POLÍTICA DE CERTIFICACIÓN

ADSIB-FD-POLT-015

ASESORÍA LEGAL
UNIDAD DE INFRAESTRUCTURA DE SERVICIOS

	ELABORADO POR	REVISADO POR	APROBADO POR
Nombres:	José Flores Daza José Machicado Moya	Comité de Calidad, Seguridad de la Información y Emergencia	Bladimir Magne Molina
Cargos:	Asesor Legal Jefe Unidad de Infraestructura de Servicios		Director Ejecutivo
Firma:	Firmado Digitalmente	Firmado Digitalmente	Firmado Digitalmente
Fecha:	03/11/2024	04/11/2024	05/11/2024

POLÍTICA DE CERTIFICACIÓN DIGITAL

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.

1.1.1. Propósito.

El certificado digital para firma 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 de revocación 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.

El Artículo 83. (CERTIFICADOS DIGITALES PARA EL SECTOR PÚBLICO) de la Ley N° 164, establece: La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB, prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la presente Ley, y velará por la autenticidad, integridad y no repudio entre las partes.

En fecha 05 de marzo de 2021 la ADSIB firma el contrato ATT-DJ-CON SCD 1/21 con la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, por el cual se autoriza la prestación de servicios de certificación digital a la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

Las oficinas administrativas 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 Principal se encuentran en instalaciones del Edifico de la Vicepresidencia del Estado, en la parte del subsuelo y su Centro de Procesamiento de Datos Alterno se encuentra en el Piso 1 del edificio de la ADSIB.

Las funciones de la Entidad Certificadora Pública ADSIB están establecidas en el **ARTÍCULO 39.- (FUNCIONES DE LA ENTIDAD CERTIFICADORA) del Decreto Supremo N.º 1793,** que indica:

- Emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales;
- Facilitar servicios de generación de firmas digitales;
- Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario;
- Validar y comprobar cuando corresponda, la identidad y existencia real de la persona natural o jurídica;
- Reconocer y validar los certificados digitales emitidos en el exterior;
- Otras funciones relacionadas con la prestación de servicios 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 2.3.

1.2.3. Fecha de elaboración.

El documento fue actualizado en Septiembre de 2024.

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/politica2024.pdf

1.2.6. Identificador de Objeto.

Éste 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.

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 relacionada 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 éste 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 CRLs u OCSP.

Nota: Se puede encontrar más información sobre éste 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.

Cuando la Entidad Certificadora Pública ADSIB realice modificaciones a la presente “Política de Certificación”, deberán ser remitidas al ente regulador ATT con la correspondiente justificación, para posterior socialización y publicación de la nueva versión en su sitio web.

Para consultas y aclaraciones, la Entidad Certificadora Pública ADSIB designa el siguiente contacto:

- Dirección de correo: soporte@firmadigital.bo
- Teléfono: (591-2) 2200720 – 2200730

1.6. Definiciones y abreviaturas.

1.6.1. 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.
- **CPD:** Centro de Procesamiento de Datos.
- **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 Idenificación Tributaria emitido por el Servicio de Impuestos Nacionales.
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **OID:** (ObjectIdentifier) Identificador de Objeto.
- **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.
- **URI:** Identificador Uniforme de Recursos
- **UTF:** (Unicode Transformation Format) Formato de codificación de caracteres.

1.6.2. 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.

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.

- **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.
- **Caso Fortuito:** Obstáculo interno atribuible al hombre o a terceros vinculados, imprevisto o inevitable, relativas a las condiciones mismas en que la obligación debía ser cumplida (ataque informático, conmociones civiles, huelgas, bloqueos, revoluciones, etc.);
- **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.
- **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.
- **Firma Digital Automática:** Firma Digital generada por un sistema informático, donde el titular del certificado digital delega su usó para tareas definidas en este.
- **Fuerza Mayor:** Obstáculo externo, imprevisto o inevitable que origina una fuerza extraña al hombre que impide el cumplimiento de la obligación (incendios, inundaciones y otros desastres naturales);
- **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.
- **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.
- **Lista de confianza:** La lista de confianza establece, mantiene y publica información relativa a las Entidades de Certificación Autorizadas, posee el certificados raíz de la así

como los certificados emitidos a las Entidades de Certificación Autorizadas de la INCD, lo que permite y garantiza que las firmas digitales realizadas sean reconocidas como válidas.

- **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.
- **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.
- **Nota de Débito:** Documento que describe el monto a pagar por el usuario y especifica las cuentas bancarias a las que debe realizar el pago.
- **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.
- **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.
- **Servicio OCSP:** Servicio que permite utilizar un protocolo estándar para realizar consultas en línea al servidor establecido por una ECA sobre el estado de un Certificado Digital emitido por la misma.
- **Signatario:** Es la usuaria o usuario titular de un certificado digital emitido por una entidad certificadora autorizada, que le permite firmar digitalmente.
- **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.
- **Usuario titular:** El usuario titular para el servicio de certificación digital de la Entidad Certificadora Pública ADSIB es la persona física titular 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.

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 del día, 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 signatarios 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:

http://www.firmadigital.bo/ocsp

2.4. Términos y condiciones.

La prestación del servicio de Certificación Digital, se encuentra sujeta y sometida al cumplimiento de los Términos y condiciones ubicados en:

https://firmadigital.bo/terminos.pdf

2.5. Políticas de Certificación.

La “Política de Certificación” vigente se encuentra en:

https://firmadigital.bo/politicas2024.pdf

2.6. Declaración de prácticas.

La Declaración de Prácticas de Certificación vigente se encuentran en:

https://firmadigital.bo/practicas2024.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.
- Confirmación física o virtual de la identidad del solicitante o signatario.
- Otros medios de verificación que garanticen la identidad del usuario solicitante y prueba de vida que estén disponibles.

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 Infraestructure 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 y otras entidades. Se pueden realizar 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, no 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 signatario, autenticando la respectiva identidad de la persona a la presentación de los respectivos requisitos según el tipo de Certificado.

En cada caso los Oficiales de Registro deberán realizar la confirmación física o virtual de la identidad del signatario.

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

El Parágrafo I del Artículo 12 de la constitución política del estado Plurinacional de Bolivia, establece:
"...
Artículo 12.
I. El Estado se organiza y estructura su poder público a través de los órganos Legislativo, Ejecutivo, Judicial y Electoral. La organización del Estado está fundamentada en la independencia, separación, coordinación y cooperación de estos órganos."

En aplicación del parágrafo anterior, la Entidad Certificadora Pública ADSIB podrá establecer mediante la firma de convenios de coordinación y cooperación interinstitucional con entidades públicas, para que estas puedan designar a servidores públicos de su dependencia como "Oficiales de Registro Delegados". Estos servidores públicos designados tendrán la misma responsabilidad que los Oficiales de Registro de la Agencia de Registro de la ADSIB y serán responsables de cumplir con toda la normativa vigente relacionada con el servicio Certificación Digital, el registro, la validación de la documentación y otras, dentro de su entidad. La Entidad Certificadora Pública ADSIB realizará la capacitación y certificación de estos servidores públicos designados, para que cuenten con los conocimientos y habilidades necesarios para realizar su trabajo de manera efectiva, cumpliendo con todos los estándares de calidad y seguridad establecidos dentro de la Entidad Certificadora Pública ADSIB.

4.1. Requisitos para la obtención de certificado digital.

Los requisitos para la obtención de un Certificado Digital son:
De manera general:

- 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.
- Confirmación física o virtual de la identidad del usuario solicitante.

De manera general:

- 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 confirmación física o virtual de la identidad del usuario solicitante. En caso de ser necesario, el usuario solicitante podrá a personarse 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 (privada y pública) en un dispositivo 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 (público y privado) por software, en un dispositivo seguro 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 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 los requisitos que se requieran 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 nueva nota de débito con las formas de pago recomendadas.

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 Entidad Certificadora Pública ADSIB, en cumplimiento de la normativa vigente, tendrá un plazo máximo de 72 horas para la emisión de los certificados digitales 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.

Recibida la notificación de la emisión del Certificado Digital, es obligación del usuario titular realizar la importación del certificado digital a su respectivo medio de almacenamiento junto con su clave privada y proceder a firmar el contrato de adhesión; la no realización de estas acciones no afecta el cumplimiento del servicio.

El signatario debe firmar digitalmente el contrato de adhesión al servicio. Para ello tiene un plazo máximo de 120 horas, en caso de no firmar el contrato de adhesión en ese plazo el certificado digital será revocado de manera automática.

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 la normativa vigente y/o en las Resoluciones Administrativas Regulatorias emitidas por la ATT, para cada tipo de certificado digital que corresponda.

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 Digitales se la puede realizar hasta en tres (3) oportunidades consecutivas, siempre y cuando dicha solicitud se realice mientras el Certificado Digital a ser renovado se encuentre vigente. En estos casos todo el procedimiento es en línea a través del Sistema de Agencia de Registro. Asimismo, la solicitud de la 4ta renovación del Certificado Digital deberá ser procesada como una nueva solicitud.

La vigencia del Certificado Digital obtenido a partir de una renovación, será de un (1) año calendario.

Para certificados de firma digital automática la vigencia a partir de una renovación no podrá exceder los dos (2) años calendario.

La solicitud de renovación del Certificado Digital será responsabilidad del signatario o usuario corporativo.

La renovación del Certificado Digital puede ser realizada a partir de los últimos treinta (30) días calendario del periodo de vigencia del Certificado Digital a renovarse. La Entidad Certificadora Pública ADSIB enviará notificaciones para recordarle al usuario que puede realizar su renovación, de acuerdo al siguiente cronograma:

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

Las solicitudes de renovación se atenderán en los tiempos establecidos según normativa.

4.9. Solicitud de revocación de certificados.

El signatario 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 corporativo.

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 efectuar 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 cuarta (4) solicitud de reemisión en el periodo de vigencia del certificado, ya sea realizada por el signatario o por el usuario corporativo 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 signatario puede solicitar la reemisión de su certificado desde el sistema de 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 firma de un nuevo **contrato de adhesión**.

Las cuatro (4) reemisiones de Certificados Digitales no tienen ningún costo.

4.11. Servicio de estado de los certificados.

La Entidad Certificadora Pública ADSIB posee dos (2) servicios para comprobar el estado de los certificados digitales:

- Publicación de 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 siempre y cuando exista una nueva revocación.
- Protocolo de comprobación del Estado de un Certificado (OCSP), 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 sin posterior reemisión.

4.13. Recuperación de la clave.

En casos excepcionales siempre y cuando sea posible los oficiales de registro a solicitud exclusiva del usuario titular, brindarán apoyo en el desbloqueo del dispositivo criptográfico token. La recuperación de claves no aplica cuando la clave privada este resguarda en un HSM o software y 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 202/2019 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.

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.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los procedimientos de recuperación y continuidad del servicio.

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 su 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 módulos criptográficos, su gestión, sus controles y custodia.

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 la clave privada del módulo criptográfico, basado en un procedimiento multipersonal, donde solo el personal autorizado posee las claves necesarias descritas en estos procedimientos.

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 202/2019.

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 para la emisión de certificados digitales están sujetos a estrictos controles de seguridad y únicamente son accesibles desde la red interna de la Unidad de Infraestructura de Servicios. La red se encuentra segmentada y protegida por firewalls en alta disponibilidad, los sistemas de información están protegidos contra virus y software malicioso.

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 nivel 3.

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/

Asimismo, 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 Nacional de Certificación Digital de Bolivia.

El certificado utilizado para la verificación de una respuesta OCSP contiene 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”, se realiza en base a la experiencia institucional de la Entidad Certificadora Publica ADSIB 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, 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.

9.2.1. Pago y Facturación.

Para realizar el pago del certificado digital, la Entidad Certificadora Pública ADSIB brinda diversas modalidades de pago, mismas se encuentran disponibles en el sitio web de la Entidad Certificadora Pública, asimismo la forma de pago recomendada se establecerá en la nota de débito que sea generado en el momento de la solicitud del certificado.

La Entidad Certificadora Pública ADSIB, emite facturas electrónicas a nombre y número de identificación tributaria definida por el titular, una vez emitido el certificado digital. En caso de cuentas corporativas la factura electrónica 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 a la nota de débito o comprobante.

Todo depósito no asociado a una solicitud de emisión de certificado digital que no sea utilizado en un plazo de noventa (90) días calendario sera considerado como "deposito no identificado"; durante ese tiempo el depositante podrá solicitar su utilización en la emisión de certificados digitales. Concluido ese plazo será registrado como Otros Ingresos de la Entidad Certificadora Pública ADSIB y podrá ser sujeto de restitución a requerimiento del depositante.

Los depósitos "no identificados" serán publicados en el sitio web de la Entidad Certificadora Pública ADSIB por un lapso de 60 (sesenta) días calendario.

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.

En el documento “Declaración de Prácticas de Certificación” se detalla más información de la protección de datos personales.

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.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Derechos de la Entidad Certificadora Pública.

9.6.1.2. Obligaciones de la Entidad Certificadora Pública.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Derechos y Obligaciones de la Entidad Certificadora Pública.

9.6.1.3 Derechos y Obligaciones de la Entidad Certificadora Pública y ante Terceros que confían.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Derechos y Obligaciones de la Entidad Certificadora Pública y ante Terceros que confían.

9.6.1.4. Obligaciones de la Entidad Certificadora Pública ante Corte del Servicio

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Obligaciones de la Entidad Certificadora Pública ante corte del servicio.

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.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre la Responsabilidad del Titular.

9.6.2.2. Derechos del Titular del Certificado.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Derechos del Titular del Certificado.

9.6.2.3. Obligaciones del Titular del certificado.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre las Obligaciones del Titular del certificado.

9.6.3. Derechos y Obligaciones de los Usuarios.

9.6.3.1. Derechos de las usuarias y usuarios.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre los Derechos de las usuarias y usuarios.

9.6.3.2. Obligaciones de las usuarias y usuarios.

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre las Obligaciones de las usuarias y usuarios.

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

En el documento “Declaración de Prácticas de Certificación” se detalla más información sobre las Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital.

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 de reclamo 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 Infraestructure: 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-RAR-TL LP 272/2017 Estándar técnico para el funcionamiento de Agencias de Registro.**
- **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 357/2020,** Modificación al “Estándar Técnico para la emisión de Certificados Digitales”.

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	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	08/12/2020	Modificación al “Estándar Técnico para la emisión de Certificados Digitales ATT-DJ-RAR-TL LP 357/2020,	Miguel Choque	Bladimir Magne Molina	ADSIB/ RA/ 0027/2020	08/12/2020
2.3	11/2024	Ajustes al documento para el cumplimiento de las observaciones de la ATT.	Comité de Calidad, Seguridad de la Información y de Emergencia	Bladimir Magne Molina		04/11/2024

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 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.
- Documento vigente y legalmente aplicable en el que se establezca la relación laboral entre la empresa o entidad y el solicitante.
- En función al nivel de seguridad, deberá contar:
    - **Para Certificados Digitales con seguridad alta:** Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2 nivel 2 mínimamente. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web (https://www.att.gob.bo/homologados). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud
    - **Para Certificados Digitales con seguridad normal:** Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, 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. La Entidad Certificadora Pública ADSIB provee una

herramienta homologada por la ATT para la generación del par de claves por software, misma que puede ser encontrada en:

https://firmadigital.bo

7.1. Formato para Certificado Digital

7.1.1. Formato para Certificado Digital de tipo Persona Jurídica

El formato para los certificados digitales para persona jurídica tanto de seguridad alta como normal (generación de par de claves en dispositivo de seguridad hardware o software) deben cumplir con la siguiente estructura:

NOMBRE	DESCRIPCIÓN
Versión (version)	2
Número de Serie (serialNumber)	Número asignado por la Entidad Certificadora Pública ADSIB
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer)	**CN** = "Entidad Certificadora" y el nombre de la Entidad Certificadora Pública ; **O** = Razón social de la Entidad Certificadora Pública; **C**=BO (de acuerdo a ISO3166).
Periodo de validez (validity)	Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	**CN** = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; **O** = Razón social de la empresa o institución a la que representa la persona jurídica; **OU** = Unidad Organizacional de la que depende (opcional); **T** = Cargo del representante legal; **C** = estándar de acuerdo con ISO 3166 {BO}; **dnQualifier** = Tipo de documento {CI/CE}; **uidNumber** = Nro. de documento {numeral}; **uid** = número de complemento {alfanumérico} (opcional); **serialNumber** = Número de NIT {numeral} (opcional); **description** = Nivel de seguridad.
Clave pública del suscriptor (subjectPublicKey)	Algoritmo: RSA, Longitud: mínimo 2048 bits

El campo Descripción (description) puede tomar uno de los siguientes valores:

Campo Descripción (description)	Normativa
Persona Jurídica Firma Simple	RAR ATT-DJ-RA TL LP 209/2019

Persona Jurídica Firma Automática	RAR ATT-DJ-RA TL LP 209/2019
Persona Jurídica Seguridad Normal Firma Simple	RAR ATT-DJ-RA TL LP 209/2019
Persona Jurídica Seguridad Normal Firma Automática	RAR ATT-DJ-RA TL LP 209/2019

7.1.2. Extensión para Certificado Digital de tipo Persona Jurídica.

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

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

El campo Política de Certificación (certificatePolicies), además de contener la dirección de la Política de Certificación, debe contener el OID del tipo de Certificado relacionado al campo Descripción (description) y puede tomar los siguientes valores:

Campo Descripción (description)	Normativa
2.16.68.0.0.0.1.14.1.2.0.1.2.1.0.0 Persona Jurídica Firma Simple	RAR ATT-DJ-RA TL LP 209/2019
2.16.68.0.0.0.1.14.1.2.0.1.2.1.0.1 Persona Jurídica Firma Automática	RAR ATT-DJ-RA TL LP 209/2019
2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.0 Persona Jurídica Seguridad Normal Firma Simple	RAR ATT-DJ-RA TL LP 209/2019
2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.1 Persona Jurídica Seguridad Normal Firma Automática	RAR ATT-DJ-RA TL LP 209/2019

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 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, deberá contar:
    - **Para Certificados Digitales con seguridad alta:** Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2 nivel 2 mínimamente. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web (https://www.att.gob.bo/homologados). En el dispositivo de seguridad es donde se generarán el par de claves (pública y privada) para realizar la solicitud
    - **Para Certificados Digitales con seguridad normal:** Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR ATT-DJ-RA TL LP 209/2019, 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. La Entidad Certificadora Pública ADSIB provee una herramienta homologada por la ATT para la generación del par de claves por software, misma que puede ser encontrada en:

https://firmadigital.bo

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.

7.1. Perfil de Certificado de tipo Persona Natural

7.1.1. Formatos para los Certificados Digitales para persona natural o Física

El formato para los certificados digitales para persona natural debe cumplir con la siguiente estructura

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

El campo Descripción (description) puede tomar uno de los siguientes valores:

Campo Descripción (description)	Normativa
Persona Natural Firma Simple	RAR ATT-DJ-RA TL LP 209/2019
Persona Natural Firma Automática	RAR ATT-DJ-RA TL LP 209/2019
Persona Natural Seguridad Normal Firma Simple	RAR **ATT-DJ-RAR-TL LP 357/2020**
Persona Natural Seguridad Normal Firma Automática	RAR **ATT-DJ-RAR-TL LP 357/2020**

7.1.2. Extensión para Certificado Digital persona natural

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

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

El campo Política de Certificación (certificatePolicies), además de contener la dirección de la Política de Certificación, debe contener el OID del tipo de Certificado relacionado al campo Descripción (description) y puede tomar los siguientes valores:

Campo Política de Certificación (certificatePolicies)	Normativa
2.16.68.0.0.0.1.14.1.2.0.1.2.1.1.0 Persona Natural Firma Simple	RAR ATT-DJ-RA TL LP 209/2019
2.16.68.0.0.0.1.14.1.2.0.1.2.1.1.1	RAR ATT-DJ-RA TL LP 209/2019

Persona Natural Firma Automática	
2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.0 Persona Natural Seguridad Normal Firma Simple	RAR ATT-DJ-RAR-TL LP 357/2020
2.16.68.0.0.0.1.14.1.2.0.1.2.0.1.1 Persona Natural Seguridad Normal Firma Automática	RAR ATT-DJ-RAR-TL LP 357/2020