación es el servicio OCSP, que está disponible en línea 24 horas al día, los 7 días de la semana.

4.12. Finalización de la suscripción.

La suscripción del servicio de certificación digital está asociada a la vigencia del certificado digital y finaliza cuando el certificado expira o se solicita su revocación.

4.13. Recuperación de la clave.

No aplica la recuperación de claves. Si el usuario pierde el acceso a su clave privada, se deberá proceder a la reemisión de un nuevo certificado generando un nuevo par de claves y debiendo cumplir los requisitos nombrados en este documento.

4.14. Depósito de claves y recuperación.

La Entidad Certificadora Pública ADSIB no realiza el depósito de claves.

5. Controles operacionales o de gestión.

5.1. Controles de seguridad física.

Los controles de seguridad se enmarcan en los lineamientos establecidos en la Resolución Administrativa RAR -DJ-RA TL LP 202/2018 emitida por la ATT.

La Entidad Certificadora Pública ADSIB tiene establecida su política de seguridad e identificados los controles necesarios para proteger sus áreas e instalaciones, sistemas, aplicaciones y servicios implementados de acuerdo a una gestión de riesgos.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre la Ubicación y construcción del Centro de Procesamiento de Datos, el acceso físico, la alimentación eléctrica y aire acondicionado, exposición al agua, la protección y prevención de incendios. También se detalla sobre el sistema de almacenamiento, las copias de seguridad y la eliminación de residuos.

5.2. Controles de procedimiento.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los roles de confianza, el número de personas requeridas por tarea y su respectiva identificación y autenticación

5.3. Controles de seguridad del personal.

En el documento "Declaración de Prácticas de Certificación" se detalla más información sobre requerimientos de antecedentes, calificación, experiencia y acreditación, así como los procedimientos de comprobación de antecedentes, la formación y frecuencia de actualización de la formación, la rotación de tareas, las sanciones por acciones no autorizadas y los requerimientos de contratación de personal, controles periódicos de cumplimiento, finalización de los contratos de la Entidad Certificadora Pública ADSIB.

5.4. Procedimientos de Control de Seguridad.

En el documento "Declaración de Prácticas de Certificación" se detalla más información sobre los tipos de eventos registrados, la frecuencia de procesamiento de logs, su periodo de retención y su respectiva protección. También se detalla sobre los procedimientos de copia de seguridad de los logs de auditoría, el sistema de recogida de información de auditoría, las notificaciones a quien provoque el evento. También se profundiza sobre el análisis de vulnerabilidades.

5.5. Archivo de información y registros.

La Entidad Certificadora Pública ADSIB garantiza o toma las acciones para que la información generada producto de la emisión de certificados digitales se almacene durante un periodo de tiempo apropiado.

La documentación confidencial generada por la Entidad Certificadora Pública ADSIB almacenada en soportes de información físicos y digitales contienen niveles de seguridad tanto físicos como lógicos.

Los archivos de registros se mantienen bajo estricto control de acceso y están sujetos a la inspección de auditores, que, para los fines de control, podrá ser verificado por la ATT.

En el documento "Declaración de Prácticas de Certificación" se detalla más información sobre los tipos de eventos e información, así como el periodo de retención para el archivo y el sistema de recogida de información para auditoría y los procedimientos para obtener y verificar información archivada.

5.6. Cambio de clave de la ADSIB.

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

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

5.7. Recuperación de la clave de la ADSIB.

La Entidad Certificadora Pública ADSIB tiene sus procedimientos para la recuperación de la clave privada

mediante los documentos “Planes y Procedimientos para la Continuidad del Servicio y Plan de Contingencias”.

5.8. Procedimientos para recuperación de desastres.

La Entidad Certificadora Pública ADSIB cuenta con un documento de Planes y Procedimientos para la Continuidad del Servicio y un Plan de Contingencias, mediante el cual se inicia un proceso de recuperación que cubre los datos, el hardware y el software crítico, y de esa manera iniciar nuevamente sus operaciones en caso de un desastre natural o causado por humanos. El documento Planes y Procedimientos para la Continuidad del Servicio es revisado periódicamente según cambios de los riesgos en el ambiente.

El Plan y Procedimiento para la Continuidad del Servicio está orientado a:

- Fallas/corrupción de recursos de computación;
- Compromiso de la integridad de la clave; y
- Desastres naturales y terminación.

La Dirección Ejecutiva deberá decidir sobre las acciones correctivas y comenzar las actividades necesarias para restablecer el sistema de certificación en el momento de presentarse un escenario de desastre. En el Plan y Procedimiento para la Continuidad del Servicio, se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre.

5.9. Cese de actividades de la Entidad Certificadora Pública ADSIB.

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

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los roles involucrados y los procedimientos para el cese de actividades

6. Controles de Seguridad Técnica.

6.1. Generación e instalación de par de claves

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre la generación del par de claves de la Entidad Certificadora Pública ADSIB, la gestión del par de claves, tamaño de claves, parámetros de generación de clave pública, hardware y software de generación de claves y los fines de uso de las claves.

6.2. Protección de la clave privada.

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

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los estándares

para los módulos criptográficos y sus respectivos controles multipersonales, custodia. También se detalla aspectos sobre copia de seguridad y el archivo de la clave privada, así como su introducción al módulo criptográfico. Por último, se menciona el método de activación de la clave privada, el método de destrucción de la clave privada y la clasificación de los módulos criptográficos.

6.3. Otros aspectos de la gestión del par de claves.

En el documento “Declaración de Prácticas de Certificación” se detalla los aspectos generales del par de claves, los periodos operativos de los certificados y el período de uso para el par de claves.

6.4. Datos de activación.

La Entidad Certificadora Pública ADSIB dispone de procedimientos para la generación de claves de activación de la clave privada del módulo criptográfico, basado en un procedimiento multipersonal, donde solo el personal autorizado posee las claves necesarias.

Las claves de acceso son confidenciales, personales e intransferibles.

6.5. Controles de seguridad informática.

La Entidad Certificadora Pública ADSIB tiene definida una serie de controles de seguridad aplicables a los equipos informáticos, tales como el uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y pruebas de seguridad.

El acceso a los sistemas de la Entidad Certificadora Pública ADSIB está restringido al personal autorizado según los roles asignados, bajo los procedimientos y controles establecidos.

6.6. Controles de seguridad del ciclo de vida.

El software de la Entidad Certificadora Pública ADSIB que utiliza la clave pública para la emisión de los certificados y el manejo del ciclo de vida ha sido desarrollado de acuerdo con los requerimientos de la Resolución Administrativa de la ATT-DJ-RA TL LP 202/2015.

El HSM utilizado por la Entidad Certificadora Pública ADSIB para firmar los Certificados cumple con los requerimientos FIPS 140-2. Los controles para el manejo de la seguridad se cumplen mediante una separación adecuada de roles mismos que definen el cumplimiento de los requerimientos descritos en la política de seguridad establecida, durante todo el ciclo de vida de las claves se tienen implementados controles de seguridad permitiendo instrumentar y auditar cada fase de los sistemas de la Entidad Certificadora Pública ADSIB.

Existen controles de seguridad para la operativa y el ciclo de vida de los sistemas de la entidad, incluyendo:

a) Registro y reporte de acceso físico
b) Registro y reporte de acceso lógico.
c) Procedimientos de actualización e implementación de sistemas

6.7. Controles de seguridad de la red.

El hardware y software para la infraestructura de clave pública de la Entidad Certificadora Pública ADSIB se mantienen "off-line" en un perímetro de seguridad física con alta seguridad, su acceso es restringido solo a personal autorizado y protegido mediante una combinación de procedimientos de accesos administrativos y físicos.

La infraestructura tecnológica necesaria para el procedimiento de Certificación Digital tiene implementado un sistema de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso.

6.8. Controles de los módulos criptográficos.

La Entidad Certificadora Pública ADSIB únicamente utiliza módulos criptográficos bajo el estándar FIPS 140-2.

6.9. Sincronización horaria.

El gabinete de la firma digital de la Entidad Certificadora Pública ADSIB que contiene la infraestructura de clave pública se mantiene "off-line", por lo que, la sincronización horaria en línea no se lleva a cabo.

7. Perfil de los Certificados, CRL y OCSP

7.1. Perfil de Certificado según tipo del certificado.

La ATT es la entidad encargada de definir y delimitar los Tipo s de Certificado a emitirse por las Entidades Certificadoras Autorizadas. Según el tipo de Certificado digital solicitado por cada usuario, el perfil varía en cumplimiento a normativa y reglamentación vigente.

Los perfiles de cada tipo de Certificado se encuentran especificados en reglamentación vigente, publicadas en el portal de la ATT, en su rol de Entidad Certificadora Raíz: https://ecrb.att.gob.bo/

Asi mismo, los perfiles de Certificados Digitales emitidos por la Entidad Certificadora Pública ADSIB, se encuentran publicados en el portal https://firmadigital.bo/

7.2. Perfil del Certificado de la Entidad Certificadora Raíz (ECR) ATT

El documento “Declaración de Prácticas de Certificación” detalla el perfil del Certificado de la Entidad Certificadora Raíz (ECR).

7.3. Perfil del Certificado de la Entidad Certificadora Pública ADSIB

El documento “Declaración de Prácticas de Certificación” detalla el perfil del Certificado de la Entidad Certificadora Pública ADSIB

7.4. Perfiles de la CRL

El documento “Declaración de Prácticas de Certificación” detalla el perfil del Certificado de la CRL y sus extensiones.

7.5. Perfiles de la OCSP

El documento “Declaración de Prácticas de Certificación” detalla el perfil del Certificado del OCSP y sus extensiones.

Las respuestas OCSP están firmadas digitalmente por la Entidad Certificadora Pública ADSIB en el marco de la Infraestructura de Clave Pública de Bolivia.

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

8. Administración Documental.

La responsabilidad de la administración de esta “Política de Certificación” corresponde a la Entidad Certificadora Pública ADSIB.

La publicación de las revisiones de esta “Política de Certificación” deberá ser presentada a la ATT.

8.1. Procedimiento para cambio de especificaciones.

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

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

8.2. Frecuencia de actualización

La revisión de la “Política de Certificación”, debe ser realizada al menos una vez al año, en base a la experiencia institucional en su aplicación, a la efectividad y oportunidad de sus procesos, su interrelación con otros sistemas, la dinámica administrativa y la situación de la normativa vigente. Producto de la revisión, se podrá actualizar el documento para que sea presentado a la ATT.

8.3. Procedimiento de Publicación y Notificaciones

La Entidad Certificadora Pública ADSIB presentará a la ATT las modificaciones aprobadas a la presente Política de Certificación, indicando, en cada caso las secciones y/o textos reemplazados junto con la publicación de la nueva versión.

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

En ningún caso la Entidad Certificadora Pública ADSIB será responsable por la pérdida de las comunicaciones enviadas al titular, cualquiera que sea el medio utilizado (correo electrónico, teléfono, otros.), pudiendo proceder a hacer efectivas las acciones informadas en ellas.

9. Otras cuestiones legales y de actividad.

9.1. Contrato de adhesión.

Los certificados emitidos por la Entidad Certificadora Pública ADSIB, están asociadas a la aceptación del Contrato de Adhesión del servicio, el mismo que está interpretado como un contrato condicional y sus características son:

- La eficacia o la resolución de un contrato puede estar subordinada a un acontecimiento futuro e incierto.
- Toda condición debe cumplirse de la manera que las partes han querido y entendido que se cumpla.

El contrato de adhesión debe firmarse digitalmente en el plazo establecido en el punto 4.6 del presente documento, caso contrario se procederá a la revocación automática del mismo.

9.2. Tarifas.

Las tarifas establecidas para la emisión de Certificados Digitales están enmarcadas bajo la normativa vigente, y serán publicadas en el sitio web de la Entidad Certificadora Pública ADSIB.

El acceso a la información relativa al estado de los certificados o de los certificados revocados es gratuito, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

9.2.1. Pago y Facturación.

Para realizar el pago del certificado digital, la Entidad Certificadora Pública ADSIB brinda diversas modalidades de pago, entre ellas, el más recomendado es el uso de la PPTE (Plataforma de Pagos de Tramites del Estado) a través de CPT (Código de Pago de Tramites), no siendo la única forma de pago disponible, todas las formas de pago adicionales se encuentran disponibles en el sitio web de la Entidad Certificadora Pública.

La emisión de la factura se realizará por medio electrónico a nombre y número de identificación tributaria definida por el titular, una vez emitido el certificado digital. En caso de cuentas corporativas l factura será emitida según coordinación realizada entre partes.

9.2.2. Reembolso.

La Entidad Certificadora Pública, realizará reembolsos a depósitos realizados por aquellos servicios no prestados, considerando los siguientes aspectos:

- Exista una solicitud formal por parte del depositante,
- No se hubiera emitido un certificado asociado al comprobante o CPT.

Los depósitos no utilizados durante diez (10) días calendario después de la fecha de depósito serán publicados en el sitio web de la Entidad Certificadora Pública ADSIB. Cada depósito permanecerá publicado por un lapso de 60 (sesenta) días calendario. Durante ese tiempo, el depositante podrá hacer uso del mismo o solicitar la restitución del monto. Pasado este lapso, todo depósito no utilizado pasará a favor de Entidad Certificadora Pública ADSIB.

9.3. Política de confidencialidad.

Toda la recopilación y uso de la información compilada por la Entidad Certificadora Pública ADSIB es realizada cumpliendo con la normativa vigente relacionada a certificación digital y protección de datos cumpliendo lo descrito en el artículo 56 del Decreto Supremo N.º 1793, basándose en las distinciones suministradas en el documento de Declaración de Prácticas de Certificación.

9.4. Ámbito de la Información confidencial.

La Entidad Certificadora Pública ADSIB considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial a no ser que exista una imposición legal.

9.5. Protección de Datos Personales.

A fin de garantizar los datos personales y la seguridad informática de los mismos se adoptan las siguientes previsiones:

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

La Entidad Certificadora Pública ADSIB adoptará las medidas de índole técnica y organizativa necesaria que garantice la seguridad de los datos personales y eviten su alteración, pérdida y tratamiento no autorizado que deberán ajustarse de conformidad con el estado de la tecnología.

El usuario que se adhiere al servicio de certificación digital de la Entidad Certificadora Pública ADSIB, acepta la publicación por parte de la ADSIB de la información contenida en su clave pública y el certificado firmado por la ADSIB.

9.6. Derechos y Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital.

9.6.1. Derechos y Obligaciones de la Entidad Certificadora Pública.

9.6.1.1. Derechos de la Entidad Certificadora Pública.

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 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.

9.6.1.2. Obligaciones de la Entidad Certificadora Pública.

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.
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 según 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) 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.

Para garantizar la publicidad, seguridad, integridad y eficacia del certificado digital, la Entidad Certificadora Pública tiene las siguientes obligaciones según 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 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.

9.6.1.3. 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 y la Resolución Administrativa RAR-DJ-RA TL LP 845/2018 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, 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 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 usuario titular o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

9.6.2. Derechos y Obligaciones de los Titulares del Certificado Digital.

Según 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 que hayan solicitado por sí y para sí una certificación que acredite su firma digital.

9.6.2.1. Responsabilidad del titular.

Según 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) El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
c) Asimismo, acorde a los procedimientos de la Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB a la brevedad posible y solicitar la revocación del certificado digital. 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.

9.6.2.2. 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.

9.6.2.3. 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:

1. 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;
h) No delegar el uso del Certificado a terceras personas ni a intermediarios, dado que la responsabilidad por los documentos firmados se asigna directamente al titular del Certificado Digital. Este aspecto no aplica a los Certificados emitidos para Firma Automática.

2. 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.

9.6.3. Derechos y Obligaciones de los Usuarios.

9.6.3.1. Derechos de las usuarias y usuarios.

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 según 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, corte del servicio o modificación de tarifas por vigencia de una nueva estructura tarifaria en la venta de dispositivos criptográficos.
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.

9.6.3.2. Obligaciones de las usuarias y usuarios.

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:

- Pagar sus facturas por los servicios recibidos, de conformidad con los precios o tarifas establecidas.
- 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.
- No causar daño a las instalaciones, redes y equipos de la Entidad Certificadora Pública.
- 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.
- No causar interferencias perjudiciales a operaciones debidamente autorizadas.
- 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.

9.7. Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital.

La Entidad Certificadora Pública ADSIB se obliga según lo dispuesto en este documento, así como lo dispuesto en las normativas y reglamentaciones vigentes sobre la prestación del servicio de certificación digital a:

a. Cumplir y hacer cumplir con lo dispuesto en la presente Declaración de Prácticas de Certificación.
b. Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT.
c. Publicar esta Declaración de Prácticas de Certificación, las Políticas de Certificación para cada tipo de certificado digital en el sitio web de la Entidad Certificadora Pública ADSIB
d. Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, reemisión, tarifas y uso vigentes establecidos para sus certificados digitales, el mismo que deberá ser publicado en el sitio web de la Entidad Certificadora Pública ADSIB.
e. Informar sobre las modificaciones aprobadas de esta Declaración de Prácticas de Certificación a los usuarios y Agencias de Registro que estén vinculadas a la Entidad Certificadora Pública ADSIB, mediante la publicación de éstas y sus respectivas modificaciones en el sitio web de la ADSIB.
f. Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario.
g. Revocar el certificado digital al producirse alguna de las causales establecidas en la presente Declaración de Prácticas de Certificación.
h. Mantener la información relativa a los certificados digitales emitidos, por un periodo mínimo de 5 (cinco) años posteriores al periodo de vigencia.

La Entidad Certificadora Pública ADSIB considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial a no ser que exista una imposición legal.

9.8. Infracciones y Sanciones.

Las infracciones y sanciones son establecidos por la Autoridad que regula el servicio que brinda la Entidad Certificadora Pública ADSIB.

9.9. Resolución de Conflictos.

Toda controversia o conflicto que se derive del presente documento, se resolverá mediante una negociación entre el titular y la Entidad Certificadora Pública ADSIB, dentro de quince (15) días hábiles luego de generado un ticket en el sistema de reclamos en el Sistema de Agencia de Registro.

Si no se logra conformidad para el titular se escalará el reclamo a la autoridad de fiscalización y telecomunicaciones ATT como ente regulador.

En caso de no llegar a ningún acuerdo quedará libre la vía de reclamo por proceso legal.

La Entidad Certificadora Pública ADSIB, salvo orden judicial de la autoridad competente, no intervendrá en manera alguna en la resolución de conflictos relacionados con el uso del certificado digital de los titulares con terceros.

El personal de la Entidad Certificadora Pública ADSIB no tendrá en ningún momento acceso a la clave privada de los titulares, por lo mismo se exime de cualquier responsabilidad con respecto a cualquier evento que comprometa dicha clave y las consecuencias derivadas de su uso.

9.10. Legislación aplicable.

Las políticas de certificación de la Entidad Certificadora Pública ADSIB fueron elaboradas en el marco de:

- Constitución Política del Estado Plurinacional de Bolivia
- Decreto Supremo 26553 de Creación de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- La Ley N°164 General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- El Decreto Supremo 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- El Decreto Supremo 3527 que modifica el Decreto Supremo 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- Las recomendaciones de la (Request for comments) RFC 3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) como encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras según la Ley N.º 164 emite

una serie de Resoluciones Administrativas Regulatorias y que fueron consideradas para la elaboración del presente documento:

- **ATT-DJ-RA TL LP 245/2018,** Documentos Públicos de la Entidad Certificadora Raíz.
- **ATT-DJ-RA TL LP 202/2019,** Requisitos y otros aspectos para la prestación del servicio de Certificación Digital.
- **ATT-DJ-RA TL LP 209/2019,** Estándar Técnico para la emisión de Certificados Digitales.
- **ATT-DJ-RAR-TL LP 272/2017** Estándar técnico para el funcionamiento de Agencias de Registro.

9.11. Conformidad con la ley aplicable.

Todos los procesos, procedimientos, información técnica y legal contenida en la presente "Política de Certificación" se encuentran elaborados en conformidad a lo establecido en la normativa legal vigente, así como en las Resoluciones Administrativas Regulatorias emitidas por la ATT como ente regulador.

10. 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 (ADSIB-FD-POLT-010 – Persona Jurídica y ADSIB-FD-POLT-011 – Persona Natural)	Reynaldo Alonzo Vera Arias	María Jannett Ibañez Flores	ADSIB/RA/0074/2018	31/12/2018
2.1	24/06/2019	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		

ANEXO 1: Particularidades del Certificado Digital de tipo Persona Jurídica

1.4.1. Usos apropiados del Certificado Digital

Se permite el uso de estos certificados digitales, en las relaciones del titular en representación de una entidad con particulares mediante la firma digital, y el uso de sistemas que estén adecuados para el uso de la firma digital.

Así mismo, un certificado digital de tipo Persona Jurídica tendrá los usos permitidos y limitaciones de acuerdo a normativa vigente.

1.4.2. Usos no autorizados de los certificados de persona jurídica.

Los certificados digitales de tipo Personal Jurídica solo pueden ser utilizados conforme a normativa y reglamentación vigente.

Además, sin contravenir lo expresado en el párrafo anterior, los certificados digitales de tipo Persona Jurídica no se pueden utilizar para firmar trámites realizados a nombre exclusivo del titular y/o sin establecer la relación de la personería jurídica.

4.1. Requisitos para la obtención de certificado digital.

Los requisitos adicionales para la obtención de un Certificado Digital de tipo Persona Jurídica son:

- 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.
- Nota de Autorización original para el solicitante, firmada por la Máxima Autoridad Ejecutiva o el Representante Legal de la Empresa.
- En función al nivel de seguridad del certificado a solicitar contar con:
  - Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards 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.

ANEXO 2: Particularidades del Certificado Digital de tipo Persona Natural

1.4.1. Usos apropiados del Certificado Digital

Se permite el uso de estos certificados digitales, en las relaciones del titular con particulares mediante la firma digital, y el uso de sistemas que estén adecuados para el uso de la firma digital.

Así mismo, un certificado digital de tipo Persona Natural tendrá los usos permitidos y limitaciones de acuerdo a normativa vigente.

1.4.2. Usos no autorizados de los certificados.

Los certificados digitales de tipo Personal Natural solo pueden ser utilizados conforme a normativa y reglamentación vigente.

4.1. Requisitos para la obtención de certificado digital.

Los requisitos adicionales para la obtención de un Certificado Digital de tipo Persona Natural son:

- Última factura de pago de luz, agua o teléfono u otro servicio que permita verificar su dirección actual del titular o solicitante. La dirección podrá referirse a su domicilio real o laboral.
- En función al nivel de seguridad del certificado a solicitar contar con:
  - Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards 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.

Se debe resaltar que la dirección declarada por el usuario solicitante debe ser similar a la que se encuentra descrita en la factura del servicio que se presenta como parte de los requisitos.