

## **DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA ECP**

ADSIB-FD-POLT-005    Unidad de Gestión de Servicios

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

## DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA ECP

### Contenido

1.Introducción.....	5
1.1.Presentación.....	5
1.1.1.Propósito.....	5
1.1.2.Descripción de la Entidad Certificadora.....	5
1.2.Identificación y nombre del documento.....	6
1.3.Participantes de la Infraestructura Nacional de Certificación Digital del Estado.....	6
1.3.1.Primer nivel: Entidad Certificadora Raíz.....	6
1.3.2.Segundo Nivel: Entidad de Certificación.....	7
1.3.3.Tercer nivel: Agencia de Registro.....	7
1.3.4.Cuarto nivel: Signatarios.....	7
1.4.Uso de los certificados.....	7
1.4.1.Usos Permitidos de los Certificados.....	7
1.4.2.Restricciones en el Uso de los Certificados.....	8
1.4.3.Fiabilidad de la firma digital a lo largo del tiempo.....	8
1.5.Administración de la Declaración de Prácticas de Certificación.....	8
1.6.Definiciones y abreviaturas.....	9
1.6.1.Abreviaturas.....	9
1.6.2.Definiciones.....	10
2.Publicación de información y del repositorio.....	11
2.1.Repositorio.....	11
2.2.Repositorio CRL.....	11
2.3.Servicio OCSP.....	12
2.4.Términos y condiciones.....	12
2.5.Políticas de Certificación.....	12
2.6.Declaración de prácticas.....	12
2.7.Publicación.....	12
2.8.Frecuencia de actualización.....	12
2.9.Controles de acceso al repositorio.....	13
3.Identificación y Autenticación de los usuarios titulares de los certificados.....	13
3.1.Registro de nombres.....	13
3.1.1.Tipos de nombres.....	13
3.1.2.Significado de los nombres.....	13
3.1.3.Interpretación de formatos de nombres.....	13
3.1.4.Unicidad de nombres.....	13
3.1.5.Resolución de conflictos relativos a nombres.....	14
3.2.Validación de la identidad inicial.....	14
3.2.1.Métodos de prueba de posesión de la clave privada.....	14
3.2.2.Autenticación de la identidad de una organización.....	14
3.2.3.Autenticación de la identidad del solicitante.....	14
4.Ciclo de Vida de los Certificados.....	15



4.1.Requisitos para la obtención de un Certificado Digital .....	15
4.1.1.Requisitos documentales.....	15
4.1.2.Requisitos Técnicos para Acceder al Servicio .....	15
4.2.Solicitud del Certificado .....	16
4.3.Tramitación de solicitud de certificado.....	16
4.4.Emisión del certificado .....	18
4.5.Aceptación del certificado .....	19
4.6.Uso del certificado y del par de claves .....	19
4.7.Renovación del certificado digital .....	19
4.8.Reemisión del Certificado Digital .....	20
4.9.Revocación del Certificado.....	21
4.9.1.Revocación Presencial .....	22
4.9.2.Revocación telefónica.....	23
4.9.3.Revocación en línea a través del Sistema de AR .....	23
4.9.4.Revocación vía correo electrónico.....	23
4.10.Servicio de estado de los certificados .....	24
4.11.Finalización de la suscripción.....	24
4.12.Recuperación de la clave. ....	24
5.Controles de seguridad física, gestión y de operaciones.....	24
5.1.Controles de seguridad física.....	24
5.1.1.Ubicación y construcción.....	24
5.1.2.Acceso físico.....	25
5.1.3.Alimentación eléctrica y aire acondicionado .....	25
5.1.4.Exposición al Agua .....	25
5.1.5.Protección y prevención de incendios.....	26
5.1.6.Sistema de almacenamiento.....	26
5.1.7.Eliminación de residuos.....	26
5.1.8.Copia de Seguridad.....	26
5.2.Controles de procedimiento .....	26
5.2.1.Roles de confianza .....	26
5.2.2.Número de personas requerida por tarea .....	27
5.2.3.Identificación y autenticación para cada rol. ....	27
5.3.Controles de seguridad del personal .....	27
5.3.1.Requerimientos de antecedentes, calificación, experiencia y acreditación.....	27
5.3.2.Procedimientos de comprobación de antecedentes.....	27
5.3.3.Formación y frecuencia de actualización de la formación.....	27
5.3.4.Frecuencia y secuencia de rotación de tareas.....	27
5.3.5.Sanciones por acciones no autorizadas .....	27
5.3.6.Requerimientos de contratación de personal, controles periódicos de cumplimiento, finalización de los contratos. ....	28
5.4.Procedimientos de Control de Seguridad.....	28
5.4.1.Tipos de eventos registrados .....	28
5.4.2.Frecuencia de procesado de logs.....	28
5.4.3.Periodo de retención para los logs de auditoría .....	29
5.4.4.Protección de los logs de auditoría .....	29



5.4.5.Procedimientos de copia de seguridad de los logs de auditoría.....	29
5.4.6.Sistema de recogida de información de auditoría .....	29
5.4.7.Notificación al sujeto causa del evento.....	29
5.4.8.Análisis de vulnerabilidades .....	29
5.5.Archivo de información y registros .....	29
5.5.1.Tipo de información y eventos registrados .....	30
5.5.2.Periodo de retención para el archivo.....	30
5.5.3.Sistema de recogida de información para auditoría .....	30
5.5.4.Procedimientos para obtener y verificar información archivada .....	30
5.6.Cambio de clave de la ADSIB .....	30
5.7.Recuperación de la clave de la ADSIB .....	31
5.8.Procedimientos para recuperación de desastres .....	31
5.9.Cese de actividades de la Entidad Certificadora Pública ADSIB .....	31
5.9.1.Sujetos involucrados.....	31
5.9.2.Procedimiento para el cese de actividades.....	31
6.Controles de Seguridad Técnica. ....	34
6.1.Generación e instalación de par de claves .....	34
6.1.1.Generación del par de claves .....	34
6.1.2.Entrega de la clave privada y pública a la ADSIB .....	34
6.1.3.Entrega de la clave pública y privada a los usuarios titulares.....	34
6.1.4.Tamaño de las claves .....	34
6.1.5.Parámetros de generación de la clave pública y comprobación de la calidad de los parámetros. ....	34
6.1.6.Hardware y software de generación de claves .....	35
6.1.7.Fines del uso de la clave .....	35
6.2.Protección de la clave privada .....	35
6.2.1.Estándares para los módulos criptográficos.....	35
6.2.2.Controles Multipersonales de la clave privada .....	35
6.2.3.Custodia de la clave privada .....	35
6.2.4.Copia de seguridad de la clave privada.....	36
6.2.5.Archivo de la clave privada .....	36
6.2.6.Introducción de la clave privada al módulo criptográfico .....	36
6.2.7.Método de activación de la clave privada.....	36
6.2.8.Método de destrucción de la clave privada.....	36
6.2.9.Clasificación de los módulos criptográficos .....	36
6.3.Otros aspectos de la gestión del par de claves. ....	37
6.3.1.Archivo de la clave pública.....	37
6.3.2.Períodos operativos de los certificados y período de uso para el par de claves.....	37
6.4.Datos de activación.....	37
6.5.Controles de seguridad informática .....	37
6.6.Controles de seguridad del ciclo de vida .....	37
6.7.Controles de seguridad de la red.....	38
6.8.Controles de los módulos criptográficos.....	38
6.9.Sincronización horaria. ....	38
7.Perfiles de Certificado y de la lista de certificados revocados.....	38
7.1.Perfil del Certificado de la Entidad Certificadora Raíz (ECR).....	38



7.2.Perfil del Certificado de la Entidad Certificadora Pública ADSIB .....	39
7.3.Perfil de la CRL de la Entidad Certificadora Pública .....	41
7.4.Perfil del OCSP de la Entidad Certificadora Pública.....	41
8.Auditoría de Conformidad. ....	42
8.1.Frecuencia de los controles de conformidad para la ADSIB .....	43
8.2.Relación entre el auditor y la entidad auditada. ....	43
8.3.Comunicación de resultados. ....	43
9.Otras cuestiones legales y de actividad.....	43
9.1.Contrato de adhesión. ....	43
9.2.Tarifas. ....	43
9.3.Política de confidencialidad.....	44
9.4.Ámbito de la Información confidencial. ....	44
9.5.Protección de Datos Personales. ....	44
9.6.Derechos y Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital .....44	
9.6.1.Derechos y Obligaciones de la Entidad Certificadora Pública. ....	44
9.6.2.Derechos y Obligaciones de los Titulares del Certificado Digital .....	47
9.6.3.Derechos y Obligaciones de los Usuarios.....	48
9.7.Obligaciones de los participantes de la Infraestructura Nacional de Certificación Digital. ....	50
9.8.Modificaciones al presente documento.....	50
9.9.Resolución de Conflictos. ....	50
9.10.Legislación aplicable. ....	51
9.11.Conformidad con la ley aplicable. ....	51
10.VERSIONES: .....	52



# DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA ECP

## 1. Introducción

### 1.1. Presentación

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia ADSIB es una entidad que fue creada mediante Decreto Supremo N.º 26553, de fecha 19 de marzo de 2002, como entidad descentralizada, bajo tuición de la Vicepresidencia, con independencia de gestión administrativa y técnica, sujeta a la Ley N.º 1178 – SAFCO.

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, de acuerdo a la Ley N.º 164 de 08/08/2011 que establece que la ADSIB prestará el servicio de certificación para el sector público y la población en general a nivel nacional, por lo que se realizaron las gestiones para que la ATT autorizara el funcionamiento de la ADSIB como Entidad Certificadora Pública.

En fecha 5 de febrero de 2016 la ADSIB firma Contrato ATT-DJ-CON SCD 1/2016 de 05/02/2016 con la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, donde se autoriza la prestación de servicios de certificación digital a la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

La Declaración de prácticas es un instrumento que describe las reglas y procedimientos específicos para brindar el servicio de certificación digital.

La ADSIB contempla la emisión de distintos tipos de certificados, descritos en el documento “Política de Certificación”.

#### 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 Jaime Mendoza No 981 Zona San Miguel - La Paz Bolivia, así mismo, las dependencias de su Centro de Procesamiento de Datos se encuentran en instalaciones del edificio de la Vicepresidencia, en la parte del subsuelo.

La Entidad Certificadora Pública ADSIB tiene las siguientes funciones:

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

## **1.2. Identificación y nombre del documento.**

Este documento se titula “Declaración de Prácticas de Certificación”. La fecha de entrada en vigor de este documento es a partir de su aprobación por Resolución Administrativa de la Entidad Certificadora Pública ADSIB y permanece vigente hasta la liberación de una nueva versión que será notificada a los interesados.

Nombre:	Declaración de Practicas de Certificación (DPC)
Versión:	2.1
Descripción:	Declaración de Prácticas de Certificación de la Entidad Certificadora Pública ADSIB
Fecha de emisión:	Octubre 2020
OID	2.16.68.0.0.0.1.14.1.2.0.1.0.1
Localización	<a href="https://firmadigital.bo/ecpadsib.pdf">https://firmadigital.bo/ecpadsib.pdf</a>

## **1.3. Participantes de la Infraestructura Nacional de Certificación Digital del Estado**

La Jerarquía Nacional de Certificación Digital, según el Artículo N.º 36 del Decreto Supremo N° 1793, establece los niveles de la Infraestructura Nacional de Certificación Digital (INCD), misma que será descrita a continuación:

### **1.3.1. Primer nivel: Entidad Certificadora Raíz**

La ATT es la entidad de certificación de nivel superior dentro de la Infraestructura Nacional de Certificación Digital que auto firma su certificado y emite certificados digitales a las entidades certificadoras públicas y privadas subordinadas.



### 1.3.2. Segundo Nivel: Entidad de Certificación

Son las Entidades Certificadoras Pública o Privadas subordinadas de la Entidad Certificadora Raíz. La entidad certificadora pública es la ADSIB y las entidades certificadoras privadas, son todas aquellas autorizadas por la ATT para prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

La Entidad Certificadora Pública ADSIB elaboró los documentos públicos y privados exigidos por la entidad reguladora ATT. Así mismo establece los precios y promociones que se pueden aplicar al servicio de emisión de Certificados Digitales.

### 1.3.3. Tercer nivel: Agencia de Registro

Es la agencia dependiente de una entidad certificadora, encargada de realizar el registro y la identificación del futuro titular del Certificado Digital en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además, es quien se encarga de solicitar la emisión o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital.

### 1.3.4. Cuarto nivel: Signatarios

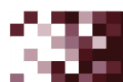
También denominados Usuarios titulares, son todos los usuarios y usuarias titulares de un certificado digital emitido por una entidad certificadora autorizada dentro de la INCD y que firman documentos digitalmente.

## 1.4. Uso de los certificados.

### 1.4.1. Usos Permitidos de los Certificados

La Entidad Certificadora Pública ADSIB emite certificados digitales para firmar las listas de certificados revocados (CRL) y Firmar las respuestas que emite el protocolo de comprobación del Estado de un Certificado (OCSP). Los usos de ambos certificados emitidos por la Entidad Certificadora Pública ADSIB se detallan a continuación:

TIPOS DE CERTIFICADO	USO
Lista de Revocación de Certificado (CRL)	Firma de Lista de Revocación de Certificados
Protocolo de comprobación del Estado de un Certificado (OCSP)	Firma las respuestas OCSP
Adicionalmente la Entidad Certificadora Pública ADSIB emite diferentes tipos de Certificados Digitales	





cuyo uso será limitado por la presente “Declaración de Prácticas” y por el documento “Políticas de Certificación” y otros documentos que sean emitidos por autoridades competentes.

#### **1.4.2. Restricciones en el Uso de los Certificados.**

La restricción de uso se establece bajo los criterios presentes en la sección anterior, considerando además la exclusión en su validez jurídica de los actos descritos en el artículo 79 de la Ley N.º 164:

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

Queda expresamente indicado que cualquier violación a las normas, usos y/o leyes del Estado Plurinacional de Bolivia está bajo la responsabilidad del usuario titular del Certificado, así como los daños y perjuicios que ocasionare. La ADSIB cumple su responsabilidad al momento de la emisión del Certificado Digital, a partir de ese momento, toda acción es responsabilidad del usuario titular.

Adicionalmente, en caso de incumplimiento de las responsabilidades, le será revocado el certificado digital y el usuario titular del certificado asume la responsabilidad de indemnizar a la Entidad Certificadora Pública ADSIB por daños y perjuicios ocasionados a terceros derivados de reclamos, acciones, efectos de acción, pérdidas o daños (incluyendo multas legales) que se generaren por el uso indebido, por parte del usuario titular del servicio contratado con ADSIB, de acuerdo a lo establecido por el ente regulador ATT u otras entidades competentes.

#### **1.4.3. Fiabilidad de la firma digital a lo largo del tiempo.**

La validez de la firma digital está garantizada cuando el documento fue firmado con un certificado vigente dentro de la INCD. Para validar documentos firmados digitalmente se tiene la siguiente dirección:

<https://validar.firmadigital.bo/>

#### **1.5. Administración de la Declaración de Prácticas de Certificación.**

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

Cuando la Entidad Certificadora Pública ADSIB realice modificaciones a la presente “Declaración de Prácticas 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
- Fax: (591-2) 2200740

## 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.
- **ECA:** Entidad Certificadora Autorizada.
- **ECR:** Entidad Certificadora Raíz.
- **ECP:** Entidad Certificadora Pública
- **HSM:** (Hardware Security Module) Módulo de Hardware de Seguridad<sup>1</sup>.
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **INCD:** Infraestructura Nacional de Certificación Digital.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.
- **NIT:** Número de Identificación Tributaria emitido por el Servicio de Impuestos Nacionales.
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RFC:** (Request For Comments<sup>2</sup>) 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.

<sup>1</sup>Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas

<sup>2</sup>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

- **Autenticación:** Proceso técnico de verificación por el cual se garantiza la identidad del signatario en un mensaje electrónico de datos o documento digital, que contenga firma digital.
- **Certificado Digital:** Es un archivo digital firmado digitalmente por una entidad certificadora autorizada que incluye datos que permiten identificar al titular del certificado, a la entidad certificadora que lo emitió, el periodo de vigencia e información necesaria para verificar la firma digital.
- **Par de claves:** Es el conjunto de la clave privada y la clave pública. Las dos claves se generan al mismo tiempo por el mismo mecanismo criptográfico. Estas dos claves son complementarias, y para cualquier operación que implique el uso de una de las dos claves, se necesita la segunda clave para cumplir la operación.
- **Clave privada:** Conjunto de caracteres alfanuméricos generados mediante un sistema de cifrado que contiene datos únicos que el signatario emplea en la generación de una firma electrónica o digital sobre un mensaje electrónico de datos o documento digital.
- **Clave pública:** Conjunto de caracteres de conocimiento público, generados mediante el mismo sistema de cifrado de la clave privada; contiene datos únicos que permiten verificar la firma digital del signatario en el Certificado Digital.
- **Firma digital:** Es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración. Este tipo de Firma tiene validez legal desde el año 2011.
- **Firma Digital Automática:** Firma digital generada en forma desatendida o automática por un sistema informático, el titular del certificado digital delega el uso de su certificado para tareas definidas.
- **Nivel de seguridad:** En caso de que el par de claves sea generado por un dispositivo criptográfico basado en hardware, el certificado tendrá nivel de seguridad alto, en caso de que el par de claves sea generado por software tendrá nivel de seguridad normal.
- **Solicitud de firma de certificado:** Una solicitud de firma de certificado (en inglés Certificate Signing Request - CSR) es un archivo digital que un solicitante transmite a una Entidad Certificadora para obtener la firma de su certificado. La solicitud de firma de certificado contiene los datos de identidad y la clave pública del solicitante, y está firmada con la clave privada del solicitante para certificar que la solicitud es auténtica.
- **Infraestructura de clave pública:** La infraestructura de clave pública es el conjunto de todas las entidades certificadoras y usuarios de los certificados digitales y de las relaciones entre estos actores. Una infraestructura de clave pública es organizada de manera jerárquica, encabezada por una entidad certificadora raíz con certificado auto-firmado, y por debajo entidades certificadoras que emiten certificados para los usuarios. Todos los certificados emitidos en una infraestructura de clave pública pueden ser validados siguiendo un camino lógico hasta la entidad certificadora raíz, en la cual está depositada la confianza en la infraestructura de clave pública. En el caso de la infraestructura de clave pública de Bolivia, la Entidad Certificadora Raíz es la ATT, y la Entidad Certificadora Pública es la ADSIB.
- **Módulo criptográfico basado en hardware:** Es un dispositivo de seguridad basado en hardware (Por ejemplo, HSM, token o smartcard) que genera, almacena y protege claves criptográficas. Los dispositivos criptográficos deberán estar homologados por la ATT.



- **Usuario titular:** El usuario titular para el servicio de certificación digital de la Entidad Certificadora Pública ADSIB es la persona física poseedora del certificado digital y, en consecuencia, tendrá los derechos de revocación, reemisión y renovación sobre el certificado. El certificado puede ser de persona natural o persona jurídica.
- **Usuario corporativo:** Entidades públicas o privadas que establecen un vínculo contractual o de convenio con la Entidad Certificadora Pública ADSIB, para las operaciones sobre certificados digitales de su personal interno se les habilitará cuentas corporativas.
- **Lista de certificados revocados:** Una lista de revocatoria de certificados (en inglés Certificate Revocation List - CRL) es un archivo digital que contiene una lista de certificados revocados. La revocatoria de un certificado corresponde a revocar su validez, por algún motivo, antes de su fecha de expiración. La lista de revocatoria de certificados está firmada por una autoridad reconocida dentro de la infraestructura de clave pública. En el caso de la Entidad Certificadora Pública ADSIB, la lista de revocatoria está firmada con un par de claves y un certificado dedicados de la ADSIB.
- **Emisión de Certificados:** La Entidad Certificadora Pública ADSIB emitirá los certificados que se soliciten a través de una Agencia de Registro autorizada mediante un CSR; las solicitudes son remitidas una vez que el Oficial de Registro de la Agencia de Registro haya comprobado el cumplimiento de los requisitos.
- **Repositorio:** Es el lugar en el sitio web donde se publican los documentos relacionados al servicio de certificación digital, así como los servicios relacionados que se encargan de comprobar el estado de los certificados

## 2. Publicación de información y del repositorio

### 2.1. Repositorio

La Entidad Certificadora Pública ADSIB mantiene un repositorio público de información en el sitio web:

<https://firmadigital.bo/>

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

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

### 2.2. Repositorio CRL

El Repositorio con la lista de certificados revocados (CRL) se encuentra en:

[https://firmadigital.bo/firmadigital\\_bo.crl](https://firmadigital.bo/firmadigital_bo.crl)



### **2.3. Servicio OCSP**

El servicio de consulta o Protocolo de comprobación del Estado de un Certificado en línea (OCSP) se encuentra en:

<https://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/assets/terminos.pdf>

### **2.5. Políticas de Certificación**

La Entidad Certificadora Pública ADSIB, tiene un documento denominado “Políticas de Certificación”.

### **2.6. Declaración de prácticas**

La Declaración de Prácticas de Certificación se encuentran en:

<https://firmadigital.bo/ecpadsib.pdf>

### **2.7. Publicación**

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

- Los certificados digitales de la Entidad Certificadora Pública, Entidad Certificadora Raíz 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 compuestos por el presente documento y la Política de Certificación de los diferentes tipos de certificados. 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 alterar la información (al incluir, actualizar o eliminar datos).

## **3. Identificación y Autenticación de los usuarios titulares de los certificados.**

A continuación, se describen los procedimientos y criterios aplicados por la Entidad Certificadora Pública ADSIB para las Agencias de Registro en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado digital.

### **3.1. Registro de nombres**

#### **3.1.1. Tipos de nombres**

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

En el documento “Políticas de Certificación” se especifican los atributos que conforman el Distinguished Name (DN).

#### **3.1.2. Significado de los nombres**

Los usuarios que requieran el servicio deberán suscribirse (crear cuenta en el sistema de Agencia de Registro) al servicio de certificación digital con sus nombres y apellidos completos conforme fueron registrados en el SEGIP. Únicamente se consideran los nombres y apellidos (primero y segundo) como atributos para definir la identidad de un usuario titular.

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 a algún usuario. En caso de que el titular pertenezca a una población indígena serán considerados los nombres que figuran en el documento de identidad.

#### **3.1.3. Interpretación de formatos de nombres**

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

#### **3.1.4. Unicidad de nombres**

Se garantiza que los nombres (campo DN) 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 dos identidades cuando existan problemas de duplicidad de nombres (homónimos). Así mismo en el documento “Políticas de Certificación” se establece el contenido del campo DN, que garantiza que los certificados sean únicos.

### **3.1.5. Resolución de conflictos relativos a nombres**

En el caso de una ocurrencia de conflicto de nombres o duplicidad en la identidad debe ser resuelto ante el SEGIP.

## **3.2. Validación de la identidad inicial**

### **3.2.1. Métodos de prueba de posesión de la clave privada**

La Entidad Certificadora Pública ADSIB, previo a la emisión del certificado digital, requiere que el solicitante de un tipo de certificado genere su clave pública y clave privada mediante un procedimiento que garantice su confidencialidad y su vinculación con la identidad del solicitante.

El futuro usuario titular del certificado digital es la única persona autorizada para crear su propio par de claves (clave privada y clave pública), la clave privada permanece exclusivamente en posesión del titular del certificado y en ningún momento es conocida por la ADSIB, mientras que la clave pública si es conocida por ADSIB porque debe ir contenida en el certificado a emitir. Los Oficiales de Registro de cada Agencia de Registro autorizada podrán apoyar en el proceso de creación del par de claves, asesorando en el manejo de los sistemas para tal fin.

El método utilizado para comprobar que el solicitante posee la clave privada que corresponde a la clave pública, para la que se solicita se emita el certificado digital, será probado mediante el envío del CSR en el cual se incluye la clave pública y está firmada por la clave privada asociada.

La Entidad Certificadora Pública ADSIB emitirá los certificados de acuerdo a estructura aprobada por la ATT en base a la información ingresada por el usuario solicitante.

### **3.2.2. Autenticación de la identidad de una organización**

La Entidad Certificadora Pública ADSIB emite Certificados digitales a nombre de un titular o persona, de acuerdo al tipo de certificado el mismo contendrá los datos referidos a la organización si corresponde.

Cualquier organización puede solicitar un certificado digital para su o sus representantes y que ellos puedan firmar a nombre de la organización, en este caso se procede a la autenticación de la identidad de la persona y registrar los datos de la organización.

### **3.2.3. Autenticación de la identidad del solicitante**

Durante el registro, las Agencias de Registro son las encargadas de verificar la información primaria del titular a través de sistemas implementados con servicios de interoperabilidad con el SEGIP y con cualquier otra entidad que se vea conveniente.



Las Agencias de Registro se reservan el derecho de rechazar la solicitud de un certificado si consideran que la documentación presentada no es suficiente para autenticar la identidad del solicitante.

Para emitir un certificado se exige la verificación de los datos del titular, para demostrar su identidad de la siguiente forma:

- Documento de identidad vigente y original para contrastar los datos con el SEGIP.
- Toma de Fotografía para verificación visual con documento de identidad.
- Captura de huella dactilar para verificación de identidad a través de datos biométricos.

Los requisitos específicos para cada tipo de Certificado Digital están detallados en el documento “Políticas de Certificación”.

Además, toda información suministrada en la solicitud de emisión de certificado a través del sistema será revisada por el Oficial de Registro, quien se encargará de verificar que la información sea original, suficiente y adecuada de acuerdo con los procedimientos internos definidos.

## 4. Ciclo de Vida de los Certificados

### 4.1. Requisitos para la obtención de un Certificado Digital

#### 4.1.1. Requisitos documentales

Cada tipo de certificado tiene sus propios requisitos que se encuentran detallados el documento “Políticas de Certificación”. Las Agencias de Registro tienen la obligación de verificar el cumplimiento de los requisitos.

Los documentos requeridos pueden ser cargados en el Sistema de Agencia de Registro o pueden ser presentados ante un Oficial de Registro de una Agencia de Registro, para que pueda brindar apoyo para cargarlos en el sistema.

#### 4.1.2. Requisitos Técnicos para Acceder al Servicio

Para que un usuario pueda acceder al servicio de certificación digital deberá:

- Contar con acceso a Internet.
- Darse de alta como usuario en el sistema de Agencia de Registro
- En función al nivel de seguridad del certificado a solicitar, deberá contar con:
  - Para Certificados Digitales con **Seguridad alta**: Dispositivo de seguridad (HSM, token o tarjetas inteligentes – smartcards) que cumplan con el estándar FIPS 140-2. Los modelos deberán estar en la lista de dispositivos homologados por la ATT, misma que se encuentra en su respectivo sitio web. En el dispositivo de seguridad es donde se generarán el par de claves para realizar la solicitud.
  - Para Certificados Digitales con **Seguridad Normal**: Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 845/2018, que esté homologado por la ATT. El usuario debe estar consciente de que el par de claves se almacena en





el contenedor de software donde realiza la solicitud, y el certificado una vez generado debe almacenarse junto a la clave privada para permitir la firma de documentos. 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:

<http://firmadigital.bo/>

## 4.2. Solicitud del Certificado

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

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

- **Firma Digital Simple:** cuando el usuario titular administra el certificado para cada una de las firmas a realizar.
- **Firma Digital Automática:** cuando la firma digital se realiza a través de un sistema informático, donde el titular del certificado delega su uso para tareas definidas en éste.

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

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

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

## 4.3. Tramitación de solicitud de certificado

El usuario titular podrá realizar la solicitud a través del Sistema de Agencia de Registro. También puede realizar la solicitud de manera presencial en cualquier Agencia de Registro con ayuda de un Oficial de Registro.

Las Agencias de Registro brindarán mínimamente la siguiente información necesaria sobre los procesos y procedimientos para la solicitud de certificados digitales:

- Documentación necesaria que deben presentar para el procedimiento de obtención de certificado digital y para autenticar la identidad del solicitante.
- Información sobre los procesos y procedimientos de emisión, revocación, reemisión y renovación del certificado digital, así como las condiciones de uso.
- El acceso a los documentos normativos vigentes, al presente documento y a la Políticas de Certificación.



Para iniciar el proceso de solicitud de emisión de certificado digital, el usuario solicitante deberá disponer de una cuenta en el sistema de Agencia de Registro, con todas las validaciones necesarias requeridas por la normativa vigente.

El usuario elegirá la Agencia de Registro y solicitará mediante el sistema el tipo de certificado digital requerido.

El documento “Políticas de Certificación” especifica la documentación adicional requerida para la solicitud de los mismos. El usuario deberá presentar los requisitos establecidos de acuerdo con el tipo de certificado solicitado.

El usuario deberá crear su par de claves y enviar su clave pública a través de mecanismos que garanticen que el procedimiento es seguro. Si el usuario no supiera realizar la operación, los Oficiales de Registro le proporcionarán el soporte necesario, mismo que podrá ser realizado en cualquier Agencia de Registro autorizada siempre y cuando se utilice un Token o Smartcard como medio de almacenamiento del Certificado; en caso de Certificados almacenados en un contenedor de Software o en un HSM, la responsabilidad de la generación del par de claves es del usuario solicitante.

La Entidad Certificadora Pública ADSIB pone a disposición de sus usuarios dos herramientas para la generación del par de claves y la gestión del Software:

- Para certificados con nivel de seguridad alto, almacenados en un dispositivo criptográfico Token, se pone a disposición la herramienta Jacobitus-FIDO, que se encuentra en el siguiente enlace:

<https://firmadigital.bo/herramientas/>

- Para certificados con nivel de seguridad normal, almacenados en un archivo (contenedor PKCS#12), se pone a disposición la herramienta Jacobitus-SOFT, que se encuentra en el siguiente enlace:

<https://firmadigital.bo/software/>

En ningún caso los Oficiales de Registro podrán intervenir en la generación del par de claves del usuario, debido a que constituye una acción privada.

Las distintas Agencias de Registro deben asegurarse que los usuarios solicitantes han sido plenamente identificados y que la petición de certificado es verificada y completa. Para ello, la Agencia de Registro podrá disponer de diferentes medios para realizar la respectiva verificación de documentos, validación de identidad y registro de foto. El solicitante asume la responsabilidad por la veracidad y exactitud de la información proporcionada y presentada en el sistema y al Oficial de Registro para la solicitud del certificado.

La Agencia de Registro debe realizar un proceso de validación de la identidad del solicitante a través de servicios de interoperabilidad, además de la verificación de cumplimiento de requisitos y verificación del pago correspondiente.

El Oficial de Registro una vez verificada la solicitud, envía el CSR firmado digitalmente a la Entidad



Certificadora Pública ADSIB.

El Oficial de Registro podrá rechazar una solicitud en los siguientes casos:

- Documentación incompleta o no vigente.
- Suplantación de identidad; en cuyo caso deberá realizarse las gestiones correspondientes según normativa vigente.
- En caso de no poderse comprobar la identidad del solicitante.

En estos casos el Oficial de Registro debe informar al solicitante los motivos que originaron el rechazo de la solicitud.

Todo CSR registrado y enviado por la Agencia de Registro, que no llegue a ser procesado por la Entidad Certificadora Pública en los plazos establecidos, por casos fortuitos o de fuerza mayor, deberán ser informadas mediante nota oficial al ente regulador ATT para su conocimiento y seguimiento.

Para las entidades públicas se procederá a realizar la emisión de los certificados digitales una vez se cumpla el respectivo procedimiento administrativo de contratación con la Entidad Certificadora Pública ADSIB, según normativa vigente.

Para las entidades privadas se procederá a realizar la emisión de los certificados digitales previa solicitud y, constancia de pago o firma de contrato/documento equivalente que garantice el compromiso de pago.

En caso de las cuentas corporativas, la entidad beneficiada deberá remitir formalmente a la Entidad Certificadora Pública ADSIB el listado del personal autorizado para obtener un certificado digital por el servicio adquirido. Estas entidades serán responsables de informar a sus dependientes sobre los procesos de generación de cada solicitud, y agotarán esfuerzos de coordinación para que los mismos se presenten para la toma de los datos biométricos previniendo cualquier tipo de contratiempo.

#### **4.4. Emisión del certificado**

La Entidad Certificadora Pública ADSIB será responsable de atender todo CSR remitido y emitir el certificado en los plazos establecidos. Las Agencias de Registro son responsables de centralizar la información digital generada y obtenida en los procesos de solicitud, renovación, reemisión y revocación de certificados digitales.

La Entidad Certificadora Pública ADSIB una vez que recibe la solicitud CSR firmada, estará en condiciones de emitir el certificado, para ello dispone de procedimientos internos que incluyen una ceremonia de Firma Digital de los certificados que garantizan la seguridad e integridad de los datos.

La Entidad Certificadora Pública ADSIB tiene procedimientos internos para realizar una evaluación por muestreo de los requisitos presentados en cada solicitud de emisión de certificado digital, posterior a la emisión del certificado, a través de un control cruzado de los documentos. Si en la evaluación se comprueba que no se han cumplido los requisitos, la Entidad Certificadora Pública ADSIB procederá a reportar oficialmente a la Agencia de Registro para la respectiva corrección. Se tienen procedimientos internos



establecidos para este fin.

La Entidad Certificadora Pública ADSIB dando cumplimiento a la normativa vigente, tendrá un plazo máximo de 72 horas para la emisión de los certificados y poner a disposición de los solicitantes su certificado digital firmado, salvo en caso fortuito, de coyuntura, fuerza mayor o decisión técnicamente justificada, informando la razón al usuario solicitante y al ente regulador.

#### **4.5. Aceptación del certificado**

Los certificados emitidos por la Entidad Certificadora Pública son enviados al sistema de Agencia de Registro, donde los usuarios titulares poseedores de la clave privada podrán descargar el certificado correspondiente, previa autenticación. La vigencia del Certificado Digital inicia al momento de su emisión. Con la emisión y el envío del certificado a la cuenta del titular en el sistema de la respectiva Agencia de Registro autorizada, se da por cumplido el servicio de Certificación Digital.

El contrato de adhesión, que debe ser firmado digitalmente por el usuario titular, garantiza el reconocimiento de las condiciones de uso, así como las obligaciones y derechos establecidos para éste; en caso de no realizarse la firma del contrato en el plazo establecido, el certificado digital será revocado. El plazo para la firma del contrato se encuentra establecido en el documento de Políticas de Certificación.

#### **4.6. Uso del certificado y del par de claves**

Los certificados digitales podrán ser utilizados según lo estipulado en esta Declaración de Prácticas de Certificación, en las Políticas de Certificación correspondientes y en cualquier otro documento complementario emitido por la Entidad Certificadora Pública ADSIB y aprobado por la ATT.

Los terceros de confianza son las entidades o personas (diferentes al usuario titular) que deciden aceptar y confiar en un certificado digital emitido por la Entidad Certificadora Pública ADSIB.

Es responsabilidad de los terceros de confianza verificar el documento firmado digitalmente mediante los servicios ofrecidos por la Entidad Certificadora Pública ADSIB.

En caso de verse comprometida su clave privada, el titular del certificado digital deberá realizar la Revocación de su certificado digital de acuerdo con los procedimientos establecidos en el presente documento.

#### **4.7. Renovación del certificado digital**

Para este procedimiento el usuario titular deberá acceder al Sistema de Agencia de Registro con las credenciales de usuario que obtuvo al momento de crear la cuenta y solicitar la respectiva renovación de alguno de sus Certificados Digitales vigentes.

La primera acción que se debe realizar para renovar un Certificado Digital es firmar digitalmente el Contrato de Adhesión correspondiente al nuevo Certificado Digital por emitirse. Una vez se tenga el Contrato de Adhesión debidamente firmado, se deberá decidir si desea generar un nuevo par de claves o conservar el par de claves para la renovación del Certificado.



Se puede realizar la solicitud de renovación hasta en tres (3) oportunidades, siempre y cuando el certificado este vigente. Si se ha excedido el periodo de vigencia del certificado, se debe realizar una solicitud de un nuevo certificado. La cuarta renovación consecutiva será tratada como una solicitud nueva, necesitando cumplir todos los procedimientos establecidos por la Entidad Certificadora Pública ADSIB.

El periodo habilitado para realizar una solicitud de renovación del Certificado Digital es de 30 días antes de que termine la vigencia del certificado digital inicial. La Entidad Certificadora Pública ADSIB enviará notificaciones para recordarle al usuario que puede realizar su renovación.

La vigencia del certificado digital renovado comenzará a partir de la expiración del certificado digital inicial.

Solamente se podrá proceder a la renovación del certificado digital directamente por el sistema de Agencia de Registro si se cumple con las siguientes condiciones:

- Que la solicitud de renovación mantenga todos los datos y tipo del certificado emitido inicialmente.
- Se firme digitalmente el Contrato de Adhesión correspondiente al nuevo certificado digital.
- El certificado aún se encuentra vigente durante la firma del contrato de Adhesión. Una vez firmado el nuevo contrato de adhesión, se tiene un plazo de 10 días calendario a partir de la expiración del certificado inicial para que se concluya el proceso de solicitud de renovación. Si en el plazo establecido no se envía la solicitud de renovación, se procederá a cancelar la emisión; y se deberá proceder a realizar una solicitud como si se tratase de un nuevo certificado.
- Solicitar la primera, segunda o tercera renovación. La cuarta solicitud de renovación debe realizarse como si se tratase de una nueva solicitud.
- Se firme digitalmente la solicitud de firma de certificado (CSR) para enviarlo a la Entidad Certificadora Pública ADSIB.
- Se realice el pago correspondiente de acuerdo a la estructura tarifaria vigente.
- Que la solicitud sea realizada únicamente por el usuario titular del certificado, considerando la autenticidad del solicitante, mediante el acceso al sistema por su usuario y contraseña.

En caso de cambiar el tipo de certificado o alguno de los datos que sean permitidos de acuerdo con las políticas de certificación de cada tipo de certificado, se deberá seguir el procedimiento como si se tratase de un nuevo Certificado.

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

#### **4.8. Reemisión del Certificado Digital**

La reemisión de un certificado digital es un procedimiento que se realiza a través del sistema de Agencia de Registro.

La solicitud de reemisión de certificado digital podrá realizarse con un nuevo par de claves para el nuevo certificado digital. Así mismo todas las solicitudes de reemisión deberán estar firmadas digitalmente por un Oficial de Registro antes de ser enviadas a la ECP, garantizando la seguridad del proceso de reemisión.



Al enviar la solicitud de reemisión, el Sistema de Agencia de Registro determinará el periodo de validez correspondiente en base al tiempo restante del certificado digital inicial.

Cuando un usuario con Certificado Digital con Token solicite una reemisión, puede solicitar también la reposición del token. Para ello debe cancelar el costo de reposición del dispositivo y coordinar la entrega a través de los medios habilitados por las Agencias de Registro; finalmente se debe proceder según lo establecido para una reemisión de certificado digital.

En caso de corrección de la información de los datos del certificado, el usuario solicitante deberá comunicarse con algún Oficial de Registro para que, a través de él, se modifique la información solicitada y se proceda a enviar un nuevo CSR con la información modificada.

En caso de necesitarse el cambio de titular en la reemisión, se deberá proceder como si de un nuevo certificado digital se tratase; sin embargo, el periodo de vigencia del nuevo certificado será por el tiempo restante del certificado inicial. En estos casos, el nuevo titular deberá firmar un nuevo Contrato de Adhesión una vez se emita su certificado digital.

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

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

#### **4.9. Revocación del Certificado**

La revocación de un certificado es el acto por el cual se deja sin efecto un certificado antes que alcance su fecha de caducidad. Cualquier firma digital realizada posterior a la revocación no tendrá validez; en cambio los documentos firmados previo a la revocación del certificado seguirán teniendo toda validez legal

Una vez revocado el certificado, la Entidad Certificadora Pública lo incluye en la Lista de Certificados Revocados (CRL) con el fin de notificar a terceros que un certificado ha sido revocado. Los certificados que sean revocados no podrán por ninguna circunstancia volver al estado activo, siendo esta una acción definitiva.

La revocación se realizará de acuerdo con los procedimientos internos con los que la Entidad Certificadora Pública ADSIB trabaja y a solicitud del usuario o autoridad competente. Las entidades públicas y privadas tienen toda la responsabilidad de velar por la revocación de los certificados de su personal que se desvincule.

Un certificado digital podrá ser revocado debido a las siguientes causas:

- A solicitud del titular debido a robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- Emisión defectuosa de un certificado debido a que:
  - No se ha cumplido un requisito material para la emisión del certificado.
  - Un dato fundamental relativo al certificado es falso.



- Existencia de un error de entrada de datos u otro error de proceso.
- No se firme el contrato de adhesión al servicio en el plazo establecido posterior a su emisión.
- La información contenida en un certificado o utilizada para realizar su solicitud deja de ser correcta.
- El certificado de la Entidad Certificadora Pública ADSIB o Entidad Certificadora Raíz ATT sea revocado.
- Otros fundamentos técnicos y/o legales, de interés nacional, por resguardo de la seguridad del Estado Plurinacional de Bolivia o de interés del pueblo boliviano, mediante Resolución Administrativa de su Máxima Autoridad Ejecutiva.

Las condiciones mínimas que cumplir para solicitar una revocación de certificado digital son:

- El certificado digital aún se encuentre vigente.
- Ser el usuario solicitante o ser representante legal de la entidad a la que pertenece el usuario solicitante.

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

Los usuarios corporativos pueden realizar la revocación de los certificados emitidos para los usuarios registrados según su listado de beneficiarios, sin realizar verificación alguna.

En cualquier caso, la Entidad Certificadora Pública ADSIB emite una notificación al usuario cuando la revocación se efectiviza.

#### **4.9.1. Revocación Presencial**

Al realizar una solicitud de revocación de manera presencial en alguna Agencia de Registro autorizada, el Oficial de Registro debe realizar la validación a través de la presentación de un documento que verifique la identidad del usuario titular.

En caso que el usuario titular no pueda proporcionar ningún documento que acredite su identidad, no se procederá a la revocación del Certificado Digital. Si se verifica la identidad del usuario titular, se efectivizará la revocación del certificado de manera inmediata.

#### **4.9.2. Revocación telefónica**

La Agencia de Registro establecerá un servicio de revocación por vía telefónica, cuya información será socializada y publicada en el sitio web.

La solicitud de revocación vía telefónica estará pendiente, hasta realizar la validación mediante una nueva llamada telefónica al número registrado en los datos del usuario titular. La verificación se realizará solicitando la siguiente información: número de documento de identidad, nombre completo y fecha de nacimiento del usuario titular. La Agencia de Registro tiene implementados los controles de validación correspondiente respecto a llamadas telefónicas.



En caso que se confirme la solicitud a través de la llamada telefónica, se efectivizará la revocación del certificado.

#### **4.9.3. Revocación en línea a través del Sistema de AR**

El usuario titular puede acceder al Sistema de Agencia de Registro y solicitar la revocación de su certificado digital. La Entidad Certificadora Pública considera que la autenticación a través del sistema es prueba suficiente para verificar la identidad del usuario titular, por lo que se efectivizará la revocación del certificado de manera inmediata.

Para las cuentas corporativas, el usuario responsable de dicha cuenta podrá solicitar la revocación de cualquiera de sus beneficiarios. La misma se efectivizará de manera inmediata.

#### **4.9.4. Revocación vía correo electrónico**

La Agencia de Registro puede recibir solicitudes de revocación a través de la dirección de correo electrónico soporte@firmadigital.bo, siempre y cuando se proporcione la siguiente información:

- Nombre completo
- Número de documento de identidad

El correo debe ser enviado desde la dirección registrada a nombre del usuario titular en el Sistema de Agencias de Registro.

La solicitud de revocación por correo electrónico estará pendiente hasta realizar la respectiva validación vía telefónica al número de teléfono registrado en los datos del usuario titular. La verificación se realizará solicitando la siguiente información: número de documento de identidad, nombre completo y fecha de nacimiento del usuario titular.

En caso de que se confirme la solicitud a través de la llamada telefónica, se efectivizará la revocación del certificado.

#### **4.10. Servicio de estado de los certificados**

La Entidad Certificadora Pública 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





#### **4.11. 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.

#### **4.12. 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.

### **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 202/2018 emitida por la ATT.

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

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo.

##### **5.1.1. Ubicación y construcción**

Las dependencias del Centro de Procesamiento de Datos de la Entidad Certificadora Pública ADSIB se encuentran en instalaciones del Edificio de la Vicepresidencia, en la parte del subsuelo

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 Entidad Certificadora Pública ADSIB cuenta con un Centro de Datos alternativo 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 la Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 extintores ubicados en lugares establecidos y adecuados.

### **5.1.6. Sistema de almacenamiento**

La Entidad Certificadora Pública ADSIB tiene establecido los procedimientos necesarios para disponer de



copias de seguridad de respaldo de la información crítica 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 Entidad Certificadora Pública ADSIB tiene establecidos procedimientos de respaldo, resguardo y recuperación de las copias de seguridad en un sitio alternativo, su transferencia y resguardo está 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 Entidad Certificadora Pública ADSIB 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 Entidad Certificadora Pública ADSIB dispone de copias de seguridad de la información crítica 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 realicen 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 requerida 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, contratación y comprobación de los antecedentes, experiencia y conocimiento del personal permanente, consultoría y eventual se realizará según los procedimientos internos que la Entidad Certificadora Pública dispone.

#### **5.3.3. Formación y frecuencia de actualización de la formación.**

El personal encargado de la Certificación Digital dentro de la Entidad Certificadora Pública ADSIB 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 Entidad Certificadora Pública ADSIB se encuentran asociadas a la descripción del cargo que ocupa cada empleado 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 Declaración de Prácticas 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 Entidad Certificadora Pública ADSIB y podrá ser sancionado de acuerdo a reglamentación interna.

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

La Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB que finaliza su relación contractual con la institución debe 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 Entidad Certificadora Pública ADSIB almacena registros de los eventos (logs) de seguridad más significativos relativos a su actividad como Entidad Certificadora Pública. Estos registros son almacenados automáticamente, así mismo en los casos del acceso físico se debe autorizar y registrar de acuerdo a los planes y procedimientos de seguridad de la Entidad Certificadora Pública ADSIB.

Los registros mínimos de los eventos relacionados con la seguridad de la infraestructura de clave pública son los siguientes:

- Instalación y Configuración de los Sistemas Operativos.
- Instalación y Configuración de aplicaciones instaladas
- Instalación y Configuración del Módulo Criptográfico.
- Accesos o intentos de acceso al equipo.
- Actualizaciones.
- Mantenimientos.
- 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

### 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 Entidad Certificadora Pública ADSIB.

La Entidad Certificadora Pública ADSIB dispone de herramientas tecnológicas para el monitoreo continuo de las operaciones realizadas en el equipamiento tecnológico de la infraestructura de clave pública.

### 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 Entidad Certificadora Pública ADSIB tendrán periodos de retención de logs de auditoría según el procedimiento de gestión de logs definido.

### 5.4.4. Protección de los logs de auditoría

La Entidad Certificadora Pública ADSIB 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 Entidad Certificadora Pública ADSIB tiene implementado un sistema de centralización de eventos el cual monitorea y notifica actividades dentro del equipamiento tecnológico del servicio de certificación 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 mismo se tiene un cronograma anual de análisis de vulnerabilidades en los sistemas, aplicaciones y servicios críticos relacionadas con 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 información y registros**

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

La documentación confidencial generada por la Entidad Certificadora Pública ADSIB almacenada en soportes de información físicas y digitales contienen niveles de seguridad tanto físicas 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB podrá cambiar su par de claves por los siguientes motivos:

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

### **5.7. Recuperación de la clave de la ADSIB**

La Entidad Certificadora Pública ADSIB tiene sus procedimientos para la recuperación de la clave privada mediante los documentos “Planes y Procedimientos para la Continuidad del Servicio y Plan de Contingencias”.

### **5.8. Procedimientos para recuperación de desastres**

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



Continuidad del Servicio es revisado periódicamente según cambios de los riesgos en el ambiente.

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

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

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

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

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

### **5.9.1. Sujetos involucrados.**

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

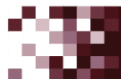
#### **5.9.2.1. *Publicación***

Ante la declaración del cese de actividades de la Entidad Certificadora Pública ADSIB, la primera tarea será publicar la información en el sitio web: [www.firmadigital.bo](http://www.firmadigital.bo) y [www.adsib.gob.bo](http://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 Entidad Certificadora Pública 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 los sitios web [www.firmadigital.bo](http://www.firmadigital.bo) y [www.adsib.gob.bo](http://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 Entidad Certificadora Pública ADSIB, 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 Entidad Certificadora Pública ADSIB deberá proceder de la siguiente manera para la revocación de los certificados.

- a) Se podrá revocar certificados digitales hasta el mismo día y hora del cese de actividades. Solamente podrá efectuar revocaciones a solicitud de los usuarios titulares. Si los usuarios titulares, 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) Se 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB, 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB, 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB, 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 Pública 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 Entidad Certificadora Pública 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 Físicos y Digitalizados de la Entidad Certificadora.

Asimismo, la Entidad Certificadora Pública ADSIB conservará toda la información relacionada con su servicio de certificación digital, detalladas a continuación:

- Los archivos de documentación presentada por solicitantes y usuarios titulares.
- La documentación relacionada con pedidos de revocación.
- La documentación generada en las ceremonias digitales.
- La última lista de certificados revocados.
- El respaldo 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Pública ADSIB, 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.

La generación del par de claves por software en un dispositivo debe estar establecido bajo el criterio de la FIPS 140-2 nivel 1, en el que se establece como nivel de seguridad normal, 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 Entidad Certificadora Pública ADSIB puede ser usada 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB y que participen 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 Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB está resguardada en módulos HSM protegidos física y lógicamente.

### 6.2.5. Archivo de la clave privada

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

Las claves de acceso son confidenciales, personales e intransferibles.

#### **6.5. Controles de seguridad informática**

La Entidad Certificadora Pública ADSIB tiene 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 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 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 202/2015.

El HSM utilizado por la clave pública de la Entidad Certificadora Pública ADSIB 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 que permitan instrumentar y auditar cada fase de los sistemas de la Entidad Certificadora Pública 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 Entidad Certificadora Pública ADSIB se mantienen "off-line" en un perímetro de seguridad física de alta seguridad, su acceso es restringido solo a personal autorizado y protegido mediante una combinación de procedimientos de acceso administrativo y accesos físicos.

La infraestructura tecnológica que alberga el procedimiento de certificación digital tiene implementado un sistema de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los



controles de acceso.

## 6.8. Controles de los módulos criptográficos.

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

## 6.9. Sincronización horaria.

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

## 7. Perfiles de Certificado y de la lista de certificados revocados.

El perfil de los certificados corresponde con el propuesto en las políticas de certificación particulares y son coherentes con la normativa internacional.

### 7.1. Perfil del Certificado de la Entidad Certificadora Raíz (ECR)

El formato para el Certificado Digital de la ECR tendrá los siguientes atributos y contenidos:

NOMBRE	VALOR
Versión (versión)	2
Número de Serie (serialNumber)	Asignado por la ECR
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Periodo de validez (validity)	Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Información de la clave pública del suscriptor (subjectPublicKey)	Algoritmo: RSA, Longitud: 4096 bits.

Las extensiones del Certificado Digital de la ECR serán las siguientes:



NOMBRE	VALOR
Identificador de la clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey.
Uso de Claves (keyUsage)	digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
Política de Certificación (certificatePolicies)	URI: (archivo en formato de texto)
Restricciones Básicas (basicConstraints)	CA = TRUE, pathLenConstraint = "1".
Punto de distribución de las CRL (cRLDistributionPoints)	URI: (.crl).

## 7.2. Perfil del Certificado de la Entidad Certificadora Pública ADSIB

El formato para el Certificado Digital de la Entidad Certificadora Pública ADSIB tendrá los siguientes atributos y contenidos:

NOMBRE	VALOR
Versión (version)	2
Número de Serie (serialNumber)	Asignado por la ECR
Algoritmo de firmas (signatureAlgorithm)	OID: 1.2.840.113549.1.15 (SHA256withRSA)
Nombre del Emisor (issuer)	CN = Entidad Certificadora Raíz de Bolivia; O = ATT; C = BO de acuerdo con ISO3166.
Periodo de validez (validity)	Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time)
Nombre suscriptor (subject)	CN = "Entidad Certificadora Pública ADSIB"; O = "ADSIB"; C = "BO".
Información de la clave pública	Algoritmo: RSA, Longitud: 4096 bits.





del suscriptor (subjectPublicKey)

Las extensiones del Certificado Digital de una ECA serán las siguientes:

NOMBRE	VALOR
Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier)	Identificador de la clave pública de la ECR
Identificador de la clave del suscriptor (subjectKeyIdentifier)	Función Hash (SHA1) del atributo subjectPublicKey.
Uso de Claves (keyUsage)	digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.
Política de Certificación (certificatePolicies)	URI: (archivo en formato de texto)
Restricciones Básicas (basicConstraints)	CA = TRUE, pathLenConstraint = "1".
Punto de distribución de las CRL (cRLDistributionPoints)	URI: (.crl).
Información de Acceso de la ECA (authorityInformationAccess)	URI: (.crt).

### 7.3. Perfil de la CRL de la Entidad Certificadora Pública

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 (signatureAlgorithm)	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 Pública 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

#### 7.4. Perfil del OCSP de la Entidad Certificadora Pública

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 (optional 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 (unknown), 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 Entidad Certificadora Pública ADSIB en el marco de la Infraestructura de Clave Pública de Bolivia.

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

## **8. Auditoría de Conformidad.**

La Entidad Certificadora Pública ADSIB está sujeta a auditorías de control y seguimiento establecidas en el marco normativo vigente y son implementadas por la ATT como ente regulador.

### **8.1. Frecuencia de los controles de conformidad para la ADSIB**

La Entidad Certificadora Pública ADSIB está sujeta a las disposiciones de la ATT como Entidad Certificadora Raíz, por lo que la frecuencia de los controles de conformidad está definida por la ATT.

### **8.2. Relación entre el auditor y la entidad auditada.**

La relación entre el auditor y la Entidad Certificadora Pública ADSIB como entidad certificadora pública se detalla en el Decreto Supremo 1793 del 13 de noviembre de 2013, que establece en su artículo 46:

- I. Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.



### **8.3. Comunicación de resultados.**

La Entidad Certificadora Pública ADSIB está sujeta a las disposiciones de la ATT como Entidad Certificadora Raíz, por lo que la comunicación de los resultados de las auditorías será definida por la ATT.

## **9. Otras cuestiones legales y de actividad.**

### **9.1. Contrato de adhesión.**

Los certificados emitidos por la Entidad Certificadora Pública ADSIB, está asociado 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 los plazos establecidos según el documento “Políticas de Certificación”, caso contrario se procederá a la revocación automática del mismo.

### **9.2. Tarifas.**

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

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

Las tarifas aplicables a otros servicios relacionados a la certificación digital se negociarán entre la Entidad Certificadora Pública ADSIB y el solicitante del servicio, misma que se pondrá en conocimiento y aprobación de la ATT como ente regulador.

### **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 presente documento.

### **9.4. Ámbito de la Información confidencial.**

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



## **9.5. Protección de Datos Personales.**

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

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

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

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

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

### **9.6.1. Derechos y Obligaciones de la Entidad Certificadora Pública.**

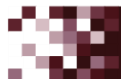
#### **9.6.1.1. Derechos de la Entidad Certificadora Pública**

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

- a) Recibir oportunamente el pago por los servicios provistos, de conformidad con los precios o tarifas establecidas.
- b) Cortar el servicio provisto por falta de pago por parte de las usuarias o usuarios, previa comunicación, conforme a lo establecido por reglamento.
- c) Recibir protección frente a interferencias perjudiciales a operaciones debidamente autorizadas.
- d) Otros que se deriven de la aplicación de la Constitución Política del Estado, la Ley N° 164 y demás normas aplicables.

#### **9.6.1.2. Obligaciones de la Entidad Certificadora Pública**

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



- a) Someterse a la jurisdicción y competencia de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- b) Proveer en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida, los servicios de telecomunicaciones y tecnologías de información y comunicación.
- c) Proporcionar información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a las usuarias o los usuarios.
- d) Proporcionar información clara, precisa, cierta, completa y oportuna a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- e) Proveer gratuitamente los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, que determine la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- f) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación según los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- g) Efectuar el reintegro o devolución de montos que resulten a favor de las usuarias o los usuarios por errores de facturación, deficiencias o corte del servicio, con los respectivos intereses legales.
- h) Atender las solicitudes y las reclamaciones realizadas por las usuarias o los usuarios.
- i) Informar oportunamente la desconexión o cortes programados de los servicios.
- j) Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley.
- k) Facilitar a las usuarias o usuarios en situación de discapacidad y personas de la tercera edad, el acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en reglamento.
- l) Proveer servicios que no causen daños a la salud y al medio ambiente.
- m) Actualizar periódicamente su plataforma tecnológica y los procesos de atención a las usuarias y los usuarios.
- n) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

Para garantizar la publicidad, seguridad, integridad y eficacia del certificado digital, la Entidad Certificadora Pública tiene las siguientes obligaciones según a lo establecido en el Artículo 43 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación:

- a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;
- b) Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT;
- c) Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web entre otros medios;
- d) Mantener el control, reserva y cuidado de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Cualquier anomalía que pueda comprometer su confidencialidad deberá ser comunicada inmediatamente a la ATT;
- e) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
- f) Mantener un sistema de información de acceso libre, permanente y actualizado donde se publiquen los procedimientos de certificación digital, así como los certificados digitales emitidos consignando,



- su número único de serie, su fecha de emisión, vigencia y restricciones aplicables, así como el detalle de los certificados digitales suspendidos y revocados;
- g) Las entidades certificadoras que derivan de la certificadora raíz (ATT) deberán mantener un sistema de información con las mismas características mencionadas en el punto anterior, ubicado en territorio y bajo legislación del Estado Plurinacional de Bolivia;
  - h) Revocar el certificado digital al producirse alguna de las causales señaladas en los puntos anteriores;
  - i) Mantener la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso;
  - j) Mantener la información relativa a los certificados digitales emitidos, por un período mínimo de cinco (5) años posteriores al periodo de su validez o vigencia;
  - k) Facilitar información y prestar la colaboración debida al personal autorizado por la ATT, en el ejercicio de sus funciones, para efectos de control, seguimiento, supervisión y fiscalización del servicio de certificación digital, demostrando que los controles técnicos que emplea son adecuados y efectivos cuando así sea requerido;
  - l) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
  - m) Notificar a la ATT cualquier cambio en la personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos o correo electrónico;
  - n) Verificar toda la información proporcionada por el solicitante del servicio, bajo su exclusiva responsabilidad;
  - o) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;
  - p) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidos que administra.

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

De conformidad a lo establecido en el Artículo 44 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación y la Resolución Administrativa RAR-DJ-RA TL LP 845/2018 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, la Responsabilidad de la Entidad Certificadora Pública ante terceros, se da en los siguientes casos:

- a) Será responsable por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus usuarios.
- b) La entidad certificadora se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.
- c) La entidad certificadora responderá por posibles perjuicios que se causen al usuario titular o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

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

Según lo establecido en el Artículo 52 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, son titulares de la firma digital y del certificado digital las personas jurídicas que hayan solicitado por sí y para sí una certificación que acredite su firma digital.



### **9.6.2.1. Responsabilidad del titular**

Según lo establecido en el Artículo 53 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular será responsable en los siguientes casos:

- a) Por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como titular.
- b) El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
- c) Asimismo, acorde a los procedimientos de la Entidad Certificadora Pública ADSIB, la entidad no podrá acceder en ningún momento a la clave privada del usuario, por lo que éste es el único responsable de su generación, administración, uso y custodia. En caso de verse comprometida por cualquier razón dicha clave, el usuario deberá informar a la Entidad Certificadora Pública ADSIB a la brevedad posible y solicitar la revocación del certificado digital. Todos los efectos o daños que pudieran ocasionarse al usuario o a terceros, en el transcurso comprendido entre la generación del certificado y su revocatoria, son de exclusiva responsabilidad del usuario.

### **9.6.2.2. Derechos del Titular del Certificado**

De conformidad a lo señalado en el Artículo 54 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular del certificado digital tiene los siguientes derechos:

- a) A ser informado por la entidad certificadora de las características generales, de los procedimientos de creación y verificación de firma digital, así como de las reglas sobre prácticas de certificación y toda información generada que guarde relación con la prestación del servicio con carácter previo al inicio del mismo, así como de toda modificación posterior,
- b) A la confidencialidad de la información proporcionada a la entidad certificadora;
- c) A recibir información de las características generales del servicio, con carácter previo al inicio de la prestación del mismo;
- d) A ser informado, antes de la suscripción del contrato para la emisión de certificados digitales, acerca del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, de las condiciones precisas para la utilización del certificado, de las limitaciones de uso, de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o los que se acordaren;
- e) A que la entidad certificadora le proporcione la información sobre su domicilio legal en el país y sobre todos los medios a los que el titular pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del servicio contratado, o la forma en que presentará sus reclamos;
- f) A ser informado, al menos con dos (2) meses de anticipación, por la entidad certificadora del cese de sus actividades, con el fin de hacer valer su aceptación u oposición al traspaso de los datos de sus certificados a otra entidad certificadora.

### **9.6.2.3. Obligaciones del Titular del certificado**

De conformidad a lo señalado en el Artículo 55 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el titular del certificado digital tiene las siguientes obligaciones:





1. El titular de la firma digital mediante el certificado digital correspondiente tiene las siguientes obligaciones:
  - a) Proporcionar información fidedigna y susceptible de verificación a la entidad certificadora;
  - b) Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado;
  - c) Observar las condiciones establecidas por la entidad certificadora para la utilización del certificado digital y la generación de la firma digital;
  - d) Notificar oportunamente a la certificadora que los datos de creación de su firma digital han sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada, en este caso deberá solicitar la baja de su certificado digital;
  - e) Actuar con diligencia y tomar medidas de seguridad necesarias para mantener los datos de generación de la firma digital bajo su estricto control, evitando la utilización no autorizada del certificado digital;
  - f) Comunicar a la entidad certificadora cuando exista el riesgo de que los datos de su firma digital sean de conocimiento no autorizado de terceros, por el titular y pueda ser utilizada indebidamente;
  - g) No utilizar los datos de creación de firma digital cuando haya expirado el período de validez del certificado digital; o la entidad de certificación le notifique la suspensión de su vigencia o la conclusión de su validez;
  - h) No delegar el uso del Certificado a terceras personas ni a intermediarios, dado que la responsabilidad por los documentos firmados se asigna directamente al titular del Certificado Digital. Este aspecto no aplica a los Certificados emitidos para Firma Automática.
2. El incumplimiento de las obligaciones antes detalladas, hará responsable al titular de la firma digital de las consecuencias generadas por el uso indebido de su firma digital.

### **9.6.3. Derechos y Obligaciones de los Usuarios**

#### **9.6.3.1. Derechos de las usuarias y usuarios**

De conformidad a lo señalado en el Artículo 54 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, las usuarias y usuarios tienen los siguientes derechos:

- a) Acceder en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida a los servicios de telecomunicaciones y tecnologías de información y comunicación.
- b) Acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a ser proporcionada por la Entidad Certificadora Pública.
- c) Acceder gratuitamente a los servicios de telecomunicaciones y tecnologías de información y comunicación en casos de emergencia, de acuerdo a determinación de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- d) Recibir de forma oportuna, comprensible y veraz la factura mensual desglosada de todos los cargos y servicios del cual es usuario, en la forma y por el medio en que se garantice su privacidad.
- e) Exigir respeto a la privacidad e inviolabilidad de sus comunicaciones, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.
- f) Conocer los indicadores de calidad de prestación de los servicios al público de los proveedores de telecomunicaciones y tecnologías de información y comunicación.



- g) Suscribir contratos de los servicios de telecomunicaciones y tecnologías de información y comunicación según los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- h) Ser informado por la Entidad Certificadora Pública oportunamente, cuando se produzca un cambio de los precios, las tarifas o los planes contratados previamente.
- i) Recibir el reintegro o devolución de montos que resulten a su favor por errores de facturación, deficiencias, corte del servicio o modificación de tarifas por vigencia de una nueva estructura tarifaria en la venta de dispositivos criptográficos.
- j) Obtener respuesta efectiva a las solicitudes realizadas a la Entidad Certificadora Pública.
- k) Reclamar ante la Entidad Certificadora Pública y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna.
- l) Disponer, como usuaria o usuario en situación de discapacidad y persona de la tercera edad facilidades de acceso a los servicios de telecomunicaciones y tecnologías de información y comunicación, determinados en un reglamento especial.
- m) Otros que se deriven de la aplicación de la Constitución Política del Estado, Tratados Internacionales, las leyes y demás normas aplicables.

#### **9.6.3.2. Obligaciones de las usuarias y usuarios**

De conformidad a lo establecido en el Artículo 55 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, las usuarias y usuarios tienen las siguientes obligaciones:

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

- a. Cumplir y hacer cumplir con lo dispuesto en la presente Declaración de Prácticas de Certificación.
- b. Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT.
- c. Publicar esta Declaración de Prácticas de Certificación y las “Políticas de Certificación” en el sitio web de la Entidad Certificadora Pública ADSIB



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

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

### **9.8. Modificaciones al presente documento.**

La responsabilidad de la administración y modificación de del presente documento “Declaración de Prácticas de Certificación” corresponde a la Entidad Certificadora Pública ADSIB.

Cuando la Entidad Certificadora Pública ADSIB realice modificaciones a la presente Declaración de Prácticas, estas deberán ser aprobadas por el ente regulador 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.

### **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 después de iniciado el conflicto, posteriormente se someterá dicha controversia a la autoridad de fiscalización y telecomunicaciones ATT como ente regulador de la Entidad Certificadora Pública ADSIB. 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 cualquier responsabilidad con respecto a cualquier evento que comprometa dicha clave y las consecuencias derivadas de su uso.

### **9.10. Legislación aplicable.**

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



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

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) como encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras según la Ley N.º 164 emite una serie de Resoluciones Administrativas Regulatorias y que fueron consideradas para la elaboración del presente documento:

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

### 9.11. Conformidad con la ley aplicable.

Todos los procesos, procedimientos, información técnica y legal contenida en el presente documento de Declaración de Prácticas de Certificación, se encuentra elaborado en conformidad a todo 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
2.0	8/11/2018	Elaboración del documento. Se considera versión 2 debido a que los cambios anteriores realizados fueron cambios menores	Reynaldo Alonzo Vera Arias	María Jannett Ibañez Flores	ADSIB/ RA/007 4/2018	31/12/2018
2.1	24/06/2019	Ajustes al documento en base a	Reynaldo	José Luis	ADSIB/	24/06/2019



		la nueva reglamentación según Resolución ATT-DJ-RA TL LP 209/2019 emitida por la ATT	Alonzo Vera Arias	Machicado	RA/002 6/2019	
2.2	10/2020	Ajustes al documento en el marco de reglamentación aprobada mediante Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 209/2019, y las recomendaciones realizadas por la ATT	Reynaldo Alonzo Vera Arias	José Luis Machicado		

