POLÍTICA DE CERTIFICACIÓN TIPO DE CERTIFICADO PERSONA NATURAL

ADSIB-INST-POLT-01 Unidad de Gestión de Servicios

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:		Reynaldo Alonzo Vera Arias José Luis Machicado Moya	María Jannett Ibañez Flores
Cargo:		Jefe de la Unidad de Gestión de Servicios Jefe de la Unidad de Infraestructura de Servicios	Directora Ejecutiva
Firma:			
Fecha:		08/10/2018	

POLÍTICA DE CERTIFICACIÓN “TIPO DE CERTIFICADO PERSONA NATURAL”

POLÍTICA DE CERTIFICACIÓN "TIPO DE CERTIFICADO PERSONA NATURAL"

1. Introducción

1.1. Descripción General.

El presente documento presenta la Política de Certificación Digital para el tipo de certificado Persona Natural, 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 N° 1793 y Decreto Supremo N° 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. Así mismo, se tiene una Política de Certificación de tipo de Persona Jurídica.

En este documento se presentan las condiciones particulares referentes a los Certificados Digitales de tipo Persona Natural, el mismo que está sujeto al cumplimiento de la Declaración de Prácticas de Certificación de la ADSIB.

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

Este documento fue desarrollado de acuerdo con las Resoluciones Administrativas Regulatorias RAR ATT-DJ-RAR-TL LP 32/2015, RAR ATT-DJ-RAR-TL LP 1538/2015, RAR ATT-DJ-RAR-TL LP 272/2017, emitido 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 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.

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 ADSIB se encuentran ubicadas en la calle Ayacucho y Mercado No 308 - Edificio de la Vicepresidencia del Estado, Piso 3, así mismo, las dependencias de su Data Center se encuentran en las mismas instalaciones en la parte del subsuelo.

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.
- Garantizar la validez de las firmas digitales, sus 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 y nombre del documento.

1.2.1. Nombre

El presente documento lleva como título “Política de Certificación tipo de certificado Persona Natural”.

1.2.2. Versión

El documento se encuentra en su versión 1.

1.2.3. Fecha de elaboración

El documento fue elaborado en noviembre de 2018.

1.2.4. Fecha de actualización

Esta es la primera versión.

1.2.5. Localización.

La presente política se la puede localizar en: https://firmadigital.bo/files/PCPN.pdf

1.3. Infraestructura Nacional de Certificación Digital.

La Infraestructura Nacional de Certificación Digital, está establecida en el Decreto Supremo N.º 1793, la 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 del INCD.

1.4. Uso de los certificados.

1.4.1. Usos apropiados de los certificados de persona natural

Los certificados digitales de tipo Persona Natural 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 de tipo Persona Natural 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

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.

1.4.2. Usos no autorizados de los certificados de persona natural

No se permite el uso de los certificados digitales para persona natural 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 y la Política de Certificación para el tipo Persona Natural.

No se autoriza el uso de los certificados digitales de tipo Persona Natural para firmar CRLs o firma de OCSP.

Todo uso no autorizado o malintencionado que concluya en un proceso por daños y prejuicios, solamente surten efecto entre los usuarios intervinientes del acto o negocio jurídico. La 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 integridad de los certificados emitidos.

1.5. Administración de las Políticas de Certificación de Persona Natural.

La responsabilidad de la administración de esta “Política de Certificación Tipo de Certificado Persona Natural” corresponde a la ADSIB como Entidad Certificadora Pública.

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

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.
- **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.
- **ECP:** Entidad Certificadora Pública.
- **ECR:** Entidad Certificadora Raíz.
- **HSM:** (Hardware Security Module) Modulo de Hardware de Seguridad[1].
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **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.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **RFC:** (Request For Comments[2]) Requerimiento de Comentarios.
- **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.
- **UTF:** (Unicode Transformation Format) Formato de codificación de caracteres

[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.

1.6.2. Definiciones

- **Certificado digital:** Es un archivo digital firmado digitalmente por una entidad certificadora autorizada que vincula una clave pública a un signatario. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.
- **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 alfanuméricos 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 un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un documento digital, o un correo electrónico, que certifica la identidad del signatario y la integridad del documento digital firmado. La firma digital está compuesta por el "hash" del documento digital cifrado por la clave privada del signatario, y por el certificado digital del signatario.
- **Módulo criptográfico o token:** Es un dispositivo de seguridad basado en hardware que genera, almacena y protege claves criptográficas
- **Usuario titular:** El usuario titular para el servicio de certificación digital de la ADSIB es la persona física poseedora del certificado digital y en consecuencia, tendrá los derechos de revocación, remisión y renovación sobre el certificado. El certificado puede ser de persona natural o persona jurídica.
- **Usuario corporativo:** Las cuentas corporativas son las entidades que establecen un vínculo contractual o de convenio con la ECP para adquirir certificados digitales para su personal interno.

2. Publicación de información y del repositorio

2.1. Repositorio

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

https://firmadigital.bo/

La ADSIB como Entidad Certificadora Pública 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 contingencias en el sitio web, la ADSIB, aplicará el procedimiento de gestión de incidentes para que el sitio web 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 ECP que para fines del servicio se constituyen como sus Términos y Condiciones.

2.5. Políticas de Certificación

Las Políticas de Certificación de la ECP se encuentran en:

https://firmadigital.bo/files/POL%C3%8DTICAS%20DE%20CERTIFICACI%C3%93N%20PARA%20UNA%20ENTIDAD%20CERTIFICADORA.pdf

2.6. Declaración de prácticas

La Declaración de Prácticas de Certificación se encuentran en:

https://firmadigital.bo/files/DECLARACI%C3%93N%20DE%20PRACTICAS%20DE%20CERTIFICACI%C3%93N.pdf

2.7. Publicación

La ADSIB proporciona acceso público a la siguiente información:

- Los certificados digitales de la Entidad Certificadora Publica, Entidad Certificadora Raiz 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 compuestos por la presente Política de Certificación y los documentos de Políticas de los diferentes tipos de certificados, así como la Declaración de Prácticas de Certificación.
- Histórico de las versiones anteriores de los documentos públicos.
- 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 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 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.

Todos los certificados requieren un nombre distinguido conforme al estándar X.500.

No serán admitidos o procesados por la ADSIB los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el usuario. En 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 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

Todos los certificados requieren un nombre distinguido conforme al estándar X.500.
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 solicitantes de certificados digitales de tipo Persona Natural, mediante servicios de interoperabilidad establecidos con el SEGIP y el SERECI.

3.3. Identificación y autenticación de las solicitudes de renovación de clave.

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 ADSIB pueden solicitar la renovación del certificado digital, autenticando la identidad de la persona a la presentación del documento de identidad (carnet de identidad o carnet de extranjero).

3.4. 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 de que el usuario no conteste después de tres intentos igual se realizará la revocación, registrando 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 registrados según su listado de beneficiarios, sin realizar verificación alguna.

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

4.1. Requisitos para obtención de certificado digital como persona natural

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

- Documento de Identidad vigente (Carnet de identidad o extranjero, según corresponda).
- Última factura de un servicio básico (Luz o agua) que permita verificar su dirección actual.
- Registro y solicitud de un certificado digital de tipo persona natural en el sistema de la Agencia de registro.

4.2. Procesamiento de la solicitud del certificado

Para realizar una solicitud de certificado digital debe ser mayor de 18 años.

Las solicitudes para obtener un Certificado Digital de tipo Persona Natural, se inician desde el sistema de Agencia de Registro, siguiendo todos los procedimientos indicados en el mismo. Para concluir su solicitud debe apersonarse a alguna de las sucursales de la Agencia de Registro seleccionada, donde procederán a completar la solicitud, mediante la captura de la foto y registro de huellas para su respectiva validación.

El solicitante podrá **generar el par de claves** directamente desde el Sistema de Agencia de Registro, según procedimientos publicados por la Agencia de Registro. Así mismo, los Oficiales de Registro brindarán el apoyo necesario para la generación del par de claves de ser necesario y requerido por el solicitante, no debiendo participar de manera directa, debido a que se constituye una acción privada.

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) para el solicitante, debe ser firmada digitalmente y remitida a la Entidad Certificadora Pública.

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

Una vez revisada la solicitud y concluido el proceso de registro y verificación de documentos, la AR debe firmar digitalmente la solicitud de firma de certificado (CSR) y remitirla a la ECA a través del Sistema de Agencia de Registro.

4.3. Emisión de certificados

La ADSIB como Entidad Certificadora Pública dispone de procedimientos internos para la ceremonia de Firma Digital de los certificados que son estrictamente aplicados a las solicitudes 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, y enviará a la respectiva Agencia de Registro el certificado digital firmado, salvo en caso fortuito, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante.

4.4. Aceptación del certificado

Los certificados emitidos por la Entidad Certificadora Pública son enviados al sistema de Agencia de Registro. La misma deberá notificar al usuario titular poseedor de la clave privada que ya puede descargar su certificado correspondiente.

La aceptación del certificado se realiza con la firma del contrato de adhesión del servicio de forma digital, en caso de no realizarse esta aceptación el certificado será revocado.

4.5. 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 ADSIB como Entidad Certificadora Pública y aprobado por la ATT.

4.6. Solicitud de renovación de certificados

La renovación de certificados digitales se la puede realizar hasta tres oportunidades, siempre y cuando el certificado este vigente. La presencia física del usuario solicitante no es necesaria para realizar dicha solicitud.

La vigencia del Certificado Digital de tipo Persona Natural obtenido a partir de una renovación, tendrá una duración máxima de un año.

La solicitud de renovación del certificado digital será responsabilidad de su titular, y lo puede realizar desde el sistema de Agencia de Registro, realizando el pago correspondiente según la estructura tarifaría 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, mismas que serán notificadas al titular del certificado digital vía correo electrónico.

Los procedimientos establecidos para la renovación de un certificado digital serán válidos mientras el certificado digital se encuentre vigente.

En caso de que la vigencia del certificado haya finalizado o el usuario titular haya realizado tres renovaciones consecutivas, la solicitud del certificado digital debe ser procesada como una nueva emisión.

4.7. 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.

El Titular del certificado digital podrá realizar la revocación de su certificado digital, mientras se encuentre vigente, bajo los procedimientos establecidos en la Declaración de Prácticas de Certificación.

La revocación del certificado se hará efectiva después de realizar la verificación de la solicitud de revocación en el sistema de la Agencia de Registro y/o de a través de correo electrónico o llamada telefónica y/o inmediatamente cuando se realice la solicitud en presencia de un Oficial de Registro.

En caso de los usuarios corporativos, la revocación podrá realizarse, por el usuario responsable, a través del Sistema de Agencia de Registro y será efectiva inmediatamente.

4.8. Solicitud de reemisión de certificados

La reemisión de un certificado digital es un procedimiento que no requiere la presencia física del usuario titular, y las condiciones para realizarlo son:

- Haber solicitado revocación del certificado.
- La solicitud debe realizarse en el periodo de vigencia del certificado digital inicial
- No supere la segunda solicitud de reemisión en el periodo.

La solicitud de reemisión de certificado digital debe aplicarse a un certificado previamente revocado. 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 revocado inicialmente.

El titular del certificado digital puede realizar la reemisión de su certificado desde el sistema de la Agencia de Registro.

4.9. Servicio de estado de los certificados

La ADSIB posee dos (2) servicios de comprobación de estado de los certificados.
Uno de los servicios es la lista de certificados digitales revocados (CRL), que tiene la finalidad de comprobar si un certificado ha sido revocado por una autoridad certificadora. Esta se actualiza periódicamente cada 15 minutos.

Otro método de comprobación se realiza mediante el acceso al servicio OCSP, que estará disponible en línea las 24 horas, los 7 días de la semana

4.10. Finalización de la suscripción

La suscripción del servicio de certificación digital es por un año calendario, el fin de suscripción se produce cuando expira el periodo de vigencia del certificado o se realiza una revocación sin posterior reemisión.

4.11. Recuperación de la clave

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

4.12. Depósito de claves y recuperación

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

5. Controles de seguridad física, gestión y de operaciones.

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 31/2015 emitida por la ATT.
La ADSIB como Entidad Certificadora Pública 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.

5.1.1. Ubicación y construcción

El Centro de Datos de la ADSIB se encuentra en el Edificio de la Vicepresidencia del Estado Plurinacional de Bolivia, ubicado en el centro de la ciudad de La Paz, entre las calles Ayacucho y Mercado No 308.
La construcción del Centro de Datos reúne y mantiene los requisitos de operación, que impone la normativa en materia de seguridad. El Centro de Datos opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

La ADSIB cuenta con un Centro de Datos alterno que dispone controles de seguridad físico ambientales y solidez en la construcción, con vigilancia durante las 24 horas al día, los trescientos sesenta y cinco (365) días del año.

5.1.2. Acceso físico

El acceso físico al centro de datos mantiene medidas de control de acceso tanto lógicas como físicas garantizando la integridad y seguridad de los servicios prestados. Para el control de acceso físico existen cinco (5) niveles de seguridad, desde el exterior hasta el gabinete de la firma digital donde se encuentra la infraestructura necesaria del servicio

Los procedimientos de seguridad permiten o restringen el acceso al Centro de Datos, desde el exterior hasta los servidores. El acceso está permitido solo al personal autorizado mediante: Login y contraseña, accesos biométricos y cerraduras físicas.

Para el acceso al gabinete de la firma digital donde se ubican los procesos criptográficos es necesario la autorización previa de ADSIB según los planes y procedimientos de ingreso al centro de datos.

Se cuenta con sistema de vídeo vigilancia y de grabación que monitoriza los elementos con los que la ADSIB presta el servicio de certificación dentro del centro de datos y áreas o instalaciones destinadas al servicio.

5.1.3. Alimentación eléctrica y aire acondicionado

La construcción donde se encuentran instalados los servidores de la ADSIB cuenta con fuentes de energía ininterrumpida (UPS), las cuales a su vez están conectadas a un sistema de alimentación eléctrica alterno con un grupo electrógeno.

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

Las salas donde se ubican los equipos que componen los sistemas de certificación de la ADSIB y donde se realiza el proceso de emisión de certificados, disponen de suministro eléctrico garantizado por un grupo electrógeno, unidades de alimentación ininterrumpida y aire acondicionado para la operativa normal del servicio; además tienen instalados mecanismos que mantienen controlados el calor y la humedad a niveles acordes con los equipos que se encuentran instalados en el lugar.

5.1.4. Exposición al Agua

Las instalaciones del Centro de Datos y Cabina de Firma Digital están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se encuentra ubicados los equipos informáticos disponen de un sistema de detección de humedad.

5.1.5. Protección y prevención de incendios

Las instalaciones del Centro de Datos, Cabina de Firma Digital y áreas de trabajo para el servicio tienen incorporados alarmas y sensores de detección contra fuego y humo, ante cualquiera eventualidad que se presente, los cuales son monitorizados mediante un sistema de detección automática.

Se tienen extinguidores ubicados en lugares establecidos y adecuados.

5.1.6. Sistema de almacenamiento

La ECP tiene establecido los procedimientos necesarios para disponer de copias de seguridad de respaldo de la información critica relacionada al servicio, almacenada de manera interna y externa garantizando su integridad y confidencialidad, los soportes de las copias de seguridad se almacenan de forma segura.
La ECP tiene establecidos procedimientos de respaldo, resguardo y recuperación de las copias de seguridad en un sitio alterno, su transferencia y resguardo esta definida según procedimientos, la información enviada y almacenada en soportes de información se encuentra cifrada.

5.1.7. Eliminación de residuos

Los soportes que contengan información confidencial de la ECP deberán ser destruidas, de tal manera que la información sea irrecuperable previniendo de esta manera el uso no autorizado y el acceso o divulgación de la información contenida en los desechos.

5.1.8. Copia de Seguridad

La ECP dispone de copias de seguridad de la información critica del servicio en instalaciones seguras fuera del sitio principal, las mismas se enmarcan de acuerdo a los procedimientos de respaldo, resguardo, recuperación y entrega de copias de seguridad en conformidad al plan de contingencias y continuidad.

5.2. Controles de procedimiento

5.2.1. Roles de confianza

La Entidad Certificadora Pública mantendrá un esquema de gestión y operación basado en una estructura plana, sustentada sobre la interacción e interdependencia del personal en sus diversos roles y funciones.
La Entidad Certificadora Pública se encuentra dividida en funciones de operación y administración. La Dirección Ejecutiva es la que se encarga de la toma de decisiones; la Unidad de Infraestructura de Servicios es la encargada de la parte operativa y del mantenimiento del Centro de Datos.
Todas las decisiones que se realizaren a las operaciones técnicas y administrativa serán evaluadas por el Comité de Calidad, Seguridad de la Información y de Emergencia.

5.2.2. Número de personas requeridas por tarea

El número de personas requeridas por tarea, y el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección Ejecutiva, misma que deberá formalizarla de manera escrita.

5.2.3. Identificación y autenticación para cada rol.

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

5.3. Controles de seguridad del personal

5.3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación

El personal involucrado en el control y operación de la firma y certificado digital está suficientemente calificado y dispone de la experiencia necesaria para cumplir con las funciones asignadas a su rol, así mismo recibirá capacitación continua para garantizar los niveles de calidad sobre las políticas de seguridad y los procedimientos.

5.3.2. Procedimientos de comprobación de antecedentes

La calificación y comprobación de los antecedentes, experiencia y conocimiento del personal se lo realizará según los procedimientos internos que la Entidad Certificadora Pública dispone para la contratación de personal permanente, consultoría y eventual.

5.3.3. Formación y frecuencia de actualización de la formación.

El personal encargado de la Certificación Digital dentro de la ECP debe recibir capacitación al menos una vez al año, en áreas asociadas a su labor directa u orientadas al desarrollo de destrezas necesarias para la prestación acorde y conforme de sus servicios.

5.3.4. Frecuencia y secuencia de rotación de tareas

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

5.3.5. Sanciones por acciones no autorizadas

Todo procedimiento no contemplado en el presente documento de Políticas de Certificación deberá contar con la aprobación expresa de la Dirección Ejecutiva de la ADSIB, de lo contrario será considerado como acto de sabotaje a los fines internos de la ADSIB y será sancionado con despido justificado, por incumplimiento de las obligaciones que impone la relación de trabajo.

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

La ADSIB sigue la normativa definida bajo el sistema de contratación de bienes y servicios estipulado por el Estado Plurinacional de Bolivia y cuenta con controles periódicos a través de la presentación de informes internos relacionado a cada acción que deba ser informada.
Todo personal de la ADSIB que finaliza su relación contractual con la institución debe cumplir con los procedimientos administrativos correspondientes y guardar confidencialidad sobre la información a la que tuvo acceso en la entidad.

5.4. Procedimientos de Control de Seguridad

5.4.1. Tipos de eventos registrados

La ADSIB almacena registros de los eventos (logs) de seguridad mas significativos relativos a su actividad como Entidad Certificadora Pública. Estos registros son almacenadosautomáticamente, así mismo en los casos del acceso físico se debe autorizar y registrar de acuerdo a los planes y procedimientos de seguridad de la ECP.

Los registros mínimos de los eventos relacionados con la seguridad de la infraestructura de clave publica deben ser los siguientes:

- Instalación y Configuración de los Sistemas Operativos.
- Instalación y Configuración de cualquier aplicación instalada en el equipo.
- Instalación y Configuración de la Autoridad de Certificación.
- Instalación y Configuración del Módulo Criptográfico.
- Accesos o intentos de acceso al equipo.
- Actualizaciones.
- Mantenimientos.
- Realización de copias de seguridad.
- Eventos del software de certificación:
  - Gestión de usuarios.
  - Gestión de Roles.
  - Gestión de Certificados (todo lo contemplado en el ciclo su vida)
- Eventos relacionados con el acceso físico
- Eventos de acciones correctivas y preventivas

5.4.2. Frecuencia de procesado de logs

La frecuencia con la que se llevan a cabo el procesado de registros de logs, son en el preciso momento que se realiza la operación en los sistemas, aplicaciones y servicios de la ECP.

La ECP dispone de herramientas tecnologicas para el monitoreo continuo de las operaciones realizadas en el equipamiento tecnológico de la infraestructura de clave publica.

5.4.3. Periodo de retención para los logs de auditoría

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

Los sistemas, aplicaciones y servicios de la ECP tendrán periodos de retención de logs de auditoria según el procedimiento de gestión de logs definido..

5.4.4. Protección de los logs de auditoría

La ADSIB como Entidad Certificadora Publica (ECP) dispone de medidas para garantizar la disponibilidad, integridad y conservación de los logs de auditoría de los sistemas, aplicaciones y servicios asociados al servicio y la infraestructura tecnológica para a la emisión de certificados digitales

5.4.5. Procedimientos de copia de seguridad de los logs de auditoría

Se generan copias de respaldo incrementales, de acuerdo a la Política de Respaldo, Resguardo y Recuperación y Procedimiento de Gestión de Logs.

5.4.6. Sistema de recogida de información de auditoría

La ECP tiene implementado un sistema de centralización de eventosel cual monitorea y notifica actividades dentro del equipamiento tecnológico del servicio de certificacion digital, el cual combina procesos automáticos y manuales.

5.4.7. Notificación al sujeto causa del evento

No estipulado.

5.4.8. Análisis de vulnerabilidades

A fin de estar preparados ante contingencias que involucren interrupciones en el servicio de certificación digital y garantizar la continuidad del mismose tiene un cronograma anual de análisis de vulnerabilidades en los sistemas, aplicaciones y servicios críticos relacionadas a la Entidad Certificadora Pública.
Los análisis son internos y externos, esta última para tener independencia de valoración en cuanto a la criticidad de la información.
Se tiene un procedimiento de plan de pruebas que incluye la realización de análisis de vulnerabilidades y otros que son necesarios en el CPD.

5.5. Archivo de informaciones y registros

La ECP debe garantizar que la informacion generada producto de la emisión de certificados digitales se almacene durante un periodo de tiempo apropiado.
La documentación confidencial generada por la ECP almacenada en soportes de información físicas y digitales contienen niveles de seguridad tanto fisicas como lógicas.
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.

5.5.1. Tipo de información y eventos registrados

La ADSIB archivará la información referente a:

- Registro de usuarios
- Solicitud de certificados
- Renovación de certificados
- Revocación de certificados
- Reemisión de certificados.

5.5.2. Periodo de retención para el archivo

Todos los registros de la ADSIB referentes a la operación de sus servicios de certificación son archivados conforme a la normativa de conservación de documentos del Estado Plurinacional de Bolivia.

5.5.3. Sistema de recogida de información para auditoría

Cada uno de los servidores de certificación posee un módulo para almacenar los registros de eventos de certificación, dicho registro permite ser utilizados para auditorías, verificando los intentos de acceso, los accesos y las operaciones dañinas, sean estas intencionales o no, como también las operaciones normales realizadas para la firma de certificados.

5.5.4. Procedimientos para obtener y verificar información archivada

La información descrita en el punto anterior se la podrá obtener bajo una solicitud dirigida a la Dirección Ejecutiva de la ADSIB, explicando los motivos de la solicitud, que tras el análisis de este se aceptará o no el acceso a esta información.

5.6. Cambio de clave de la ADSIB

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

a) De algún modo se ha visto comprometida la clave privada de la ADSIB como ECP.
b) Por la caducidad del certificado firmado por la ATT para las operaciones de la ADSIB como ECP.
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 ADSIB tiene sus procedimientos para la recuperación de la clave privada mediante los documentos “Planes y Procedimientos para laContinuidad del Servicio y Plan de Contingencias”.

5.8. Procedimientos para recuperación de desastres

La ADSIB cuenta con Planes y Procedimientos para la de 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 comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. El documento Planes y Procedimientos para la de Continuidad del Servicio es revisado periódicamente según cambios de los riesgos en el ambiente.
El Plan y Procedimiento para la de 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 de 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 ADSIB como Entidad Certificadora Pública.

El cese de actividades de la ADSIB como Entidad Certificadora Pública 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.

5.9.1. Sujetos involucrados.

El cese de actividades de la ADSIB como Entidad Certificadora Pública involucrará directamente a todos los usuarios titulares de los certificados digitales.

5.9.2. Procedimiento para el cese de actividades.

El período de implementación del procedimiento para el cese de actividades se realizará desde la declaración de cese de actividades hasta la inhabilitación lógica y física de la ADSIB del servicio de certificación digital, que a partir de la declaración de cese de actividades la ADSIB ya no emitirá certificados digitales de solicitudes nuevas, renovaciones y reemisiones, solo publicará la lista de certificados revocados.

5.9.2.1. Publicación

Ante la declaración del cese de actividades de la ADSIB como ECP, la primera tarea será publicar la información en el sitio web: www.firmadigital.bo y www.adsib.gob.bo así mismo se publicará en un medio de difusión nacional para conocimiento de todos los usuarios.

5.9.2.2. Notificación

La ADSIB notificará a todos los usuarios titulares del cese de actividades cuyos certificados permanezcan en vigencia. La misma se llevará a cabo con una antelación mínima de dos (2) meses.
La notificación se realizará mediante correo electrónico firmado digitalmente y mediante la página web www.firmadigital.bo y www.adsib.gob.bo, por el transcurso del tiempo que dure la transición del servicio a otra entidad. Las mismas indicarán las fechas precisas del cese de actividades, señalando además que, de no existir objeción a la transferencia de los certificados digitales dentro del plazo de quince (15) días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido la transferencia de los mismos.

5.9.2.3. Solicitudes de certificados

Una vez anunciado el cese de actividades de la ADSIB como Entidad Certificadora Pública, se rechazará la solicitud de emisión de un nuevo certificado, de cualquier tipo, ya sea por renovación, reemisión o solicitudes nuevas por parte del usuario titular dentro de los sesenta (60) sesenta días calendarios anteriores a la fecha prevista para el cese.

5.9.2.4. Revocación de Certificados y Lista de Certificados Revocados

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

a) Se podrá revocar certificados de suscriptores hasta el mismo día y hora del cese de actividades. Solamente podrá efectuar revocaciones a solicitud de sus suscriptores. Si los suscriptores, después de haber sido notificados del cese de actividades de la Entidad Certificadora, dentro del plazo de quince (15) días calendario, se entenderá que el usuario ha consentido la transferencia del certificado digital.
b) La ADSIB realizará una transferencia de los certificados emitidos a sus usuarios titulares a favor de otra entidad certificadora, según lo establecido en la Ley 164, previo acuerdo entre ambas entidades certificadoras, con aprobación de la ATT como Entidad Certificadora Raíz.
c) Actualizará la lista del repositorio de los certificados digitales.

d) Emitirá una lista de certificados revocados (CRL) hasta la fecha prevista de cese de actividades.
e) Inmediatamente de revocados los certificados, la ADSIB emitirá una última lista de certificados revocados.
f) La última lista CRL estará disponible para consultas, como mínimo hasta el último día del cese de funciones.

5.9.2.5. Desactivación y custodia de los equipos

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

a) Satisfacer eventuales requerimientos de información, en caso de que suscitaren conflictos.
b) La posible necesidad de rehacer la última lista de certificados revocados.

Después, del periodo de custodia, la ADSIB podrá disponer libremente de los equipos que hubiese dispuesto para el servicio de la certificación digital.
En forma previa a la desactivación se generarán copias de respaldo de toda la información disponible.
Los equipos de publicación de CRL continuarán prestando el servicio hasta la finalización del último día de la fecha del cese de actividades de la ADSIB como Entidad Certificadora, según lo mencionado en el punto "10.2.4.- Revocación de Certificados y Lista de Certificados Revocados" del presente documento.

5.9.2.6. Transferencia de certificados

Al producirse el cese de sus actividades, la ADSIB realizará una transferencia de los certificados emitidos a sus usuarios titulares a favor de otra entidad certificadora, establecido en la Ley 164. Para ello se requerirá un acuerdo previo entre ambas entidades certificadoras, con aprobación de la ATT como Entidad Certificadora Raíz, que deberá ser firmado por las máximas autoridades respectivas.
Dicho acuerdo debe indicar que la Entidad Certificadora continuadora recibirá los certificados y toma a su cargo la administración de la totalidad de los certificados emitidos por la ADSIB que cesa sus actividades, que no hubieran sido revocados a la fecha de la transferencia. Se enviará copias del mencionado acuerdo a la ATT para su archivo.
La ADSIB transferirá a la Entidad Certificadora continuadora toda la documentación que obre en su poder y que hubiera generado en el proceso de emisión y administración de certificados, así como la totalidad de los archivos y copias de resguardo, en cualquier formato y toda otra documentación referida a su operatoria.

5.9.2.7. Procedimientos

Una vez anunciada la fecha del cese de funciones de la ADSIB como Entidad Certificadora Pública, se socializará y comunicará a todo el personal, directa o indirectamente involucrado, sobre las acciones a asumir para el cese de actividades de la Entidad Certificadora Publica - ADSIB.
El Comité de Calidad, Seguridad de la Información y de Emergencia de la Entidad Certificadora ejercerá la supervisión de las operaciones relacionadas, tomando en cuenta el resguardo de la información generada.

5.9.2.8. Resguardo de información histórica

Al finalizar el cese de actividades, la ADSIB deberá resguardar una importante cantidad de información. Los plazos para la conservación de documentos están detallados en el documento de Procedimientos y Condiciones para la conservación de documentos de la Entidad Certificadora.
Asimismo, ADSIB conservará toda la información relacionada con su servicio de certificación digital, detalladas a continuación:

- Los archivos de documentación presentada por solicitantes y suscriptores.
- La documentación relacionada con pedidos de revocación.
- La documentación generada en las ceremonias digitales.
- La última lista de certificados revocados.
- El backup de los servidores y de su configuración.
- Los libros de Actas.

6. Controles de Seguridad Técnica.

6.1. Generación e instalación de par de claves

6.1.1. Generación del par de claves

La ADSIB genera su par de claves (pública y privada) bajo los procedimientos establecidos en la entidad y en cumplimiento de la normativa vigente con respecto a la certificación digital y las regulaciones de la ATT como ente regulador.
El resguardo de la clave privada se desarrolla conforme a la regulación establecida por la ATT.

6.1.2. Entrega de la clave privada y pública a la ADSIB

La ADSIB dispone de los procedimientos para la generación de su propio par de claves pública y privada, por lo que no se realiza la entrega de estos bajo los procedimientos actuales.

6.1.3. Entrega de la clave pública y privada a los usuarios titulares

Las claves serán generadas por el solicitante, utilizando aplicaciones y/o herramientas proveídas por la Agencia de Registro o Entidad Certificadora Autorizada, por lo que la responsabilidad de la clave privada es del usuario titular.

6.1.4. Tamaño de las claves

Los módulos de la raíz de certificación y las claves tienen una longitud de al menos 4096 bits y utiliza el algoritmo RSA.

6.1.5. Parámetros de generación de la clave pública y comprobación de la calidad de los parámetros.

Los parámetros utilizados se basan en el estándar ITU X.509 “Information Technology – Open System Interconnection – The Directory: Public Key and attribute certificate frameworks” y en el RFC 5280.

6.1.6. Hardware y software de generación de claves

El hardware criptográfico para la solicitud de certificados debe estar establecido bajo el criterio de la FIPS 140-2, en el que se establece como nivel de seguridad alto, y el mismo evita todo tipo de manipulaciones, así mismo debe estar homologado por la ATT como ente regulador.

6.1.7. Fines del uso de la clave

La clave privada de la ADSIB como Entidad Certificadora Pública puede ser usado para:

- Firma de certificados establecidos en la presentes Declaración de Prácticas de Certificación.
- Firma de certificados para la firma de lista de revocados CRL y OCSP.
- Firma de certificados para la certificación cruzada.

6.2. Protección de la clave privada

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

6.2.1. Estándares para los módulos criptográficos

Los módulos criptográficos utilizados por la ADSIB cumplen con el estándar FIPS 140-2.

6.2.2. Controles Multipersonales de la clave privada

Se utiliza un control multipersonal para la clave privada, según los roles asignados a los funcionarios de la ADSIB y que participan de las ceremonias de firma de certificados.
El control multipersonal es la implementación de la autenticación M de N, que implica una división de la contraseña de autenticación en múltiples partes o divisiones. La contraseña compartida se distribuye entre varios tokens PED, donde es necesario contar con M=2 de N=4 para poder acceder al par de claves situado en el HSM.
La autenticación M de N permite hacer cumplir el control de acceso multipersona donde ninguna persona pueda acceder al HSM sin la cooperación de otros titulares.

6.2.3. Custodia de la clave privada

La ADSIB posee la clave pública y privada en dispositivos criptográficos seguros certificados por el estándar FIPS 140-2.

6.2.4. Copia de seguridad de la clave privada

La clave privada de la ADSIB está resguardada en módulos HSM protegidos física y lógicamente.

6.2.5. Archivo de la clave privada

La clave privada de la ADSIB se encuentra almacenada en un componente de hardware denominado HSM, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son almacenados, por lo que la ADSIB se asegura mantenerlo en resguardo en un lugar seguro y fuera del Centro de Datos principal.

6.2.6. Introducción de la clave privada al módulo criptográfico

La ADSIB dispone de lineamientos donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico, las mismas se detallan a continuación:

- Se generará el nuevo Módulo de Seguridad.
- Se instalará la ADSIB bajo la modalidad de subordinada y se generará la petición de certificado.
- Se generará el respectivo certificado por parte de la ATT.
- Se instalará y activará el certificado de la ADSIB.

6.2.7. Método de activación de la clave privada

Para la activación de la clave privada es necesario utilizar los dispositivos tokens PED , se requiere dos de los cuatro tokens de administrador y una de dos tokens de Oficiales, adicionalmentees necesario el acceso al sistema operativo del servidor de certificación.

6.2.8. Método de destrucción de la clave privada

Una vez finalizada la firma de certificados el módulo criptográfico y el servidor HSM son desactivados.
La destrucción de la clave privada implica, generalmente, la revocación del certificado correspondiente.
La clave privada será destruida de forma segura conforme a los procedimientos y dentro del HSM, junto con todas las copias de seguridad.

6.2.9. Clasificación de los módulos criptográficos

La ADSIB utiliza un módulo criptográfico para clasificar de forma segura su clave privada.

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

6.3.1. Archivo de la clave pública

La ADSIB realiza la respectiva publicación de su clave pública hasta el vencimiento del último certificado emitido por la misma.

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

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

6.4. Datos de activación

La 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 ADSIB tiene definido una serie de controles de seguridad aplicables a los equipos informáticos, tales como el uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y pruebas de seguridad.
El acceso a los sistemas de la 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 ADSIB usado por la clave pública para la emisión de certificado y el manejo del ciclo de vida ha sido desarrollado de acuerdo con los requerimientos de la Resolución Administrativa de la ATT-DJ-RA TL LP 32/2015.
El HSM utilizado por la clave pública de la ADSIB cumple con los requerimientos FIPS 140-2. Los controles para el manejo de la seguridad se cumplen mediante una separación rígida de los roles del Oficial para cumplir los requerimientos de la política de seguridad establecida durante todo el ciclo de vida de las claves se deben implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la ADSIB.
Existen controles de seguridad para 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 ADSIB son mantenidos “off-line” en una instalación de alta seguridad dentro de un exhaustivo control de seguridad y rigurosos controles de acceso interno.
Se mantiene sistemas de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso. Adicionalmente, la raíz de certificación de la ADSIB se mantiene fuera de línea y no se relaciona con ningún componente externo.

6.8. Controles de los módulos criptográficos.

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

6.9. Sincronización horaria.

El gabinete de la firma digital de la ECP que contiene la infraestructura de clave pública se mantiene “off-line”, por lo que, la sincronización permanente en línea de la hora no se lleva acabo.

7. Perfil de los Certificados Digitales para CRL y OCSP.

7.1. Perfil de Certificado de tipo Persona Natural

7.1.1. Formato para Certificado Digital persona natural

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

NOMBRE	DESCRIPCIÓN
Versión (version)	2
Número de Serie (serialNumber)	Número asignado por la ECP
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer)	**CN** = "Entidad Certificadora" y el nombre de la ECA; **O** = Razón social de la ECA; **C**=BO (de acuerdo a ISO3166).
Periodo de validez (validity)	Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	**CN** = Nombres y Apellidos de la persona natural; **C** = estándar de acuerdo 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).
Clave pública del suscriptor (subjectPublicKey)	Algoritmo: RSA, Longitud: mínimo 2048 bits

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 ECP - 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)
Restricciones Básicas (basicConstraints)	CA = FALSE
Punto de distribución de las CRL (cRLDistributionPoints)	URI: (.crl)
Información de Acceso de la ECA (authorityInformationAccess)	URI:(.crt)
Nombre Alternativo del Suscriptor (subjectAlternativeName)	E = Correo electrónico del suscriptor

7.2. Perfiles de la CRL

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

NOMBRE	VALOR
Versión (version)	1 (corresponde a la versión 2 del estándar)
Algoritmo de firmas (signa-tureAlgorithm)	Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Pública para firmar la Lista de Certificados Revocados

Nombre del Emisor (issuer)	CN = “Entidad Certificadora ADSIB”; O = “ADSIB”; C = “BO”.
Día y Hora de Vigencia (This Update)	Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
Próxima actualización (Next Update)	Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
Certificados Revocados (Revoked Certificates)	contiene la lista de certificados revocados, identificados mediante su número de serie, la fecha de revocación y una serie de extensiones específicas

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

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

7.3. Perfiles de la OCSP

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

1. El requerimiento de inclusión de los siguientes datos en las consultas OCSP:
   a) Versión (version)
   b) Requerimiento de servicio (service request).
   c) Identificador del certificado bajo consulta (target certificate identifier).
   d) Extensiones que puedan incluirse en forma opcional (optionals extensions) para su procesamiento por quien responde. Cuando se recibe una consulta OCSP, quien responde debe considerar al menos los siguientes aspectos:
      1. Que el formato de la consulta sea el apropiado

2. Que el emisor sea una entidad autorizada para responder la consulta.
3. Que la consulta contenga la información que necesita quien responde
4. Si estas condiciones son verificadas, se devuelve una respuesta. De lo contrario, si alguna de estas condiciones no se cumpliera, se deberá emitir un mensaje de error.

2. Cuando se emite una respuesta OCSP, se sugiere requerir que se consideren los siguientes datos:
   a) Versión.
   b) Identificador de la Entidad Certificante Autorizada o de la entidad habilitada que emite la respuesta.
   c) Fecha y hora correspondiente a la generación de la respuesta.
   d) Respuesta sobre el estado del certificado.
   e) Extensiones opcionales.
   f) Identificador de objeto (OID) del algoritmo de firma.
   g) Firma de respuesta.

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

Las respuestas OCSP están firmadas digitalmente por la ADSIB como Entidad Certificadora Pública 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 de tipo de dertificado Persona Natural” corresponde a la ADSIB como Entidad Certificadora Pública.

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

8.1. Procedimiento para cambio de especificaciones

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

En caso de que la ADSIB desee 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 de tipo de certificado Persona Natural", 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 ADSIB como ECP 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 ADSIB deberá notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación. De la misma forma, la ADSIB deberá publicar en su sitio web cualquier modificación aprobada por la ATT y notificar a los usuarios finales de los cambios realizados en caso de ser necesario.

9. Otras cuestiones legales y de actividad.

9.1. Contrato de adhesión.

Los certificados emitidos por la Entidad Certificadora Publica – ADSIB, están asociados 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.

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 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 la página de la ADSIB.

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.

9.2.2. Reembolso

La Entidad Certificadora Publica, realizará reembolsos por aquellos servicios no prestados, considerando los siguientes aspectos:

- No haber recibido el servicio de certificado digital en los plazos establecidos; considerando que el solicitante haya cumplido con los requisitos establecidos para la obtención del certificado digital.
- No se haya emitido el certificado digital.

Todos los pagos relacionados a la emisión de un Certificado Digital de tipo Persona Natural, estarán vigente mientras la solicitud en el sistema de agencia de registro sea válida. Cuando la solicitud expire automáticamente después de tres días, el monto cancelado por el servicio pasará a formar parte de depósitos no identificados.

Los depósitos no identificados, después de los tres (3) meses, pasarán a favor de la ADSIB, los mismos se publicarán en el sitio web de la ADSIB, hasta cumplido el plazo establecido.

9.3. Política de confidencialidad.

Toda la recopilación y uso de la información compilada por la 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 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) El uso 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 con las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.

La 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 Publica.

9.6.1.1. Derechos de la Entidad Certificadora Publica

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

a) Recibir oportunamente el pago por los servicios provistos, de conformidad con los precios o tarifas 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 Publica

De conformidad a lo establecido en el Artículo 59 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, la Entidad Certificadora Pública tiene las siguientes obligaciones:

a) Someterse a la jurisdicción y competencia de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
b) Proveer en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida, los servicios de telecomunicaciones y tecnologías de información y comunicación.
c) Proporcionar información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a las usuarias o los usuarios.
d) Proporcionar información clara, precisa, cierta, completa y oportuna a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

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 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 Publica 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 31/2015** 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 signatario 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 naturales 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 ADSIB, la entidad no podrá acceder en ningún momento a la clave privada del usuario, por lo que éste es el único responsable de su generación, administración, uso y custodia. En caso de verse comprometida por cualquier razón dicha clave, el usuario deberá informar a la ADSIB a la brevedad posible y solicitar 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 de la firma 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.

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 con 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:

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

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

La 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 Declaración de Prácticas de Certificación de la ECP.
b. Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT.
c. Publicar la Declaración de Prácticas de Certificación y las Políticas de Certificación en la página de la ADSIB.
d. Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, remisión, tarifas y uso vigentes establecidos para sus certificados digitales, el mismo que está publicado en la página web de la ADSIB.
e. Informar sobre las modificaciones aprobadas de esta Política de Certificación de persona natural, mediante la publicación de éstas y sus respectivas modificaciones en la página web de la ADSIB.

f. Revocar el certificado digital al producirse alguna de las causales establecidas en la presente Política de Certificación de tipo Persona Natural.
g. Mantener la información relativa a los certificados digitales emitidos, por un periodo mínimo de 5 (cinco) años posteriores al periodo de vigencia.

9.8. Infracciones y Sanciones.

Las infracciones y sanciones son establecidos por la Autoridad que regula el servicio que brinda la ADSIB como ECP.

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 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 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 ADSIB no tendrá en ningún momento acceso a la clave privada de los titulares, por lo mismo se exime 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 ECP 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 se consideran para la elaboración del presente documento:

- **ATT-DJ-RA TL LP 31/2015,** Documentos Públicos de la Entidad Certificadora Raíz.
- **ATT-DJ-RA TL LP 32/2015,** Requisitos y otros aspectos para la prestación del servicio de Certificación Digital.
- **ATT-DJ-RA TL LP 1538/2015,** Modificación a la RAR ATT-DJ-RA TL LP 32/2015.
- **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 de tipo de Persona Natural 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	11/2018	• Elaboración del documento considerando la elaboración de Políticas separadas por tipo de certificado				