agencia para el desarrollo de la sociedad de la información en Bolivia

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA ENTIDAD CERTIFICADORA PÚBLICA ADSIB

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia
ADSIB

La Paz - Bolivia

Índice de contenido

1. Introducción.

1.1 Presentación

La ADSIB presenta este documento en cumplimiento a las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015, ATT-DJ-RA TL LP 32/2015** y **ATT-DJ-RA TL LP 1538/2015** emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la Ley N° 164 General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

El documento brinda evidencia integral a todos los clientes, proveedores y empleados sobre los procedimientos específicos a ser implementados para asegurar la calidad de la Firma Digital. Este documento también rige la creación de contenidos relacionados con la calidad.

1.2 Identificación y nombre del documento

El documento se concentra en el Anexo 5: contenido mínimo del documento de declaración de practicas de certificación para una ECA, en conformidad con lo establecido en las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015**, **ATT-DJ-RA TL LP 32/2015**, y **ATT-DJ-RA TL 1538/2015** emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

El objetivo de este documento es plantear los contenidos de Declaración de Prácticas de Certificación para cumplimiento de la ADSIB en el marco de su consolidación como Entidad Certificadora Pública.

El presente documento lleva como titulo **"Declaración de Prácticas de Certificación de la Entidad Certificadora Pública -ADSIB"**

1.3 Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia

La Jerarquía Nacional de Certificación Digital, según el artículo 36 del Decreto Supremo Reglamentario 1793, establece los niveles de Infraestructura Nacional de Certificación Digital (INCD).

Descripción breve de la jerarquía nacional de Certificación Digital del Estado Plurinacional de Bolivia y de cada uno de sus componentes.

Se describe a continuación la jerarquía nacional de certificación digital y cada uno de sus

componentes:

- **Primer nivel:** Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes: **Entidad Certificadora Raíz.**

De acuerdo a la Ley N° 164 y el Decreto Supremo N° 1793 la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), es la Entidad Certificadora de Raíz.

La ATT es la entidad de certificación de nivel superior dentro de la Jerarquía Nacional de Certificación Digital que auto firmará su certificado y emitirá certificados digitales a las entidades certificadoras pública y privadas subordinadas.

- **Segundo Nivel: Entidad de Certificación**

Son las entidades certificadoras públicas 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 ATT a prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

- **Tercer nivel: Agencia de Registro**

Es la agencia dependiente de una entidad certificadora, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa debe efectuar los trámites con fidelidad a la realidad. Además, es quién se encarga de solicitar la aprobación o revocación de un certificado digital

La agencia de registro es la ADSIB, tiene como objetivo asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital.

a) **Cuarto nivel: Signatarios**

Son todos los usuarios y usuarias finales a quienes se les ha emitido un certificado por una entidad certificadora, dentro de la Jerarquía Nacional de Certificación Digital.

- **Otros: Terceros aceptantes.**

Son cualquier persona física u organización que confía en los certificados de la ADSIB, al autenticar a

una persona física o al aceptar una Firma Digital, están obligados a comprobar la validez del certificado.

1.4 Uso de los certificados.

- **Usos típicos**

La ADSIB estará limitado a la firma de certificados digitales para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en el presente documento.

El uso de los certificados emitidos por la ADSIB estará limitado según el tipo de certificado, y a continuación se menciona los usos de cada uno de ellos:

TIPOS DE CERTIFICADO	USO
Persona natural	Firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático
Persona jurídica	En representación de una persona jurídica: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático
Cargo público	Como servidor público: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático.
Lista de Revocación de Certificado	Firma de Lista de Revocación de Certificado
OCSP	Firma de OCSP

- **Usos prohibidos**

El usuario contratante de certificados digitales generados por la ADSIB está obligado a utilizarlos conforme a los usos permitidos y señalados en la sección anterior o cualquier texto normativo que los sustituya y regule la actividad de certificación digital dentro del Estado Plurinacional de Bolivia y para

el uso para el cual fue adquirido, quedando expresamente indicado que cualquier violación a las normas, usos y/o leyes del Estado Plurinacional de Bolivia queda bajo la responsabilidad del usuario contratante, así como los daños y perjuicios que ocasionare le será aplicable un proceso penal establecido en el Código Penal, artículo 363 (alteración, acceso y uso indebido de datos informáticos).

Adicionalmente le será revocado el certificado digital y el usuario contratante asume la responsabilidad de indemnizar a la 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 contratante del servicio contratado con la ADSIB.

Finalmente, los certificados digitales de personal natural no pueden ser utilizados en remplazo de los certificados de persona jurídica o de cargo público, en particular no se pueden firmar documentos en representación de una persona jurídica o como servidor público con un certificado de persona natural.

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

Para garantizar la fiabilidad de una firma y certificado digital a lo largo del tiempo, ésta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo.

Esto implica que si queremos tener una firma y certificado que pueda ser validada a lo largo del tiempo, la firma digital que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada.

Para este tipo de firmas existirá un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

1.5 Administración de la Declaración de Prácticas, procedimiento de aprobación.

- **Administración de la declaración de prácticas**

La administración de la presente Declaración de Prácticas de Certificación es responsabilidad de la ADSIB.

Para consultas o sugerencias, la ADSIB designa el siguiente contacto:

Dirección de correo: contacto@firmadigital.bo

Teléfono: (591-2) 2200720 - 2200730
Fax: (591-2) 2200740
Casilla 6500

Se publicaran en el sitio web de la ADSIB, las nuevas versiones de este documento, inmediatamente después de su aprobación.

- **Procedimiento de aprobación**

La aprobación de esta Declaración de Prácticas de Certificación, así como toda modificación introducida en ella, es responsabilidad exclusiva de la ADSIB.

La ADSIB aplicará sus procedimientos internos de aprobación para garantizar la calidad y trazabilidad de sus servicios.

1.6 Definiciones y abreviaturas.

- **Abreviaturas**

- **EC:** Entidad Certificadora.
- **ECR:** Entidad Certificadora Raíz.
- **AR:** Agencia de Registro.
- **URI:** Identificador Uniforme de Recursos
- **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
- **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública.
- **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
- **SHA**: (Secure Hash Algorithm) Algoritmo de Hash Seguro.
- **RFC:** ([1]Request For Comments) Requerimiento de Comentarios.
- **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
- **HSM:** (Hardware Security Module) Modulo de Hardware de Seguridad[2].
- **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
- **ADSIB:** Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

1 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.

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

- **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.
- **TIC:** Tecnologías de Información y Comunicación.
- **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.

- **Definiciones**

a) **Certificado digital:** Es un archivo digital firmado digitalmente por una entidad certificadora autorizada que vincula una clave pública a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital.
b) **Clave privada: Archivo digital que contiene un conjunto de caracteres** alfanuméricos únicos generados mediante un sistema criptográfico, que el signatario emplea en la firma digital de un documento. La clave privada es estrictamente confidencial e individual, y su perdida posibilita la usurpación de identidad del signatario.
c) **Clave pública:** Archivo digital que contiene un conjunto de caracteres alfanuméricos únicos, generados al mismo momento que la clave privada por el mismo sistema criptográfico. La clave pública esta contenida en el certificado digital, junto a los datos de identidad del signatario. Tiene vocación a ser de conocimiento público, y permite verificar la firma digital de un documento.
d) **Firma digital:** Es un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un documento digital, o un correo electrónico, que certifica la identidad del signatario y la integridad del documento digital firmado. La firma digital esta compuesta por el hash del documento digital cifrado por la clave privada del signatario, y por el certificado digital del signatario.

2. Publicación de información y repositorio de certificados.

- **Repositorios.**

Los repositorios públicos de información de la ADSIB están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la ADSIB, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 72 horas.

A fin de garantizar la completa disponibilidad de este documento en la Declaración de Prácticas de Certificación y demás documentos esenciales, la ADSIB mantiene un repositorio en la página web del

servicio de firma digital.

El repositorio público de la ADSIB, no contiene información confidencial o privada.

- **Publicación.**

Es obligación para la ADSIB publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de los mismos. Las publicaciones que realice la ADSIB, de toda la información clasificada como pública, se anunciara en la página web de la Entidad Certificadora Pública.

Este servicio de publicación de información del certificador está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la ADSIB, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 72 horas.

- **Frecuencia de actualización.**

La ADSIB se encuentra en la obligación de ejecutar de forma periódica la publicación de la información y datos que permitan a los signatarios, y terceros aceptantes contar con los registros, datos y vínculos necesarios para la utilización de los certificados y firmas digitales conforme a lo establecido en la normativa nacional que regula la materia.

- **Controles de acceso al repositorio de certificados.**

La ADSIB brinda acceso irrestricto a toda la información contenida en el repositorio público, y establece controles adecuados para restringir la posibilidad de escritura y modificación de la información publicada, garantizando su integridad.

El acceso a la información publicada por la ADSIB será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esa función, además, se garantiza la consulta a la CRL y el presente documento.

Todos los documentos publicados por la ADSIB en el repositorio serán firmados digitalmente por la entidad. Toda información cuya firma no pueda ser verificada deberá ser considerada nula.

3. Identificación y Autenticación de los titulares de los certificados.

3.1 Registro de nombres.

- **Tipos de nombres**

La norma vigente define los tipos de nombres para cada uno de los tres tipos de certificado. Para las personas naturales, el nombre se compone de: CN = Nombres y Apellidos de la persona natural; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

Para las personas jurídicas, el nombre se compone de: CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón social de la empresa o institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

Para las cargos públicos, el nombre se compone de: CN = Nombres y Apellidos del servidor público; O = Nombre de la institución pública a la que pertenece; OU = Unidad Organizacional de la que depende el funcionario público (opcional); T = Cargo del servidor público; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

- **Significado de los nombres**

La ADSIB requerirá de los clientes contratantes de certificados digitales sus nombres y apellidos completos y conforme figuran representados en la cédula de identidad que posea el solicitante de la firma digital.

No serán admitidos o procesados por la ADSIB los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el usuario. En todos los casos serán considerados los nombres que figuran en su cédula de identidad o pasaporte.

En todo caso la ADSIB garantiza que los nombres distintivos contenidos en los campos de los certificados son lo suficientemente distintivos y significativos para poder vincular la identidad de un

usuario a su firma digital.

- **Interpretación de formatos de nombres**

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritos en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos por la ADSIB utilizan codificación UTF-8 para todos los atributos, según la RFC 3280 ("Internet X.509 Public Key Infraestructure and Certificate Revocation List (CRL) Profile").

- **Unicidad de nombres**

La ADSIB define como campo del nombre distintivo del certificado de autoridad como único y sin ambigüedad. Para ello se incluirá como parte del nombre distintivo, específicamente en el campo correspondiente, el nombre o razón social de la ADSIB, por lo tanto la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro nacional.

- **Resolución de conflictos relativos a nombres**

En el caso de una ocurrencia de conflicto de nombre entre clientes y que corresponda a nombre y apellidos iguales, se procederá a realizar las distinción de identidad y autenticación de la misma a través del uso del número de cédula de identidad de cada usuario de la ADSIB con las cuales se haya generado el conflicto de nombre.

3.2 Validación de la identidad inicial.

- **Métodos de prueba de posesión de la clave privada**

El esquema de operación de la ADSIB y su sistema de certificación se encuentran configurados para funcionar en base a una estructura de claves: pública y privada.

En virtud de lo anterior, una vez emitido cada certificado, es el usuario quien tiene la custodia y resguardo de su clave privada, presumiendo que el mismo la posee y resguarda, salvo denuncia de él mismo usuario de la perdida de su clave privada, caso en el cual se procederá a la suspensión y/o revocación de la firma digital que corresponda.

La ADSIB, en ningún momento poseerá u obtendrá la clave privada del usuario, la creación, resguardo, uso y administración de la misma es responsabilidad exclusiva del usuario.

- **Autenticación de la identidad de una persona natural, jurídica o cargo público**

La ADSIB procederá a autenticar y validar la identidad de los usuarios dependiendo del tipo de certificado que soliciten.

Personal Natural

La ADSIB verificará los requisitos presentados con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

Persona Jurídica

La ADSIB procederá a comprobar la validez de la información del usuario con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

Cargo Público

La ADSIB procederá a comprobar la documentación requerida, a través de llamadas telefónicas y con la presentación de los originales. Una vez comprobada y validada la documentación presentada por el usuario y que se haya cumplido con el procedimiento de solicitud y registro, la ADSIB procederá a la generación del certificado digital contratado por el usuario.

- **Autenticación de la identidad de un individuo**

La persona física designada para tramitar la emisión de un certificado, además de presentar la resolución de acreditación vigente ante la ADSIB, deberá demostrar su identidad de la siguiente forma:

a) cédula de identidad.
b) fotografía.

Se verifica que dichos datos además coincidan con los establecidos en la resolución de acreditación y con el sistema del SEGIP.

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

- **Identificación y autenticación de las solicitudes de renovación rutinarias**

La identificación y autenticación para la renovación del certificado se realizará de la siguiente manera:

a) El usuario solicitará la renovación a través de su cuenta de usuario.
b) La ADSIB realizará la verificación de la solicitud y pago en un plazo no mayor a 72 horas mediante los procedimientos establecidos.
c) De no ser posible la verificación se emitirá un informe que detallen los esfuerzos realizados y se esperará que el usuario se ponga nuevamente en contacto a través de los teléfonos, correo electrónico, fax, etc. de la ADSIB.
d) La ADSIB podrá o no requerir al usuario presentarse personalmente en oficinas de la entidad, dependiendo del proceso de verificación.
e) En un plazo no mayor a 72 horas desde concluida la verificación, la ADSIB pondrá a disposición del usuario su nuevo certificado a través de su cuenta de usuario.

El proceso de renovación rutinario podrá realizarse únicamente por tres veces consecutivas, Al cabo de la misma el usuario deberá generar un nuevo par de claves e iniciar el proceso como la solicitud de un nuevo certificado.

- **Solicitudes de renovación con cambio de clave privada**.

El procedimiento es el mismo al de la solicitud de un nuevo certificado y el usuario deberá completar todos los pasos necesarios.

4. Ciclo de Vida de los Certificados.

Procesamiento de solicitud del certificado

Las personas que deseen obtener un certificado digital deberán:

a) Crear una cuenta de usuario en el sistema de la página web: www.firmadigital.bo
b) Solicitar mediante su cuenta de usuario el tipo de certificado digital y completar el formulario de solicitud.
c) Aproximarse a las oficinas de la ADSIB, junto con los requisitos que se le especificarán una vez realizada su solicitud.

d) Realizar el pago correspondiente.
e) Ingresar el número de depósito o subir una imagen del comprobante bancario en su cuenta de usuario.
f) Es responsabilidad del cliente proteger la contraseña de su cuenta de usuario.
g) Entregar al momento de presentar la solicitud el token según los estándares técnicos requeridos. En la página www.firmadigital.bo se publicará una lista de proveedores de token que cumplan con los estándares solicitados.
h) Aceptar la políticas y contrato correspondiente a la prestación del servicio.

*La apertura de la cuenta es gratuita y está disponible en línea.

Emisión del certificado

La ADSIB, una vez validada la identidad del signatario y verificado el pago correspondiente, aprobará la firma del certificado correspondiente.

La ADSIB cuenta con procedimientos internos para la ceremonia de la Firma Digital.

Una vez verificados la identidad y el pago correspondiente la ADSIB tendrá un plazo máximo de 72 horas para poner a disposición del usuario su certificado firmado en su cuenta de usuario, salvo caso fortuito, fuerza mayor o decisión técnicamente justificada, casos en que la entidad deberá informar las razones del retraso al usuario.

Aceptación del certificado

La ADSIB, una vez comprobado y validado la información y los requisitos presentados por el usuario, dispondrá el certificado y firma digital en la cuenta del usuario disponible a través del sistema.

La firma del contrato entre el usuario y la ADSIB implica que el usuario acepta los términos y condiciones del uso del certificado y firma digital.

Generación del par de claves y uso del certificado

- **La generación de las claves para la firma**

El usuario deberá generar el par de claves pública y privada en su dispositivo de firma digital. Al contar el usuario con su clave pública y privada, el usuario pondrá su clave pública a disposición de la

ADSIB a través de su cuenta de usuario. El proceso de la generación de claves es privado, la ADSIB no intervendrá en ningún momento del mismo, así el usuario garantizará que un tercer no ha tenido conocimiento de su clave privada.

El titular sólo puede utilizar la clave privada y el certificado para usos autorizados en este documento.

El usuario es el único responsable de la custodia y cuidado de su clave privada.

En caso de verse comprometida su clave privada, el usuario deberá suspender o revocar su firma a través de su cuenta de usuario o contactarse con la ADSIB, sin menoscabo de responder personalmente por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados por parte de terceras personas.

Renovación del certificado

Se realizará la renovación del certificado cuando se haya cumplido la validez del certificado, de 365 días calendario. Todo certificado generado por la ADSIB podrá ser renovado, siempre y cuando sean cumplidas las siguientes condiciones:

1. Que la firma o certificado digital no haya sido revocado por la ADSIB por razones de uso ilícito de la firma o certificado electrónico, según corresponda.

2. Que el solicitante cumpla con el proceso de solicitud y validación.

Suspensión y reactivación del certificado

No se realizan cambios de clave de certificados. En caso de ser necesario, el usuario podrá optar por la suspensión del certificado y su posterior reactivación.

La suspensión del certificado generado por ADSIB, precede a la reactivación o revocación, y se realiza a solicitud del titular del certificado.

Todo certificado generado por ADSIB podrá ser reactivado, siempre y cuando el usuario haya solicitado la misma. En caso de lo contrario, se procede a la revocación de la certificación.

Se procederá a la suspensión del certificado, siempre y cuando se cumplan las siguientes condiciones:

1. Que el usuario haya notificado la posibilidad de perdida del token que contiene el certificado digital.
2. Que el usuario haya notificado la posibilidad de que su clave privada ha sido comprometida por algún motivo.

Procedimiento de reactivación de claves del certificado

Las personas que deseen reactivar su par de claves deberán seguir el siguiente procedimiento.

a) Ingresar a su cuenta de usuario en el sistema de la página web: www.firmadigital.bo
b) Solicitar mediante su cuenta de usuario la reactivación.
c) Si el usuario evidencia que su clave ha sido comprometida o notifica la perdida podrá solicitar la revocación de su certificado mediante su cuenta de usuario.

Reemisión de claves del certificado

Se procederá a la reemisión de un nuevo certificado, siempre y cuando se cumplan las siguientes condiciones:

1. Que el usuario haya notificado la perdida del token (hsm) que contiene el certificado digital.
2. Que el usuario haya notificado que su clave privada ha sido comprometida por algún motivo

En estos casos, el usuario deberá seguir los siguientes pasos:

a) Ingresar a su cuenta de usuario en el sistema de solicitud de certificados disponible en la página web www.firmadigital.bo.
b) Solicitar mediante su cuenta de usuario la revocación del certificado comprometido.
c) Solicitar mediante su cuenta de usuario la remisión del certificado; de esta manera no realizará el pago por la emisión del nuevo certificado.
d) Realizar el procedimiento inicial de registro y proceder con la generación de su nuevo par de claves como se indica anteriormente.

El usuario podrá solicitar la reemisión de certificados por pérdida del token (hsm) o encontrarse comprometida su clave privada por un máximo de tres veces, al cabo de las cuales deberá cancelar nuevamente por el servicio de certificación digital.

Suspensión y revocación del Certificado

La suspensión del certificado generado por la ADSIB, usualmente precede a la revocación. Ambos se

harán de acuerdo a los procedimientos internos con los que la ADSIB trabaja y a solicitud del usuario o autoridad competente. La ADSIB podrá suspender o revocar un certificado por motivos fundamentados técnica y legalmente, interés nacional, resguardo de la seguridad del Estado Plurinacional de Bolivia o interés del pueblo boliviano, mediante Resolución Administrativa de su Máxima Autoridad Ejecutiva.

Procedimiento de revocación

Se procederá a la revocación de un certificado en los siguiente casos:

a. En caso que el usuario haya notificado la perdida del dispositivo y/o que su clave privada haya estado comprometida en algún caso.
b. Por vencimiento de la validez del certificado.

En estos casos, el usuario deberá seguir los siguientes casos.

a) Ingresar a su cuenta de usuario en el sistema de solicitud de certificados disponible en el sistema de solicitud de certificado de la página web www.firmadigital.bo.
b) Solicitar media su cuenta de usuario la revocación del certificado.

Servicios de estado de certificados

La ADSIB posee servicios de comprobación de estado de los certificados. Dichos servicios son la lista de certificados revocados y el acceso OCSP para acceso en línea a la comprobación del estado de las mismas.

Fin de la suscripción

El usuario podrá dar el uso permitido al certificado durante su período de vigencia. Llegado a término del período de vigencia del certificado, el usuario podrá optar al proceso de renovación. Si el usuario no opta por la renovación, tendrá a su disponibilidad en los archivos de la ADSIB por un lapso 5 años los registros correspondientes a la generación de su certificado.

Depósito de las claves y recuperación.

Si el usuario no opta por la renovación o reactivación, tendrá a su disponibilidad en los archivos de la

ADSIB por un lapso de 5 (cinco) años, los registros correspondientes a la generación de su certificado.

La clave privada de la ADSIB se custodia en un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas es necesario el uso de tarjetas inteligentes.

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.

- **Ubicación y construcción**

La ubicación del Centro de Datos de la ADSIB está en el Edificio de la Vicepresidencia del Estado Plurinacional de Bolivia, ubicado en el centro de la ciudad de La Paz, entre las calles Ayacucho y Mercado No 308.

La construcción del Centro de Datos reúne y mantiene los requisitos de operación que para este tipo de facilidades 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.

Adicionalmente el Centro de Datos reúne condiciones y características de construcción para hacer frente a diferentes situaciones de emergencia. Igualmente, mantiene un perímetro de seguridad y cuenta con cinco (5) niveles de acceso biométrico.

El Centro de Datos desde donde opera la ADSIB, mantiene respaldos en caso de ocurrencia de una contingencia que afecta la integridad física y digital de la referida sede administrativa y puede ofrecer de esa manera una garantía de su continuidad operacional.

- **Acceso físico**

Se mantienen medidas de control de acceso tanto lógicas (aplicativo de certificación) como físicas (equipos) 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 los servidores donde está instalado el gabinete de la firma digital.

Además de procedimientos de seguridad que restringen el acceso solo a personal autorizado para el

acceso a cada una de las cinco (5) capas de seguridad física y conocer la información de acceso a los equipos que conforman la cabina de la Firma Digital.

- **Alimentación eléctrica y aire acondicionado**

La construcción donde se encuentran instalados los servidores de la cabina de la Firma Digital de la ADSIB cuenta con fuentes de energía ininterrumpida (UPS), las cuales a su vez están conectadas a una (1) planta generadora de energía.

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

- **Protección y prevención de incendios**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad, la construcción aísla posibles incendios dadas las divisiones y materiales, además de contar con un sistema anti- incendios.

- **Exposición al agua**

El centro de datos, como las oficinas de archivo, se encuentran protegidos de la exposición al agua desde su estructura de construcción.

- **Sistema de almacenamiento**

La construcción reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa, al contar con planes y procedimientos de mantenimiento.

- **Eliminación de residuos**

La ADSIB cuenta con los procedimientos y servicios para la eliminación de residuos en todas sus instalaciones.

- **Copia de seguridad**

El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades

impone la normativa, al contar con planes y procedimientos de gestión de incidentes y respaldos de la información necesaria.

5.2 Controles de procedimientos.

- **Roles de confianza**

La ADSIB 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 ADSIB, se encuentra dividida en funciones de operación y administración. La Dirección Ejecutiva se constituye en el nivel con mayor poder de decisión y mando dentro de la organización. Las actividades de planificación serán coordinadas por la Encargada de Planificación y Proyectos en adición a las Unidades encargadas de la implementación, mantenimiento y actualización del Centro de Datos.

Todas las decisiones que se realizaren a las operaciones técnicas y administrativa serán evaluadas por el Comité de Gestión de Calidad.

- **Número de personas requerida por tarea**

El número de personas requeridas por tarea y establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Dirección Ejecutiva.

- **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 de personal.

- **Requerimientos de calificación, experiencia y acreditación**

El personal involucrado en el control y la operación de la firma y certificado digital estará suficientemente calificado y con la experiencia necesaria para cumplir con las funciones asignadas a su rol y recibirá entrenamiento continuo para garantizar los niveles de calidad sobre las políticas de seguridad y los procedimientos.

- **Formación y frecuencia de actualización de la formación.**

El personal de la ADSIB recibe capacitación en áreas de desarrollo asociada a su labor directa u orientadas al desarrollo de destrezas necesarias. Todo cambio en las políticas o sistemas de la Firma Digital implica necesariamente el proceso de capacitación del personal.

- **Frecuencia y secuencia de rotación de tareas**

La asignaciones de roles y funciones dentro de la 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.

- **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 y por escrito de la Dirección Ejecutiva de la ADSIB, de lo contrario será considerado como acto de sabotaje a los fines internos de la ADSIB y será sancionado conforme a la normativa vigente y el Reglamento Interno de Personal, por incumplimiento de las obligaciones que impone la relación de trabajo.

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

La contratación de personal de la ADSIB se basa en la normativa vigente para los funcionarios públicos.
El cumplimiento de tareas se realiza a través de informes y seguimiento trimestral del Plan Anual de Operaciones.
El personal que finaliza un contrato o deja la institución debe cumplir con los procedimientos administrativos correspondientes y guardar confidencialidad sobre la información a la que tuvo acceso en la entidad.

5.4 Procedimientos de control de seguridad.

- **Tipos de eventos registrados**

La ADSIB, almacena registros electrónicos de eventos relativos a su actividad como Entidad Certificadora Pública. Estos registros son almacenados de forma automática. Los registros generados automáticamente por cada equipo serán mantenidos por la ADSIB. Los registros pueden ser archivados en papel o en forma digitalizada.

- **Frecuencia de procesado de registros**

Se realiza en cualquier momento que se considere necesario, por razones técnicas o de seguridad. Una vez concluida la revisión se eleva informe respectivo sobre cualquier anomalía.

- **Periodo de retención para los registros de auditoría**

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

- **Protección de los registros de auditoría, procedimientos de copia de seguridad de los registros de auditoría, sistema de recogida de información de auditoría, notificación al sujeto causa del evento, análisis de vulnerabilidades.**

El sistema de recolección de auditoría de la ADSIB es una combinación de procesos automáticos y procedimientos manuales desempeñados por el personal operacional.

Por lo tanto, el sistema es mantenido mediante mecanismos de control de acceso y separación de roles con relación al software y el hardware que manejan la recolecciones automáticas y mediante procedimientos operacionales confidencialmente documentados, conocidos y seguidos por el personal de la ADSIB.

La ADSIB tiene planes y procedimientos para el análisis de vulnerabilidades en el desempeño de sus funciones.

5.5 Archivo de informaciones y registros.

- **Tipo de informaciones y eventos registrados**

La ADSIB archivará la información referente a:

a) solicitud de certificados
b) firma de certificados

c) suspensión, renovación y revocatoria de certificados
d) registro de usuarios
e) acciones que afecten los equipos criptográficos
f) operaciones sobre los sistemas de firma de certificados.

- **Periodo de retención para el archivo**

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

- **Sistema de recogida de información para auditoría, procedimientos para obtener y verificar información archivada**

Cada uno de los servidores de certificación posee un módulo para almacenar los registros de eventos, específicamente eventos de certificación. Este registro de eventos permite auditar y verificar los intentos de accesos, los accesos y las operaciones dañinas, sean estas intencionales o no, como también las operaciones normales realizadas para la firma de los certificados.

5.6 Cambio de clave de la Entidad Certificadora Pública.

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

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

5.7 Recuperación de la clave de la Entidad Certificadora Pública .

La ADSIB cuenta con un plan de continuidad de negocio y recuperación de ante desastres, ante el evento de un eventual compromiso parcial o total de la construcción del Centro de Datos. El Plan de recuperación ante desastre es revisado periódicamente a la luz de los cambios riesgos en el ambiente.

El plan de recuperación ante desastre está orientado a:

- Fallas/corrupción de recursos de computación;

- Compromiso de la integridad de la clave; y

- Desastres naturales y terminación.

La Dirección Ejecutiva debe tomar los correctivos y emprender las actividades necesarias para restablecer el sistema de certificación en el momento de presentarse un escenario de desastre. En el plan de continuidad de negocio y recuperación ante desastre, se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre.

5.8 Cese de actividades de la Entidad Certificadora Pública.

La ADSIB tienen establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones. La ADSIB tiene contemplado en la eventualidad que ocurra una cesación de operaciones, los siguientes supuestos:

- Extinción por vencimiento de acreditación: Proceder conforme a la Ley a solicitar la renovación de acreditación ante la ATT.
- Suspender la venta de certificados digitales a partir de la fecha de notificación del cese de operación a la ATT; y colocar a disposición de la ATT lo correspondiente a los certificados que se encuentren vigentes, hasta tanto se produzca el vencimiento de la totalidad de los certificados que hayan sido emitidos por la ADSIB.
- En el caso de ocurrencia de cualquier de los supuestos antes indicados y luego de operado el cese de operaciones, la ADSIB colocará a disposición de la ATT, el repositorio de todos los certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos.

6. Controles de Seguridad Técnica.

6.1 Generación e instalación del par de claves.

- **Generación del par de claves**

La ADSIB genera su par de claves (pública y privada) bajo el procedimiento establecido los procedimientos de la entidad y en cumplimiento de la normativa vigente con respecto a la firma digital y las regulaciones de la ATT.

Esto incluye el desarrollo de una ceremonia de generación del par de claves en presencia de representantes de la Vicepresidencia del Estado (ente tutor de la ADSIB), la ATT y Notario de Fe

Pública.

El resguardo de la clave privada se desarrolla conforme a la regulación establecida por la ATT.

- **Tamaño de las claves**

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

- **Parámetros del certificado 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, los cuales cumplen con los requerimientos establecidos en la normativa regulatoria, definidos en el punto 2 "Formato para el Certificado Digital de una ECA" del "ANEXO 1: Formato de los certificados digitales y de la lista de certificados revocados" del RAR ATT-DJ-RA TL LP 32/2015 de fecha 09 de enero de 2015.

- **Hardware y software de generación de claves**

El software utilizado por la ADSIB para la generación del par de claves y certificados es desarrollado por la misma entidad. La ADSIB utiliza un módulo criptográfico para almacenar de forma segura su clave privada. A los efectos de documentar y proveer información del hardware criptográfico utilizado por la ADSIB se señala en su dirección web.

- **Fines del uso de la clave.**

La clave privada de la ADSIB puede ser usada para:

- Firma de certificados establecidos en la presente DPC.
- Firma de certificados para la firma de Listas de Revocación de Certificado y/o OCSP.
- Firma de certificados para la certificación cruzada, aprobada por la ATT.

6.2 Protección de la clave privada.

- **Estándares para los módulos criptográficos**

El módulo criptográfico usado por la Clave Pública de la ADSIB está certificado para cumplir con los requerimientos establecidos por la normativa de la ATT.

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

- **Control multi-persona de la clave privada**

Se utiliza un control multipersonal para la clave privada, según los roles asignados a los funcionarios de la ADSIB y que participan de las ceremonias de firma de certificados.
El control multi-persona 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 token 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 multi-persona ninguna persona pueda acceder al HSM sin la cooperación de otros titulares.

- **Custodia de la clave privada**

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

- **Instalación física**

Creación del Mundo de Seguridad: Se creará el Mundo de Seguridad bajo los comandos establecidos y siguiendo los siguientes parámetros: Se crearán dos (2) tarjetas de Operador, una para acceder al HSM y la otra para respaldo. Se crearán cuatro (4) tarjetas de administrador (cifrado de la clave privada de ADSIB), dos (2) tarjetas de operador (Acceso al módulo criptográfico).

- **Copia de seguridad de la clave privada**

La clave privada de la ADSIB están resguardadas en módulos HSM protegidos física y lógicamente.

- **Archivo de la clave privada**

La clave privada de la ADSIB se encuentra almacenada en un componente de hardware denominado HSM, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son almacenados en una unidad de cinta, la cual la ADSIB, se asegurará de mantener a resguardo en un lugar seguro y fuera del Data Center.

- **Introducción de la clave privada al módulo criptográfico**

La ADSIB ha establecido los parámetros y lineamientos bajo los cuales se hará la generación de claves, las mismas se detallan a continuación:

- Se generará el nuevo Mundo de Seguridad.
- Se instalará la AC 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.

- **Método de activación de la clave privada**

Para la activación de la clave privada es necesario utilizar tarjetas inteligentes, requiere dos de cuatro tarjetas de administrador y una de dos tarjetas de operador, adicionalmente, es necesario el acceso al sistema operativo del servidor de certificación.

- **Método de desactivación de la clave privada**

Una vez finalizada la firma de certificados el módulo criptográfico y el servidor HSM son desactivados.

- **Método de destrucción de la clave privada**

La destrucción de la clave privada implica, generalmente, la revocatoria 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.

- **Clasificación de los módulos criptográficos.**

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

- **Almacenamiento de la clave privada en un módulo criptográfico**

La clave privada se genera directamente en el módulo criptográfico en el momento de la creación de las mismas y bajo los procedimientos establecidos.

- **Método de activación de la clave privada**

La clave privada de la ADSIB, se activa mediante el acceso físico a los servidores HSM mediante un sistema de autenticación multipersonal y la activación de la clave privada.

Todos los involucrados en la ceremonia firma de certificados participan del sistema de autenticación.

6.3 Otros aspectos de la gestión del par de claves.

- **Archivo de la clave pública**

La ADSIB publica su clave pública hasta el vencimiento del último certificado emitido por la misma.

- **Períodos operativos de los certificados y período de uso para el par de claves**

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

6.4 Datos de activación.

- **Generación e instalación de los datos de activación**

La ADSIB ha desarrollado los procedimientos para la generación de claves de activación de la clave privada del módulo criptográfico, basado en un procedimiento multipersonal.

- **Protección de los datos de activación**

Solo el personal autorizado de la ADSIB posee las claves necesarias para la activación de la clave privada bajo el sistema multipersonal y son responsables de su custodia.

- **Otros aspectos de los datos de activación**

Las claves de acceso son confidenciales, personales e intransferibles

6.5 Controles de seguridad informática.

La ADSIB ha 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.

- **Requerimientos técnicos de seguridad específicos**

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

La ADSIB ha definido una serie de controles de seguridad aplicables a los equipos informáticos, incluyendo:
a) Definición de roles y responsabilidades;

b) Controles de acceso físico y lógico;

c) Seguridad física de ambientes y sistemas;

d) Gestión de copias de seguridad;

e) Registros de auditoría;

f) Respuesta ante incidentes.

- **Evaluación de la seguridad informática**

Todo el software utilizado por la ADSIB pasa por controles y pruebas de seguridad. Anualmente se realizan revisiones de los sistemas utilizados.

6.6 Controles de seguridad del ciclo de vida.

Los controles de seguridad se enmarcan en los lineamientos establecidos en la Resolución Administrativa RAR -DJ-RA TL LP 31/2015 emitida por la ATT.

- **Controles de desarrollo de sistemas**

Los sistemas utilizados por la ADSIB pasan por revisiones y pruebas de seguridad según procedimiento. Los sistemas desarrollados por la ADSIB están documentados.
Toda modificación al código, reemplazo o actualización, o cambio de configuración de los sistemas pasa por un riguroso proceso de prueba y seguridad, acorde a procedimientos establecidos.

- **Controles de gestión de seguridad**

Las pruebas de funcionamiento son periódicas y el monitoreo permanente. Todos los procedimientos en cuanto a seguridad han sido establecidos para el funcionamiento de la entidad.

- **Controles de seguridad del ciclo de vida de los sistemas**

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 emisión de certificados por parte de la ADSIB son mantenidos "off-line" bajo estricto control de acceso y seguridad.

La emisión de listas de revocación se realiza con una clave distinta a la de emisión de certificados. El proceso de firma de listas de revocación se realiza "off line", sólo las listas de certificados revocados se encuentran en línea y a disposición pública.

La red para la publicación de certificados de revocatoria se encuentra protegida por firewall y los sistemas protegidos contra virus y software malicioso. El acceso de los usuarios a sus cuentas de

usuario en el sistema de la ADSIB está controlado y cifrado.

6.8 Controles de los módulos criptográficos.

La ADSIB únicamente utiliza módulos criptográficos con certificación FIPS 140-2

- **Registro de tiempo**

Los sistemas y servidores de la ADSIB se encuentran sincronizados en fecha y hora y guardan registros de todas las actividades.

7. Perfil de certificados y de Listas de certificados revocados.

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

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

a) Versión (version): el valor del campo es 2.
b) Número de Serie (serialNumber): Número asignado por la ECR, valor hasta de 20 octetos.
c) Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA)
d) Nombre del Emisor (issuer): CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
e) Periodo de validez (validity): Fecha de emisión del Certificado; Fecha de caducidad del Certificado. (YYMMDDHHMMSSZ, formato UTC Time).
f) Nombre suscriptor (subject): CN = Entidad Certificadora Raiz de Bolivia; O = ATT; C = BO de acuerdo a ISO3166.
g) Información de la clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 4096 bits.

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

a) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey.
b) Uso de Claves (keyUsage): digitalSignature = 0, nonRepudiation = 0, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 1, cRLSign = 1, encipherOnly = 0, decipherOnly = 0.

c) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
d) Restricciones Básicas (basicConstraints): CA = TRUE, pathLenConstraint = "1".
e) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).

7.2 Perfil del Certificado de la ECP

1. El formato para el Certificado Digital de la ADSIB tendrá los siguientes atributos y contenidos:

a) Versión (version): el valor del campo es 2.
b) Número de Serie (serialNumber): Número asignado por la ECR.
c) Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
d) Nombre del Emisor (issuer): CN = Entidad Certificadora Raiz de Bolivia; O =ATT; C = BO de acuerdo a ISO3166.
e) Periodo de validez (validity): Fecha de emisión del Certificado, Fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time).
f) Nombre suscriptor (subject): CN ="Entidad Certificadora ADSIB"; O = "ADSIB"; C = "BO".
g) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 4096 bits.

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

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

7.3 Perfil de la CRL de la Entidad Certificadora Raíz.

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

a) Versión (versión): el valor del campo es 1 (corresponde a la versión 2 del estándar)

b) Algoritmo de firma (signatureAlgorithm): Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Pública para firmar la Lista de Certificados Revocados
c) Nombre del Emisor (Issuer): CN =”Entidad Certificadora ADSIB”; O = “ADSIB”; C = “BO”.
d) Día y Hora de Vigencia (This Update): Fecha de emisión de la CRL (YYMMDDHHMMSSZ, formato UTC Time)
e) Próxima actualización (Next Update): Fecha límite de emisión de la próxima CRL (YYMMDDHHMMSSZ, formato UTC Time)
f) 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:

a) 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)
b) Número de Lista de Certificados Revocados (CRL Number): número entero de secuencia incremental para una CRL y una Entidad Certificadora determinadas.
c) Extensiones de un elemento de la Lista de Certificados Revocados.
d) Código de motivo (Reason code): indica la razón de revocación de un elemento de la CRL

7.4 Perfil del OCSP

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

i. El requerimiento de inclusión de los siguientes datos en las consultas OCSP:

a) Versión (version)
b) Requerimiento de servicio (service request).
c) Identificador del certificado bajo consulta (target certificate identifier).
d) Extensiones que puedan incluirse en forma opcional (optionals extensions) para su procesamiento por quien responde.

Cuando se recibe una consulta OCSP, quien responde debe considerar al menos los siguientes aspectos:

a) Que el formato de la consulta sea el apropiado
b) Que quien responde sea una entidad autorizada para responder la consulta.
c) Que la consulta contenga la información que necesita quien responde
d) 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.

ii. 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.

iii. Una respuesta a una consulta OCSP debería contener:

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

Las respuestas OCSP deben estar firmadas digitalmente por la Entidad Certificadora Autorizada correspondiente o por una entidad habilitada a tal efecto 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.

7.5. Formato para el Certificado Digital de un Persona Natural o Física.

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

a) Versión (version): El valor del campo es 2.
b) Número de Serie (serialNumber): Número asignado por la ECA.
c) Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
d) Nombre del Emisor (issuer): CN = "Entidad Certificadora" y el nombre de la ECA; O = Razón social

de la ECA;C=BO de acuerdo a ISO3166

e) Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
f) Nombre suscriptor (subject): CN = Nombres y Apellidos de la persona natural; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).
g) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

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

a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier): Valor de la Extensión subjectKeyIdentifier del certificado de la ECA emisora.
b) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función Hash (SHA1) del atributo subjectPublicKey.
c) Uso de Claves (keyUsage): digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1, keyAgreement = 0, keyCertSign = 0, cRLSign = 0, encipherOnly = 0, decipherOnly = 0.
d) Uso de Claves Extendido (Extended Key Usage): clientAuth, EmailProtection, codeSigning.
e) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
f) Restricciones Básicas (basicConstraints): CA = FALSE.
g) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).
h) Información de Acceso de la ECA (authorityInformationAccess): URI:(.crt).
i) Nombre Alternativo del Suscriptor (subjectAlternativeName): E = Correo electrónico del suscriptor

7.6. Formato para el Certificado Digital de una Persona Jurídica

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

- Versión (version): El valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECA
- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA)..
- Nombre del Emisor (issuer): CN = “Entidad Certificadora”; y el nombre de la ECA; O= Razón social de la ECA; C = BO de acuerdo a ISO3166.
- Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones; O = Razón social de la empresa o institución a la que representa la persona jurídica; OU = Unidad Organizacional de la que depende (opcional); T = Cargo del representante legal; C = estándar de acuerdo a ISO 3166 {BO};

dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: mínimo 2048 bits.

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

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

7.7. Formato para el Certificado Digital de Cargo Público

i. El formato para el Certificado Digital de Cargo Público tendrá los siguientes atributos y contenidos:

- Versión (version): El valor del campo es 2.
- Número de Serie (serialNumber): Número asignado por la ECA.
- Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
- Nombre del Emisor (issuer): CN = “Entidad Certificadora”; y el nombre de la ECA; O = Razón social de la ECA; C = BO de acuerdo a ISO3166.
- Periodo de validez (validity): Fecha de emisión del Certificado, fecha de caducidad del Certificado (YYYYMMDDHHMMSSZ, formato UTC Time).
- Nombre suscriptor (subject): CN = Nombres y Apellidos del servidor público; O = Nombre de la institución pública a la que pertenece; OU = Unidad Organizacional de la que depende el funcionario público (opcional); T = Cargo del servidor público; C = estándar de acuerdo a ISO 3166 {BO}; dnQualifier = Tipo de documento {CI/CE}; uidNumber = Nro. de documento {numeral}; uid = número de complemento {alfanumérico} (opcional); serialNumber = Número de NIT {numeral} (opcional).

- Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 2048 bits.

ii. Las extensiones del Certificado Digital de Cargo Público serán las siguientes:

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

8. Auditoría de conformidad.

8.1 Frecuencia de los controles de conformidad para cada entidad.

Las auditorías de control y seguimiento ordenadas por ley e impuestas por mandato de la ATT, serán efectuadas por el calendario coordinado entre las entidades.

9. Requisitos comerciales y legales.

9.1 Tarifas.

Serán publicadas en la página web de la Firma Digital.

9.2 Política de confidencialidad.

Toda la recopilación y uso de la información compilada por la ADSIB es realizada cumpliendo con la legislación del Estado Plurinacional de Bolivia y basándose en las distinciones suministradas en este Documento de Declaración de Prácticas de Certificación.

9.3 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, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.

Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes.

Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro; Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente; El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica, y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Al optar por el servicio de Firma Digital, el usuario acepta la publicación por parte de la ADSIB de la información contenida en su clave pública y el certificado firmado por la ADSIB.

9.4 Obligaciones de los participantes de la PKI.

Para garantizar la publicidad, seguridad, integridad y eficacia de la firma y certificado digital, las entidades certificadoras están obligadas a:

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, baja suspensión, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web.
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 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 establecidas en la presente Declaración de Prácticas de Certificación. Las causales y condiciones bajo las cuales deba efectuarse la revocatoria deben ser estipuladas en los contratos de los titulares.
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 periodo 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.

- **Responsabilidad de las autorizadas ante aceptantes**

Entidades Certificadoras

I. Las entidades certificadoras autorizadas serán responsables por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios.
II. La entidad certificadora autorizada 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.
III. Las entidades certificadoras autorizadas deberán responder por posibles perjuicios que se causen al signatario o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

9.5 Modificaciones al presente documento.

Como todo documento relacionado a la implementación de Declaración de Prácticas de Certificación deberá ser revisado y actualizado en un periodo de tiempo acordado por la Dirección Ejecutiva en dependencia a las evaluaciones, comunicaciones y acciones que ocurran en el avance del trabajo de la ADSIB.

En todo caso los ajustes a la documentación requerida por la ATT para la operación de la ADSIB, serán realizados oportunamente para la aprobación del mismo. Además en cada oportunidad que ocurra un cambio en el marco normativo y legal aplicable o cuando ocurra un cambio técnico que justifique el ajuste o cambio.

9.6 Resolución de conflictos.

La ADSIB y el usuario contratante reconocen que la solución pronta y equitativa de las controversias que puedan producirse en relación con la operación, generación o venta de la firma y certificados digitales redundará tanto en sus propios intereses como en la ejecución del servicio contratado.

A este fin, manifiestan su decisión de realizar todos los esfuerzos posibles para resolver todas las controversias que puedan plantearse mediante negociación a los niveles pertinentes. Si la controversia no se ha resuelto a través de la negociación antes referida, dentro de los quince (15) días hábiles después de iniciada la misma, entonces, a solicitud del usuario contratante se someterá la controversia a la ATT, organismo rector en la materia de certificación. En caso de no llegar a ningún acuerdo quedará libre la vía de reclamo por proceso legal.

La ADSIB rechaza cualquier responsabilidad de conflictos emergentes entre terceros relacionados con la firma digital. Igualmente no se hace responsable del uso inapropiado de la firma digital de los usuarios, ni de su extravío, robo, cesión a otras personas, operaciones no permitidas en las presentes políticas o cualquier otra situación que no esté relacionada con las responsabilidades establecidas para la Entidad Certificadora Pública en la legislación boliviana vigente.

La ADSIB, salvo orden judicial de autoridad competente, no intervendrá en manera alguna en la resolución de conflictos relacionados con la firma digital de sus usuarios con terceros.

El personal de la ADSIB no tendrá en ningún momento acceso a la clave privada de los usuarios, razón por la cual exime cualquier responsabilidad con respecto a cualquier evento que comprometa dicha clave y las consecuencias derivadas de su uso.

9.7 Legislación aplicable.

Lo no previsto en el presente Documento de la Declaración de Prácticas de Certificación, será regulado de conformidad con lo establecido en la normativa legal vigente y aplicable a la materia dentro del Estado Plurinacional de Bolivia.

9.8 Conformidad con la Ley aplicable.

Todos los procesos, procedimientos, información técnica y legal contenida en el presente documento de la Declaración de Prácticas de Certificación, se encuentra en un todo elaborada y de conformidad con lo establecido en la normativa establecida por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), en cumplimiento a la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

VERSIONES:

Versión: 4
Fecha: 2 de febrero de 2016
Cambios:

- Incorporación de la mención a la RAR ATT-DJ-RA TL 1538/2015.
- Cambio de los formatos autorizados de certificados digitales según la RAR ATT-DJ-RA TL 1538/2015.
- Supresión de la mención de verificación de los datos de servidores públicos con la Contraloría.
- Supresión de la verificación de identidad por huella, en conformidad con las Políticas de certificación.
- Corrección de la información de la subsección “Subject” de la sección “Parámetros del certificado y comprobación de la calidad de los parámetros”.
- Remplazo del término “hsm” por el término “token (hsm)”.
- Nueva redacción sobre la generación del par de claves.
- Errores de ortografía.