DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Certificaciones Digitales Digicert S.R.L.

Tabla de Contenido

0. GESTIÓN DEL DOCUMENTO

Firmado digitalmente por	Firmado digitalmente por Robin	Firmado digitalmente por

Elaborado por		Revisado por		Aprobado por	
Nombre	Miguel Gutierrez	**Nombre**	Robin Caballero	**Nombre**	Jose Luis Moron
Cargo	Operador de la ECA	**Cargo**	Oficial de Seguridad	**Cargo**	Representante Legal
Fecha	2023-11-07	**Fecha**	2023-11-07	**Fecha**	2023-11-07

1. CONTROL DE CAMBIOS

1.1. CAMBIOS A LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA ECA

La Declaración de Prácticas de Certificación será revisada con una periodicidad anual por el comité de Certificaciones Digitales Digicert S.R.L., con el objetivo de incorporar los cambios derivados de los avances tecnológicos y las modificaciones en la estructura organizativa de la sociedad, las regulaciones y normas externas.

1.2. DETALLE DE CAMBIOS

Revisión	Fecha	Detalle de modificaciones
0	2016-10-13	Versión inicial del documento
1	2018-03-12	Revisión – Comentarios ATT
2	2018-07-12	Revisión – Auditoria ATT
3	2019-08-13	Revisión – Certificado PKCS12
4	2020-08-14	Modificación para la habilitación del servicio de custodia de certificados y firma digital remota ATT-DJ-RAR-TL LP 192/2020
5	2023-11-07	Actualizar Representante Legal

2. DEFINICIONES Y ABREVIATURAS

2.1. ABREVIATURAS

- **EC:** Entidad Certificadora.
- **ECA:** Entidad Certificadora Autorizada.
- **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:** (*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.
- **CRL:** (*Certificate Revocation List*) Lista de Certificados Revocados.
- **ATT:** Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- **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.
- **OID:** (*Object Identifier*) Identificador de Objeto.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **TSP:** (Trust Service Provider) Proveedor de Servicios de Confianza
- **CA:** (Certification Authority) Autoridad de certificación

2.2. DEFINICIONES

a) **Certificado Digital:** Es un documento digital formado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma 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:** 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 digital sobre un mensaje electrónico de datos o documento digital.

c) **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 de signatario en el Certificado Digital

d) **Solicitud de firma de certificado:** Una solicitud de firma de certificado (Certificate Signing Request - CSR) es un archivo digital que un solicitante transmite a una Autoridad de Certificación para obtener la firma de su certificado. La solicitud de firma de certificado contiene los datos de identidad y la clave pública del solicitante, adicionalmente, está firmada con la clave privada del solicitante para certificar que la solicitud es auténtica.

e) **Firma electrónica:** Es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de algunos de los requisitos legales para ser considerada firma digital.

f) **Firma digital:** Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

3. INTRODUCCIÓN

3.1. PRESENTACIÓN

El presente documento constituye la Declaración de Prácticas de Certificación (*Certificate Practice Statement*) de Certificaciones Digitales Digicert S.R.L. (a partir de ahora CPS), emitido en cumplimiento a las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015**, ATT-DJ-RA TL LP 32/2015 , ATT-DJ-RA TL LP 1538/2015 y ATT-DJ-RAR TL LP 209/2019 formuladas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), de acuerdo a la Ley N° 164 General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo N° 1793.

3.2. OBJETIVO Y ALCANCE

3.2.1. OBJETIVO

El objetivo del presente documento se limita a definir y describir las políticas, prácticas y procedimientos empleados por Certificaciones Digitales Digicert S.R.L. para brindar Servicios de Certificación. Pretendiendo dar transparencia al conjunto de tareas relacionadas con la provisión de estos servicios.

3.2.2. ALCANCE

El alcance del documento se limita a todas las tareas relacionadas con la prestación de Servicios de Certificación y las personas involucradas en ellas.

Esta CPS asume que el lector conoce los conceptos de PKI, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

La presente CPS es conforme con la especificación del RFC 2527 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" propuesto por S. Chokhani y W. Ford, del *Internet Engineering Task Force* (IETF), para este tipo de documentos, y su actualización en el RFC 3647.

La presente CPS se desprende la Política de certificación (CP).

3.3. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

El presente documento lleva como título "**Declaración de Prácticas de Certificación**".

Se publicará este documento en el sitio web de Certificaciones Digitales Digicert S.R.L. inmediatamente después de su aprobación.

3.4. PARTICIPANTES DE LA PKI BOLIVIA

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

3.4.1. PRIMER NIVEL: 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 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 públicas y privadas subordinadas.

3.4.2. SEGUNDO NIVEL: ENTIDAD DE CERTIFICACIÓN

La presente CPS especifica la actuación de Certificaciones Digitales Digicert S.R.L. como ECA privada, la cual se basa en la relación de una determinada clave pública con un sujeto concreto (ya sea este sujeto físico o fiscal) por medio de un Certificado que avala esta relación.

Certificaciones Digitales Digicert S.R.L., para la firma digital será una Entidad de Certificación subordinada a la ATT en su rol de Entidad Certificadora Raíz, cumpliendo con todas las normativas y regulaciones que ello implica en materia de certificación.

3.4.3. TERCER NIVEL: AGENCIA DE REGISTRO

La Agencia de Registro (desde ahora AR), es la encargada de la gestión de solicitudes de certificación. Entre las funciones de la gestión de solicitudes cabe destacar la de identificación de los Solicitantes de Certificados, esta identificación se lleva a cabo de acuerdo a las normas y procedimientos de esta CPS y siempre actúa en conjunto con la ECA de Certificaciones Digitales Digicert S.R.L.

El servicio de registro de Certificaciones Digitales Digicert S.R.L. es tercerizado, está sujeto a las obligaciones y responsabilidades que se derivan de lo establecido en la Declaración de Prácticas de Certificación (CPS) y en las Políticas de Certificación (CP), conforme con los estándares técnicos para el funcionamiento de las Agencias de Registro.

3.4.4. CUARTO NIVEL: SIGNATARIOS

Son todos los usuarios finales a quienes se ha emitido un Certificado por una Entidad Certificadora Autorizada, dentro de la Jerarquía Nacional de Certificación Digital.

3.4.5. OTROS: TERCEROS ACEPTANTES

Son cualquier persona física u organización que valida y confía en los certificados emitidos por una Entidad Certificadora de la PKI Bolivia, sea la Entidad Certificadora Raíz o una de las ECA.

3.5. USO DE LOS CERTIFICADOS

3.5.1. USOS TÍPICOS

El uso de los certificados emitidos por Certificaciones Digitales Digicert S.R.L. está limitado según el tipo de certificado, en el caso de los certificados de Persona Natural y Persona Jurídica (para uso simple o automático) está limitado a:

- Firma de documentos.
- Protección de correo electrónico.
- Autenticación en sitio web.
- Firma de código informático.

Cabe mencionar que para el caso de certificados de Persona Jurídica los usos definidos anteriormente serán en representación de una persona jurídica (organización) como se establece en la CP.

3.5.2. USOS PROHIBIDOS

El usuario contratante de certificados digitales generados por Certificaciones Digitales Digicert S.R.L. 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 es aplicable un proceso penal establecido en el Código Penal, Artículo 363 (alteración, acceso y uso indebido de datos informáticos).

Adicionalmente le es revocado el certificado digital y el usuario contratante asume la responsabilidad de indemnizar a Certificaciones Digitales Digicert S.R.L. 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 Certificaciones Digitales Digicert S.R.L.

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

3.5.3. 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 debe 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 una estampa 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 existe un servicio que mantenga dichas evidencias, y es necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

3.6. ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS Y PROCEDIMIENTO DE APROBACIÓN

3.6.1. ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La administración de la presente Declaración de Prácticas de Certificación es responsabilidad de Certificaciones Digitales Digicert S.R.L. Por consultas o sugerencias, Certificaciones Digitales Digicert S.R.L. designa el siguiente contacto:

Dirección de correo: contacto@digicert.bo
Teléfono: (591)(3) 3340104

3.6.2. PROCEDIMIENTO DE APROBACIÓN

El sistema documental y de organización de la CPS de Certificaciones Digitales Digicert S.R.L. garantiza, a través de la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de esta Declaración de Prácticas de Certificación y de las especificaciones de servicios que están relacionados.

La aprobación de esta Declaración de Prácticas de Certificación, así como toda modificación introducida en ella, es responsabilidad exclusiva de Certificaciones Digitales Digicert S.R.L.

4. CONCEPTOS GENERALES

4.1. CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

La custodia de certificados digitales corresponde a un servicio de confianza prestado por un TSP (una ECA en el caso de Bolivia) que consiste en la custodia (gestión terciarizada) de certificados digitales para la firma digital remota de los suscriptores por parte del mismo.

4.2. CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

Los certificados digitales para la firma digital remota son aquellos cuyo par de llaves ha sido generado por un dispositivo criptográfico HSM en poder de un TSP (una ECA en el caso de Bolivia), quien se encarga también de custodiar dichos certificado y par de llaves haciendo uso del HSM y los mecanismos criptográficos necesarios para este propósito. Como consecuencia de lo anterior, este certificado digital y par de llaves, a través de algún aplicativo software, puede ser utilizado para realizar operaciones de firma digital de carácter remoto, entendiéndose que la operación de firma digital se ejecutaría en la infraestructura del TSP que custodia los mismos.

4.2.1. CONTINUIDAD DEL SERVICIO

La gestión de la continuidad del servicio hace referencia al conjunto de prácticas, políticas, procedimientos, normas y medidas empleadas para prevenir y proteger a la empresa de los efectos que pudiera tener una interrupción de los servicios de TI, bien sea que haya sido ocasionada por alguna falla técnica o por causas naturales, o que haya sido provocada voluntaria o involuntariamente por alguna persona.

4.3. ALCANCE DEL SERVICIO DE CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

El servicio de custodia de certificados digitales para la firma digital remota tiene como alcance principal tanto la gestión y almacenamiento del par de llaves y certificado digital del suscriptor, así como también la habilitación de los medios tecnológicos para que el mismo pueda realizar operaciones de firma digital remota.

4.4. COMUNIDAD DE USUARIOS Y AMBITO DE LA APLICACIÓN

4.4.1. SUSCRIPTORES

Son suscriptores todas aquellas personas e instituciones que hayan solicitado la prestación de alguno de los servicios prestados por Certificaciones Digitales Digicert S.R.L., ya sea este únicamente la certificación digital o la custodia de certificados digitales y firma digital remota.

4.4.2. TERCEROS ACEPTANTES

Son cualquier persona física u organización que valida y confía en los certificados emitidos por Certificaciones Digitales Digicert S.R.L.

4.4.3. AMBITO DE LA APLICACIÓN

El servicio de certificación digital es aplicable a cualquier casuística en la que se necesite hacer uso de la funcionalidad de firma digital. En el caso de que se quiera que a su vez esta funcionalidad cuente con las cualidades de flexibilidad y movilidad es de mayor utilidad el uso del servicio de custodia de certificados digitales para firma digital remota.

5. POLITICA DEL SERVICIO

Este apartado es un resumen de algunos puntos estratégicos de la CP.

5.1. VISTA GENERAL

El presente apartado constituye la Política de Servicio para la emisión de certificados digitales correspondientes a cualquiera de los perfiles de certificados emitidos por Certificaciones Digitales Digicert S.R.L. La presente se encuentra en cumplimiento a las Resoluciones Administrativas Regulatorias **ATT-DJ-RAR-TL LP 202/2019**, **ATT-DJ-RAR-TL LP 209/2019** y **ATT-DJ-RAR-TL LP 192/2020** formuladas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), de acuerdo a la Ley N° 164 General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo Reglamentario N° 1793.

5.2. IDENTIFICACION DE LA POLITICA

La presente política es el apartado número 5 de la CP de Certificaciones Digitales Digicert S.R.L. CP-ECA-01 y lleva como título **Política de Servicio.**

5.3. APLICACIONES DEL SERVICIO

Algunas aplicaciones comunes de los certificados digitales brindados por Certificaciones Digitales Digicert S.R.L. son la firma digital de documentos y la protección de correo electrónico.

5.4. COMUNIDAD DE USUARIOS, APLICABILIDAD, LIMITACIONES Y PROHIBICIONES

5.4.1. COMUNIDAD DE USUARIOS

Forman parte de la comunidad de usuarios todas aquellas personas e instituciones que hayan solicitado la prestación de alguno de los servicios prestados por Certificaciones Digitales Digicert S.R.L., ya sea este únicamente la certificación digital o la custodia de certificados digitales y firma digital remota.

5.4.2. USOS PERMITIDOS

El uso de los certificados emitidos por Certificaciones Digitales Digicert S.R.L. está limitado según el tipo de certificado, en el caso de los certificados de Persona Natural y Persona Jurídica (para uso simple o automático en cualquiera de diferentes tipos de almacenes de claves disponibles) está limitado a:

- Firma de documentos.
- Protección de correo electrónico.
- Autenticación en sitio web.
- Firma de código informático.

5.4.3. LIMITES DE USO

El uso de los certificados digitales está limitado para realizar únicamente operaciones en representación del titular del certificado, ya sea bien que este esté actuando de manera independiente como persona particular o como representante de su organización.

5.4.4. PROHIBICIONES DE USO

El usuario contratante de certificados digitales generados por Certificaciones Digitales Digicert S.R.L. 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 es aplicable un proceso penal establecido en el Código Penal, Artículo 363 (alteración, acceso y uso indebido de datos informáticos).

Adicionalmente le es revocado el certificado digital y el usuario contratante asume la responsabilidad de indemnizar a Certificaciones Digitales Digicert S.R.L. por daños y perjuicios ocasionados a terceros que se generaren por el uso indebido, por parte del usuario contratante del servicio contratado con Certificaciones Digitales Digicert S.R.L.

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

6. DECLARACION DE PRACTICAS DEL SERVICIO

6.1. GESTION DE LOS MODULOS CRIPTOGRAFICOS HSM

Para el servicio de custodia de certificados digitales para la firma digital remota se utilizan HSMs nCipher (en cumplimiento de FIPS 140-2 nivel 3) en ambos ambientes, producción y contingencia, los cuales son inicializados dentro de un mismo "Security World" (framework de seguridad desarrollado por nCipher) de manera tal que podamos garantizar en cualquiera de los ambientes, el poder ejecutar cualquiera de las operaciones de gestión necesarias para prestar el servicio.

6.2. GESTION DEL CICLO DE VIDA DE LOS SLOTS

Los HSMs nCipher no manejan este concepto.

6.3. DEL PAR DE CLAVES

6.3.1. GENERACION Y PROTECCION DEL PAR DE CLAVES

Los pares de claves son generados dentro del HSM (proceso de generación de por claves "por hardware").

Una vez generados, pares de claves son protegidos en forma de "key blob" (tecnología propia de nCipher).

6.3.2. DISTRIBUCION DE LA CLAVE PUBLICA

La única forma en la cual una clave pública gestionada por el servicio de custodia de certificados digitales será distribuida es por medio de los certificados digitales de clave pública.

6.3.3. DISTRIBUCION DE LA CLAVE PRIVADA

Las claves privadas gestionadas por el servicio de custodia de certificados digitales para la firma digital remota no son distribuidas.

6.4. CSR Y CERTIFICADOS DIGITALES

6.4.1. CREACION DEL CSR

El CSR PKCS#10 es creado en el momento de la generación del par de claves, el mismo es firmado con la clave privada.

6.4.2. IMPORTAR EL CERTIFICADO DIGITAL

El proceso de importación de certificado se realiza sobre el "key blob" que contiene la clave privada correspondiente al certificado que se desea importar.

6.5. USO DE LOS CERTIFICADOS DIGITALES ALMACENADOS

Los usos de los certificados digitales custodiados están restringidos a los usos definidos para el perfil de certificado al cual corresponden.

7. OBLIGACIONES Y LIMITACION DE RESPONSABILIDADES

7.1. OBLIGACIONES

7.1.1. OBLIGACIONES CON LOS SUSCRIPTORES

La ECA tiene las siguientes obligaciones:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;
b) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
c) 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 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;
d) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del Servicio de Custodia de Certificados Digitales para la Firma Digital Remota y/o en la Nube;
e) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
f) Verificar toda la información proporcionada por el signatario del servicio, bajo su exclusiva responsabilidad;
g) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;
h) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidas y los servicios que administra.

7.1.2. OBLIGACIONES CON LA ATT

De acuerdo a lo establecido en el Art. 43 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, la ECA tiene las siguientes obligaciones:

i) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;
j) 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;
k) 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;
l) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario;
m) 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 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;
n) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del Servicio de Custodia de Certificados Digitales para la Firma Digital Remota y/o en la Nube;
o) 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;

p) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
q) Notificar a la ATT cualquier cambio en la personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos o correo electrónico;
r) Verificar toda la información proporcionada por el signatario del servicio, bajo su exclusiva responsabilidad;
s) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;
t) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidas y los servicios que administra.

7.1.3. OBLIGACIONES DE LOS SUSCRIPTORES

De acuerdo a lo establecido en el Art.55 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, el usuario tiene las siguientes obligaciones:

a) Realizar el pago por el servicio solicitado, 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 interferencias perjudiciales a operaciones debidamente autorizadas.
d) Proporcionar información fidedigna y susceptible de verificación a la ECA;
e) Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado;
f) Observar las condiciones establecidas por la ECA para la utilización del Servicio de Custodia de Certificados Digitales para la Firma Digital Remota y/o en la Nube;
g) Notificar oportunamente a la ECA 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;
h) 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 Servicio de Custodia de Certificados Digitales para la Firma Digital Remota y/o en la Nube;
i) Comunicar a la ECA cuando exista el riesgo de que los datos de su firma digital sean de conocimiento no autorizado de terceros, por el signatario y pueda ser utilizada indebidamente;
j) 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.

El incumplimiento de las obligaciones antes detalladas, hará responsable al signatario de las consecuencias generadas por el uso indebido de su firma digital.

Los suscriptores tienen la obligación de hacer un buen uso de los servicios provistos por Certificaciones Digitales Digicert S.R.L., no realizar las acciones prohibidas, así como también y respete los límites de uso establecidos en esta o cualquier otra política de la PKI boliviana.

7.2. LIMITACION DE RESPONSABILIDADES

Certificaciones Digitales Digicert S.R.L. limita sus responsabilidades a aquellas establecidas de manera contractual, las cuales no incluyen, por ejemplo, proporción de la información acerca de sus usuarios a terceras partes, exportación de claves privadas de usuarios del servicio de custodia u otras tares.

8. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

- **Repositorios**

Los repositorios públicos de información de Certificaciones Digitales Digicert S.R.L. están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de Certificaciones Digitales Digicert S.R.L., ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 2 horas.

A fin de garantizar la completa disponibilidad de este documento en la Declaración de Prácticas de Certificación y demás documentos esenciales, Certificaciones Digitales Digicert S.R.L. mantiene un repositorio en la página web del servicio de firma digital.

El repositorio público de Certificaciones Digitales Digicert S.R.L., no contiene información confidencial o privada.

- **Publicación**

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

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 Certificaciones Digitales Digicert S.R.L., ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 72 horas.

- **Frecuencia de actualización**

Certificaciones Digitales Digicert S.R.L. 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**

Certificaciones Digitales Digicert S.R.L. 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 Certificaciones Digitales Digicert S.R.L. 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, al servidor OCSP y el presente documento.

Todos los documentos publicados por Certificaciones Digitales Digicert S.R.L. en el repositorio serán firmados digitalmente por la entidad.

9. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

9.1. REGISTRO DE NOMBRES

- **Tipos de nombres**

La norma vigente define los tipos de nombres para cada uno de los dos 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 =** Número de documento {numeral};
- **uid =** Número de complemento {alfanumérico} (opcional);
- **serialNumber =** Número de NIT {numeral} (opcional).
- **description=** Nivel de seguridad

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 =** Número de documento {numeral};
- **uid =** Número de complemento {alfanumérico} (opcional);
- **serialNumber =** Número de NIT {numeral} (opcional).
- **description=** Nivel de seguridad

- **Significado de los nombres**

Certificaciones Digitales Digicert S.R.L. requerirá de los clientes contratantes de certificados digitales, sus nombres y apellidos (completos y conforme figuran en la cédula de identidad que posea el solicitante de la firma digital).

No serán admitidos o procesados por Certificaciones Digitales Digicert S.R.L. 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 Certificaciones Digitales Digicert S.R.L. 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 Certificaciones Digitales Digicert S.R.L. utilizan codificación UTF-8 para sus atributos, según el RFC 3280 ("*Internet X.509 Public Key Infraestructure and Certificate Revocation List (CRL) Profile*").

- **Unicidad de nombres**

Los nombres distintivos deben ser únicos y no inducirán a ambigüedad.

Para ello se incluirá como parte del nombre común (common name) del nombre distintivo (distinguished name) el nombre del subscriptor seguido de su número de CI, con el formato "Nombres Apellidos - CI Número de CI".

Las Políticas de Certificación pueden disponer la sustitución de este mecanismo de unicidad.

- **Resolución de conflictos relativos a nombres**

Certificaciones Digitales Digicert S.R.L. no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc.

Certificaciones Digitales Digicert S.R.L. se reserva el derecho de rechazar una solicitud de certificado por causa de conflicto sobre el nombre.

9.2. EMISION DE CERTIFICADOS DIGITALES

- **Certificados digitales emitidos por dispositivo criptográfico basado en software**

Certificaciones Digitales Digicert S.R.L. pondrá a disposición de los solicitantes un software que le permita la generación de un par de claves (público y privada), garantizando la confidencialidad de la información, proporcionando al signatario un archivo PKCS#12 contenedor para el certificado, claves pública y privada.

El solicitante deberá generar el par de claves (público y privada) que cumpla con el estándar FIPS 140-2 nivel 1 mínimamente, y enviarlo a Certificaciones Digitales Digicert S.R.L.para la emisión del certificado y posterior envío del mismo al solicitante para el cargado en el archivo electrónico.

- **Certificados digitales emitidos por dispositivo criptográfico basado en hardware**

Certificaciones Digitales Digicert S.R.L. pondrá a disposición de los solicitantes un software que le permita al signatario la generación de un par de claves (público y privada) y almacenarlo en un dispositivo contenedor del certificado, claves pública y privada.

El solicitante deberá generar el par de claves (público y privada) que cumpla con el estándar FIPS 140-2 nivel 2 mínimamente, y enviarlo a Certificaciones Digitales Digicert S.R.L.para la emisión del certificado y posterior envío del mismo al solicitante para el cargado en el dispositivo.

9.3. VALIDACIÓN DE LA IDENTIDAD INICIAL

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

El esquema de operación de Certificaciones Digitales Digicert S.R.L. y su sistema de certificación se encuentran configurados para funcionar en base a una estructura de clave pública.

En virtud de lo anterior, una vez emitido cada certificado, el usuario es responsable por la custodia y resguardo de su clave privada. En caso de denuncia de extravío de su clave privada, se procederá a la suspensión y/o revocación de la firma digital luego de las validaciones correspondientes.

Certificaciones Digitales Digicert S.R.L., en ningún momento poseerá u obtendrá la clave privada del usuario. El resguardo, uso y administración de la misma es responsabilidad exclusiva del usuario.

- **Autenticación de la identidad de los titulares**

Certificaciones Digitales Digicert S.R.L. procederá a autenticar y validar la identidad de los usuarios dependiendo del tipo de certificado que soliciten. A continuación, se detallan los documentos requeridos para concretar el proceso de identificación individual para cada tipo de certificado:

Persona Natural, para los diferentes tipos de uso (simple o automático) y almacén de clave (PKCS11, con nivel de seguridad ALTO):

- Formulario de solicitud
- Carnet de identidad o carnet extranjero del solicitante.
- Ultima factura de pago de luz, agua o teléfono que permita verificar la dirección actual del solicitante.

Persona Jurídica, para los diferentes tipos de uso (simple o automático) y almacenes de clave (PKCS11 o PKCS12, con niveles de seguridad ALTO y NORMAL respectivamente):

- Formulario de solicitud
- Carnet de identidad o carnet de extranjero del Titular del Certificado Digital.
- Certificado de Inscripción al Padrón Nacional de Contribuyentes Biométrico Digital (PBD-11) y/o Documento de Exhibición de la NIT (Número de Identificación Tributaria) del solicitante.
- Carnet de identidad o carnet de extranjero del representante legal de la empresa u organización solicitante.
- Poder de nombramiento del representante legal de la empresa.

- Carta de autorización original de la persona jurídica detallando el nombre y cargo del Titular del Certificado Digital, firmada por el Representante Legal.

9.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE CLAVE

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

La renovación del certificado es posible siempre que este no haya vencido ni se haya procedido a su revocación. La cantidad máxima de renovaciones sin obligación de generar una nueva clave privada es de tres.

- **Identificación y autenticación de las solicitudes de renovación con cambio de clave privada**

La política de identificación y autenticación para la renovación de un certificado con cambio de claves será la misma que para el registro inicial, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

9.5. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE CLAVE

El procedimiento de revocación de un certificado puede realizarse mediante, mediante vía telefónica o presencial.

Las condiciones particulares para el proceso de solicitud de revocación de cada tipo de certificado se encuentran definidas en la Política de Certificación correspondiente.

Certificaciones Digitales Digicert S.R.L. puede solicitar de oficio la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomendara emprender dicha acción.

Las distintas Políticas de Certificación pueden definir la creación de una contraseña de revocación en el momento del registro del certificado.

10. CICLO DE VIDA DE LOS CERTIFICADOS

Solicitud de certificado

La Agencia de Registro de Certificaciones Digitales Digicert S.R.L. que reciba la solicitud le compete el determinar que el tipo de certificado solicitado se adecue a las características concretas del solicitante, de conformidad con el contenido de la Política de Certificación aplicable a dicho certificado y, de este modo, resolver la solicitud formulada.

En cada Política de Certificación se especifica la información que debe suministrarse con carácter previo, a quien solicite un certificado.

Emisión de certificado

Certificaciones Digitales Digicert S.R.L. no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

La emisión del certificado tendrá lugar una vez que Certificaciones Digitales Digicert S.R.L. haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es la Política de Certificación.

Cuando la ECA de Certificaciones Digitales Digicert S.R.L. emita un certificado de acuerdo con una solicitud de certificación válida, enviará una copia del mismo al solicitante y otra al repositorio de Certificaciones Digitales Digicert S.R.L.

Es tarea de Certificaciones Digitales Digicert S.R.L. notificar al subscriptor de un certificado la emisión del mismo y proporcionarle una copia.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de cada tipo de certificado.

Aceptación de certificado

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del contrato de certificación asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

Uso del par de claves y del certificado

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. pueden utilizarse, por parte de los titulares de éstos, en cualquier relación con entidades públicas o privadas, organismos, personas jurídicas o físicas que acepten los certificados.

Los certificados pueden emplearse para identificar al suscriptor de manera segura, para firmar documentos electrónicos, correo electrónico, etc. Pueden emplearse, asimismo, para cifrar información en formato electrónico de forma permanente.

Los certificados podrán ser usados para realizar Firma Digital Automática, siempre y cuando el firmado se realice en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

Los certificados digitales emitidos a través de dispositivos criptográficos basados en software solo podrán ser utilizados por Personas Jurídicas, siempre y cuando sean administrados en condiciones técnicamente seguras y confiables, que eviten su uso por terceros no autorizados.

Renovación del certificado

En cada una de las Políticas de Certificación asociadas a cada tipo de certificado emitido por Certificaciones Digitales Digicert S.R.L. se detalla la posibilidad o no de renovar los certificados, así como las condiciones para proceder a su renovación.

Renovación de claves del certificado

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

Modificación del certificado

Únicamente se pueden acordar durante el ciclo de vida de un certificado la modificación de los campos relativos a la dirección, correo electrónico y teléfono del suscriptor.

Revocación de certificados

1. Circunstancias para la revocación

Un certificado se revoca cuando:

- El subscriptor del certificado o sus claves o las claves de sus certificados se han comprometido por:
  - El robo, pérdida, revelación, modificación u otro compromiso o sospecha de compromiso de la clave privada del usuario.
  - El mal uso deliberado de claves y certificados, o la falta de observación de los requerimientos operacionales del acuerdo de suscripción, la CP asociada o la presente CPS.
- Se produce la emisión defectuosa de un certificado debido a:
  - Que no se ha satisfecho un prerrequisito material para la emisión del certificado.
  - Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
  - Un error de entrada de datos u otro error de proceso.
- El par de claves generado por un usuario final se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud se convierte en inexacta, por ejemplo, cuando el dueño de un certificado cambia su nombre.
- Una solicitud de revocación válida se recibe de un usuario final.
- Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo, una orden judicial.
- El certificado de una ECA superior en la jerarquía de confianza del certificado es revocado.

2. Entidad que puede solicitar la revocación

La revocación de un certificado se puede instar tanto por el suscriptor del mismo como por parte de Certificaciones Digitales Digicert S.R.L. Los suscriptores de certificados pueden solicitar su revocación por cualquier causa y deben solicitarla bajo las condiciones especificadas en el siguiente apartado.

3. Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente. De forma general, y sin perjuicio de lo definido en las Políticas de Certificación:

- Se aceptarán solicitudes de revocación telefónicas, las cuales podrán requerir la utilización de un código y/o contraseña generados durante la solicitud del certificado además de una identificación satisfactoria del solicitante.

- Se aceptarán solicitudes de revocación presenciales cumpliendo con los procedimientos de identificación definidos en cada Política de Certificación correspondiente.
- En el caso de producirse una solicitud de revocación sin posible verificación de la identidad del solicitante (telefónica, correo electrónico etc.), se procederá a la suspensión del certificado durante un plazo máximo de 30 días naturales, durante los que se procederá a verificar la veracidad de la solicitud. En el caso de no poder verificar la solicitud en dicho plazo, se procederá a la revocación del certificado. Es importante reseñar que el certificado no será utilizable desde el momento del procesamiento de la solicitud.
- Tras la revocación del certificado el suscriptor del mismo deberá destruir la clave privada que se corresponda con el mismo, y no hacer uso del certificado revocado. Existe un formulario de solicitud de revocación de certificados en la web de Certificaciones Digitales Digicert S.R.L., en la URL www.digicert.bo.

Una solicitud de revocación tanto si se realiza de forma presencial, electrónica (ej. página web) debe contener la información que se describe en el formulario de solicitud de revocación, recogido en cada una de las Políticas de Certificación.

Al finalizar el proceso se comunica al solicitante la revocación del certificado.

4. Período de gracia de solicitud de revocación

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso.

Suspensión de certificados

1. Circunstancias para la suspensión

La suspensión implica invalidez del certificado durante el tiempo que permanece suspendido a solicitud del usuario o contacto de revocación.

La suspensión únicamente se puede declarar de oficio por la propia Certificaciones Digitales Digicert S.R.L., cuando se ha producido una solicitud de revocación de un certificado sin posible verificación inmediata de la identidad del solicitante (telefónica, por correo electrónico sin firma digital), o cuando Certificaciones Digitales Digicert S.R.L. sospecha que se haya podido comprometer la clave privada asociada al certificado de un usuario, o si Certificaciones Digitales Digicert S.R.L. tiene dudas sobre la veracidad de los datos asociados al certificado. El plazo máximo que puede quedar suspendido un certificado por alguna de estas causas será de 30 días.

También se suspenderá un certificado si así lo dispone una autoridad judicial o administrativa, por el tiempo que la misma establezca.

2. Entidad que puede solicitar la suspensión

La suspensión de un certificado emitido por Certificaciones Digitales Digicert S.R.L. podrá ser solicitada por la propia Certificaciones Digitales Digicert S.R.L. o por una autoridad jurídica.

3. Procedimiento de solicitud de suspensión

La suspensión de un certificado deberá iniciarse por vía telefónica, contactándose con el soporte telefónico de Certificaciones Digitales Digicert S.R.L. al (591)(3) 3340104 .

4. Límites del período de suspensión

El período de suspensión de la vigencia de los certificados será normalmente de 15 días, salvo que la resolución judicial o administrativa que lo dictamine imponga un plazo superior o inferior, para lo cual, se aplicará el mismo.

Servicios de comprobación de estado de los certificados

Certificaciones Digitales Digicert S.R.L. posee servicios de comprobación de estado de los certificados. Dichos servicios son la lista de certificados revocados (CRL) y el protocolo OCSP para acceso *online* a la comprobación del estado de los mismos.

Los sistemas CRL y OCSP están disponibles durante las 24 horas los 7 días de la semana.

Requisitos de comprobación de CRL

La verificación del estado de los certificados es obligatoria para cada uso de los certificados de entidades finales. Esta comprobación puede hacerse a través de la consulta de la CRL o de otros mecanismos dispuestos por Certificaciones Digitales Digicert S.R.L.

Los terceros confiantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargarse la nueva CRL del repositorio de Certificaciones Digitales Digicert S.R.L. al finalizar el periodo de validez de la que posean.

Los certificados revocados permanecen en la CRL hasta que alcanzan su fecha de expiración. Alcanzada ésta, se eliminan de la Lista de Certificados Revocados, ante su imposibilidad de ser utilizados por estar caducados.

Requisitos de comprobación *online* del estado de los certificados

El servidor OCSP es de libre acceso y no existe ningún requisito para su uso excepto los derivados del uso del propio protocolo OCSP según se define en el RFC 2560.

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 Certificaciones Digitales Digicert S.R.L. por un lapso de cinco (5) años los registros correspondientes a la generación de su certificado.

Depósito y recuperación de las claves

La clave privada de Certificaciones Digitales Digicert S.R.L. se custodia utilizando un dispositivo de hardware criptográfico (HSM) de acuerdo con FIPS 140-2 Nivel 3 o superior nivel de seguridad. Para el acceso al repositorio de claves privadas es necesario el uso de Tokens USB configurados mediante el esquema de Shamir (m,n).

11. OPERACIÓN Y GESTION POR PARTE DE LA ECA

11.1. GESTION DE LA SEGURIDAD

Para la gestión de la seguridad se cuenta con los siguientes procesos:

- POL-ECA-01 SEGURIDAD DE LA INFORMACIÓN, el cual tiene por objeto la protección de la información contra posibles amenazas.
- PRO-ECA-03 CONTROL DE ACCESOS, el cual tiene por objeto los describir controles de acceso físicos y lógicos que se realizan dentro de la ECA.

11.2. CONTROL DE RIESGOS E INVENTARIO DE ACTIVOS

Para el control de riesgo se cuenta con el proceso POL-ECA-01 RECUPERACIÓN ANTE DESASTRES, en cual se han evaluados los riesgos asociado a la operación de la ECA.

Para el CONTROL DE INVENTARIO DE ACTIVOS FIJOS, se cuenta con un inventario de los equipos que forman parte de su infraestructura tecnológica, esta información está detallada en el documento DIT-ECA-01 DESCRIPCIÓN DE LA PLATAFORMA.

11.3. SEGURIDAD DEL PERSONAL

11.3.1. REQUERIMIENTOS DE CALIFICACIÓN, EXPERIENCIA Y ACREDITACIÓN

Certificaciones Digitales Digicert S.R.L. requiere que todo el personal que desarrolla tareas en sus instalaciones tenga la suficiente cualificación y experiencia en entornos de prestación de servicios de certificación. Todo el personal debe cumplir los requerimientos de seguridad de la organización y deben poseer:

- Conocimientos y formación sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.

11.3.2. REQUERIMIENTOS DE FORMACIÓN

El personal de Certificaciones Digitales Digicert S.R.L. está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización. Dicho plan de formación incluye los siguientes aspectos:

- Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
- Formación en seguridad de los sistemas de información.
- Conceptos básicos sobre PKI.
- Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
- Gestión de incidentes.

11.3.3. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No se ha definido ningún plan de rotación en la asignación de sus tareas para el personal de Certificaciones Digitales Digicert S.R.L.

11.3.4. SANCIONES POR ACCIONES NO AUTORIZADAS

En el caso de cometer de una acción no autorizada con respecto a la operación de Digicert S.R.L. se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, Certificaciones Digitales Digicert S.R.L. suspende el acceso de las personas involucradas a todos los sistemas de información de forma inmediata al conocimiento del hecho.

11.3.5. REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL Y CONTROLES PERIÓDICOS DE CUMPLIMIENTO

Todo el personal de Certificaciones Digitales Digicert S.R.L. debe honrar la firma del acuerdo de confidencialidad al incorporarse a su puesto. En dicho acuerdo, además, se obliga a desarrollar sus tareas de acuerdo con esta Declaración de Prácticas de Certificación (CPS), la Política de Seguridad de la Información de Certificaciones Digitales Digicert S.R.L. y los procedimientos aprobados.

El control de que el personal posee los conocimientos necesarios se lleva a cabo al finalizar las sesiones formativas y discrecionalmente, por parte del encargado de impartir estos cursos.

El control de la existencia de la documentación que los empleados deben conocer y firmar, se lleva a cabo anualmente por parte del área de Recursos Humanos.

Anualmente, el Oficial de Seguridad lleva a cabo una revisión de la adecuación de las autorizaciones otorgadas a cada empleado.

11.3.6. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Al personal que se incorpora a Certificaciones Digitales Digicert S.R.L. se le proporciona acceso a la siguiente documentación:

- Declaración de Prácticas de Certificación.
- Políticas de certificación.
- Política de Seguridad de la Información.

Se facilita acceso a la documentación relativa a normas y planes de seguridad, procedimientos de emergencia y toda aquella documentación técnica necesaria para llevar a cabo sus funciones.

11.3.7. FINALIZACIÓN DE LOS CONTRATOS

En caso de finalización de la relación laboral del personal que desarrolla sus funciones en Certificaciones Digitales Digicert S.R.L., el Oficial de Seguridad procede a llevar a cabo las acciones o comprobaciones que se detallan en los puntos siguientes, bien directamente o dando instrucciones para ello al personal adecuado:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización cuyo acceso sea restringido;
- Suprimir los privilegios de acceso del individuo a los sistemas de información de la organización, con especial atención a los privilegios de administración y a los de acceso remoto;
- Suprimir el acceso a toda información, a excepción de la considerada Pública;
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios;
- Verificar la devolución del material proporcionado por Certificaciones Digitales Digicert S.R.L. Por ejemplo: PC, llaves de mobiliario u oficinas, tarjetas de acceso, etc.

11.4. SEGURIDAD FISICA

11.4.1. UBICACIÓN Y CONSTRUCCIÓN

Los sistemas de información de Certificaciones Digitales Digicert S.R.L. se ubican en Centros de Procesamiento de Datos con niveles de protección adecuados, de acuerdo a los requisitos de la normativa en materia de seguridad.

El Centro de Datos principal opera las 24 horas del día, los 7 días a la semana y adicionalmente se cuenta con un Centro de Datos secundario, para hacer frente a diferentes situaciones de emergencia.

11.4.2. ACCESO FÍSICO

Los Centros de Procesamiento de Datos de Certificaciones Digitales Digicert S.R.L. disponen de diversos perímetros de seguridad, con requerimientos de autorización independientes. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico biométricos, sistemas de videovigilancia y de grabación, sistemas de detección de intrusos, entre otros.

Para acceder a las áreas más protegidas se requiere doble factor de autenticación.

11.4.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones disponen de UPS con una potencia suficiente para asegurar la alimentación ininterrumpida de la red eléctrica durante los períodos de apagado controlado del sistema y para proteger los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El apagado de los equipos sólo se producirá en caso de fallo de las UPS.

Se cuenta con sistema de acondicionamiento ambiental con capacidad para mantener los niveles de temperatura y humedad dentro de los márgenes de operación óptimos de los servidores, dispositivos criptográficos y equipos de comunicación.

11.4.4. EXPOSICIÓN AL AGUA

Los Centros de Datos, al igual que las oficinas de archivo, se encuentran protegidos de la exposición al agua desde su estructura de construcción.

11.4.5. PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Los Centros de Procesamiento de Datos de Certificaciones Digitales Digicert S.R.L. disponen de sistemas para la detección y extinción de incendios.

11.4.6. SISTEMA DE ALMACENAMIENTO

Los soportes de información sensible se almacenan de forma segura en armarios y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida.

El acceso a estos soportes está restringido a personal autorizado.

11.4.7. ELIMINACIÓN DE RESIDUOS

Certificaciones Digitales Digicert S.R.L. cuenta con procedimientos de eliminación adecuados para cada tipo de soporte a tratar y servicios para la eliminación de residuos en todas sus instalaciones.

11.4.8. COPIA DE SEGURIDAD

Los Centros de Datos reúnen y mantienen 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.

11.5. GESTION DE LAS OPERACIONES

Para la operativa y la gestión del servicio se han definido distintos roles y procesos internos, los cuales están bien definidos y documentados y corresponden o al Área Operativa o al Área de Tecnología.

Cualquier cambio en la operativa del proveedor del servicio involucra una actualización del documento correspondiente al procedimiento que cambia.

12. CONTROLES DE SEGURIDAD FÍSICA, GESTIÓN Y DE OPERACIONES

12.1. CONTROLES DE SEGURIDAD FÍSICA

- **Ubicación y construcción**

Los sistemas de información de Certificaciones Digitales Digicert S.R.L. se ubican en Centros de Procesamiento de Datos con niveles de protección adecuados, de acuerdo a los requisitos de la normativa en materia de seguridad.

El Centro de Datos principal opera las 24 horas del día, los 7 días a la semana y adicionalmente se cuenta con un Centro de Datos secundario, para hacer frente a diferentes situaciones de emergencia.

- **Acceso físico**

Los Centros de Procesamiento de Datos de Certificaciones Digitales Digicert S.R.L. disponen de diversos perímetros de seguridad, con requerimientos de autorización independientes. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico biométricos, sistemas de video vigilancia y de grabación, sistemas de detección de intrusos, entre otros.

Para el control de acceso físico al servidor donde se encuentra instalada la autoridad certificadora de Digicert S.R.L., se encuentran definidos 5 perímetros o niveles de seguridad. Los mismos son tenidos en cuenta para el acceso desde el exterior al gabinete donde se encuentra la autoridad certificadora y clave privada de Certificaciones digitales Digicert S.R.L.

Para acceder a las áreas más protegidas se requiere doble factor de autenticación y personal autorizado en cada nivel de acceso.

- **Alimentación eléctrica y aire acondicionado**

Las instalaciones disponen de UPS con una potencia suficiente para asegurar la alimentación ininterrumpida de la red eléctrica durante los períodos de apagado controlado del sistema y para proteger los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El apagado de los equipos sólo se producirá en caso de fallo de las UPS.

Se cuenta con sistema de acondicionamiento ambiental con capacidad para mantener los niveles de temperatura y humedad dentro de los márgenes de operación óptimos de los servidores, dispositivos criptográficos y equipos de comunicación.

- **Exposición al agua**

Los Centros de Datos, al igual que las oficinas de archivo, se encuentran protegidos de la exposición al agua desde su estructura de construcción.

- **Protección y prevención de incendios**

Los Centros de Procesamiento de Datos de Certificaciones Digitales Digicert S.R.L. disponen de sistemas para la detección y extinción de incendios.

- **Sistema de almacenamiento**

Los soportes de información sensible se almacenan de forma segura en armarios y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida.

El acceso a estos soportes está restringido a personal autorizado.

- **Eliminación de residuos**

Certificaciones Digitales Digicert S.R.L. cuenta con procedimientos de eliminación adecuados para cada tipo de soporte a tratar y servicios para la eliminación de residuos en todas sus instalaciones.

- **Copia de seguridad**

Los Centros de Datos reúnen y mantienen 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.

12.2. CONTROLES DE PROCEDIMIENTOS

Los sistemas de información y los servicios de Certificaciones Digitales Digicert S.R.L. se operan de forma segura, siguiendo procedimientos preestablecidos. Por razones de seguridad, la información relativa a los controles de procedimiento se considera material confidencial y solo se explican de forma resumida.

- **Roles de confianza**

Los roles identificados para el control y la gestión de los servicios son:

- Administrador de TI (pertenece a Certificaciones Digitales Digicert S.R.L.);
- Oficial de Seguridad (pertenece a Certificaciones Digitales Digicert S.R.L.);
- Administrador de certificados (por parte de la Certificaciones Digitales Digicert S.R.L.);
- Agente de Registro (pertenece a AR);
- Supervisor de Registro (pertenece a AR).

- **Número de personas requeridas por tarea**

Se requieren dos personas para la activación de claves de los dispositivos de generación y almacenamiento de claves, HSM. La modificación de los parámetros de configuración del hardware criptográfico implica la autenticación por parte de dos personas autorizadas y con privilegios suficientes.

- **Identificación y autenticación para cada rol**

Todos los usuarios autorizados de Certificaciones Digitales Digicert S.R.L se autentifican por medio de smart-cards criptográficas y/o dispositivos biométricos.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas de Certificaciones Digitales Digicert S.R.L.

12.3. CONTROLES DE SEGURIDAD DE PERSONAL

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

Certificaciones Digitales Digicert S.R.L. requiere que todo el personal que desarrolla tareas en sus instalaciones tenga la suficiente cualificación y experiencia en entornos de prestación de servicios de certificación. Todo el personal debe cumplir los requerimientos de seguridad de la organización y deben poseer:

- Conocimientos y formación sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.

- **Requerimientos de formación**

El personal de Certificaciones Digitales Digicert S.R.L. está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización. Dicho plan de formación incluye los siguientes aspectos:

- Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
- Formación en seguridad de los sistemas de información.

- Conceptos básicos sobre PKI.
- Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
- Gestión de incidentes.

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

No se ha definido ningún plan de rotación en la asignación de sus tareas para el personal de Certificaciones Digitales Digicert S.R.L.

- **Sanciones por acciones no autorizadas**

En el caso de cometer de una acción no autorizada con respecto a la operación de Digicert S.R.L. se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, Certificaciones Digitales Digicert S.R.L. suspenderá el acceso de las personas involucradas a todos los sistemas de información de forma inmediata al conocimiento del hecho.

- **Requerimientos de contratación de personal y controles periódicos de cumplimiento**

Todo el personal de Certificaciones Digitales Digicert S.R.L. debe honrar la firma del acuerdo de confidencialidad al incorporarse a su puesto. En dicho acuerdo, además, se obliga a desarrollar sus tareas de acuerdo con esta Declaración de Prácticas de Certificación (CPS), la Política de Seguridad de la Información de Certificaciones Digitales Digicert S.R.L. y los procedimientos aprobados.

El control de que el personal posee los conocimientos necesarios se lleva a cabo al finalizar las sesiones formativas y discrecionalmente, por parte del encargado de impartir estos cursos.

El control de la existencia de la documentación que los empleados deben conocer y firmar, se lleva a cabo anualmente por parte del área de Recursos Humanos.

Anualmente, el Oficial de Seguridad llevará a cabo una revisión de la adecuación de las autorizaciones otorgadas a cada empleado.

- **Documentación proporcionada al personal**

Al personal que se incorpora a Certificaciones Digitales Digicert S.R.L. se le proporciona acceso a la siguiente documentación:

- Declaración de Prácticas de Certificación.
- Políticas de certificación.
- Política de Seguridad de la Información.

Se facilitará acceso a la documentación relativa a normas y planes de seguridad, procedimientos de emergencia y toda aquella documentación técnica necesaria para llevar a cabo sus funciones.

- **Finalización de los contratos**

En caso de finalización de la relación laboral del personal que desarrolla sus funciones en Certificaciones Digitales Digicert S.R.L., el Oficial de Seguridad procederá a llevar a cabo las acciones o comprobaciones que se detallan en los puntos siguientes, bien directamente o dando instrucciones para ello al personal adecuado:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización cuyo acceso sea restringido;
- Suprimir los privilegios de acceso del individuo a los sistemas de información de la organización, con especial atención a los privilegios de administración y a los de acceso remoto;
- Suprimir el acceso a toda información, a excepción de la considerada Pública;
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios;
- Verificar la devolución del material proporcionado por Certificaciones Digitales Digicert S.R.L. Por ejemplo: PC, llaves de mobiliario u oficinas, tarjetas de acceso, etc.

12.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

- **Tipos de eventos registrados**

Certificaciones Digitales Digicert S.R.L. almacena registros electrónicos de eventos relativos a su actividad como Entidad Certificadora. Estos registros son almacenados de forma automática en un centralizador de logs con controles de integridad (AlienVault SIEM). Los registros generados automáticamente por cada equipo serán mantenidos por Certificaciones Digitales Digicert S.R.L. Los registros pueden ser archivados en papel o en forma digitalizada.

Dentro de los eventos registrados se encuentran:

- Accesos Físicos al Datacenter
- Alarmas del detector de intrusos (IDS)
- Eventos del firewall
- El acceso de los usuarios a los sistemas
- Los cambios de configuración
- Alarmas de potenciales incidentes de seguridad
- Escaneos de seguridad

- **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.

- **Período 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, sistema de recogida de información de auditoría, notificación al sujeto, causa del evento, análisis de vulnerabilidades**

Los registros históricos de auditoría se cifran usando la clave pública de un certificado que se emitirá para la función de auditoría de Digicert S.R.L. Las copias de respaldo de dichos registros se almacenan en las instalaciones seguras de Certificaciones Digitales Digicert S.R.L.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador de Sistemas y el Oficial de Seguridad.

- **Procedimientos de copia de seguridad de los registros de auditoría**

Se generan copias incrementales locales y remotas, de acuerdo con la Política de Copias de Seguridad de Certificaciones Digitales Digicert S.R.L.

- **Sistema de recogida de información de auditoría**

El sistema de recolección de auditorías de los sistemas de información de Certificaciones Digitales Digicert S.R.L. es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicaciones, y por el personal que las opera.

- **Notificación al sujeto causante del evento**

No estipulado.

- **Análisis de vulnerabilidades**

Se realizan análisis de vulnerabilidades periódicos de acuerdo con las Políticas y Procedimientos de Certificaciones Digitales Digicert S.R.L.

12.5. ARCHIVO DE INFORMACIONES Y REGISTROS

- **Tipos de información y eventos registrados**

Certificaciones Digitales Digicert S.R.L. archivará la información referente a:

- Solicitud de certificados;
- Firma de certificados;
- Suspensión, renovación y revocación de certificados;
- Registro de usuarios;
- Acciones que afecten los equipos criptográficos;
- Operaciones sobre los sistemas de firma de certificados.

- **Período de retención para el archivo**

Todos los registros de Certificaciones Digitales Digicert S.R.L., referentes a la operación de sus servicios de certificación son archivados conforme a la normativa de conservación de documentos especificada por la ATT.

- **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.

12.6. CAMBIO DE CLAVE DE LA ENTIDAD CERTIFICADORA

Certificaciones Digitales Digicert S.R.L. podrá cambiar su par de claves por los siguientes motivos:

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

12.7. RECUPERACIÓN DE LA CLAVE DE LA ENTIDAD CERTIFICADORA

Certificaciones Digitales Digicert S.R.L. cuenta con un plan de continuidad de negocio y recuperación de ante desastres, ante el evento de un eventual compromiso parcial o total del Centro de Datos. El Plan de recuperación ante desastre es revisado periódicamente a la luz de nuevos riesgos introducidos en el ambiente.

El plan de recuperación ante desastre está orientado a:

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

La Dirección 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.

12.8. CESE DE LAS ACTIVIDADES DE LA ENTIDAD CERTIFICADORA

Certificaciones Digitales Digicert S.R.L. tiene establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones y además cuenta con un plan de cese de actividades de acuerdo al artículo 51 del reglamento para el desarrollo de las TIC, decreto supremo Nr. 1793. Certificaciones Digitales Digicert S.R.L. tiene contemplado en la eventualidad que ocurra un cese 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 Certificaciones Digitales Digicert S.R.L.

- En el caso de ocurrencia de cualquier de los supuestos antes indicados y luego de operado el cese de operaciones, Certificaciones Digitales Digicert S.R.L. colocará a disposición de la ATT, el repositorio de todos los certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos.

13. CONTROLES DE SEGURIDAD TÉCNICA

13.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

- **Generación del par de claves**

Los pares de claves para todos los componentes internos de Certificaciones Digitales Digicert S.R.L. se generan en módulos de hardware criptográficos (HSM) con certificación FIPS 140-2 nivel 3. Los pares de claves para entidades finales se generan en función de lo estipulado en la Política de Certificación aplicable.

La generación inicial de las claves se realiza durante una ceremonia en presencia de representantes de la ATT y Notario de Fe Pública.

- **Tamaño de las claves**

Las claves de la raíz de la entidad certificadora de Certificaciones Digitales Digicert S.R.L. son claves RSA de 4096 bits de longitud.

El tamaño de las claves para cada tipo de certificado emitido por Certificaciones Digitales Digicert S.R.L. se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 2.048 bits.

- **Parámetros del certificado y comprobación de la calidad de los parámetros**

Los parámetros utilizados para la generación de los certificados se basan en el estándar X.509 y el RFC 5280 ("*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*").

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por Certificaciones Digitales Digicert S.R.L. vienen definidos por la Política de Certificación que le sea de aplicación

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

Las claves para las entidades de la PKI se generan en dispositivos HSM criptográficos con certificación FIPS 140-2 nivel 3.

El software utilizado por Certificaciones Digitales Digicert S.R.L. para la generación del par de claves y certificados es "*Enterprise Java Beans Certificate Authority*" (o EJBCA), software libre y *open source* mantenido por PrimeKey bajo una licencia GNU *General Public License*.

- **Fines de uso de la clave**

La clave privada de Certificaciones Digitales Digicert S.R.L. puede ser usada para:

- Firma de certificados establecidos en la presente CPS.

- Firma de CRL y OCSP.

Los fines del uso de la clave para cada tipo de certificado emitido por Certificaciones Digitales Digicert S.R.L. vienen definidos por la Política de Certificación que le sea de aplicación. Todos los certificados emitidos contienen las extensiones *KEY USAGE* y *EXTENDED KEY USAGE* definidas por el estándar X.509 (v3) para la definición y limitación de tales fines.

13.2. PROTECCIÓN DE LA CLAVE PRIVADA

- **Estándares para los módulos criptográficos**

Los módulos criptográficos usados por Certificaciones Digitales Digicert S.R.L. están certificados para cumplir con los requerimientos establecidos por la ATT.

Los módulos criptográficos utilizados por Certificaciones Digitales Digicert S.R.L. cumplen con el estándar FIPS 140-2 nivel 3.

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

La clave de cifrado para la clave privada de la Entidad Certificadora de Certificaciones Digitales Digicert S.R.L. se encuentra bajo control multi-personal, dividida en varios fragmentos y es necesario un mínimo de dos de esos fragmentos para poder volver a recomponer la clave.

- **Custodia de la clave privada**

Las claves privadas relacionadas a los certificados de persona natural y jurídica emitidos, son custodiadas por los mismos suscriptores en todos los casos a excepción de tratarse de certificados custodiados para la firma digital remota.

La clave privada de la Entidad Certificadora de Certificaciones Digitales Digicert S.R.L. se encuentra alojada en un dispositivo HSM con certificación FIPS 140-2 nivel 3.

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

La clave privada de Certificaciones Digitales Digicert S.R.L. está resguardada en módulos HSM protegidos física y lógicamente.

- **Archivo de la clave privada**

La clave privada de Certificaciones Digitales Digicert S.R.L. se encuentra almacenada en dispositivos de hardware criptográfico, los cuales se encargan de respaldarla y cifrarla.

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

La clave privada se crea en los módulos criptográficos al momento de la ceremonia inicial de generación de claves.

- **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 servidor de certificación.

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

Un Administrador puede proceder a la desactivación de la clave de Digicert S.R.L. mediante la detención del software EJBCA.

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

La destrucción de una clave privada suele realizarse por uno de los siguientes motivos:

- Cese del uso; o
- Compromiso de la misma (pierde la calidad de secreta).

La destrucción siempre debe ser precedida por una revocación del certificado asociado, si éste estuviese todavía vigente.

Para la destrucción de la clave privada, los dispositivos criptográficos (ya sea Token o HSM) deben reinicializarse. Durante este proceso se realiza el borrado seguro de las claves contenidas.

- **Clasificación de los módulos criptográficos**

Los módulos de hardware criptográficos (HSM) utilizados están certificados FIPS 140-2 nivel 3.

13.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

- **Archivo de la clave pública**

La clave pública de Certificaciones Digitales Digicert S.R.L. estará disponible públicamente hasta el vencimiento del último certificado emitido que deba verificarse con esta.

A su vez, Certificaciones Digitales Digicert S.R.L. mantiene un archivo de todos los certificados emitidos por un periodo de cinco (5) años.

- **Período de uso para el par de claves**

El certificado de la ECA raíz de Certificaciones Digitales Digicert S.R.L. tiene una validez de diez (10) años a partir de la emisión del mismo por parte de la ATT. Para proseguir con sus operaciones Certificaciones Digitales Digicert S.R.L. emitirá un nuevo par de claves y solicitará el certificado correspondiente a la ATT.

Los certificados de signatarios, persona física y persona jurídica, tienen la validez definida por la Política de Certificación correspondiente a cada uno.

13.4. DATOS DE ACTIVACIÓN

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

Certificaciones Digitales Digicert S.R.L. ha desarrollado los procedimientos para la generación de claves de activación de la clave privada del módulo criptográfico, basado en un esquema multi-personal.

- **Protección de los datos de activación**

Solo el personal designado por Certificaciones Digitales Digicert S.R.L. posee las claves necesarias para la activación de la clave privada bajo el sistema multi-personal y son responsables de su custodia.

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

Las claves de activación son confidenciales, personales e intransferibles.

13.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Certificaciones Digitales Digicert S.R.L. ha definido un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ISO/IEC 27.001 y una serie de controles de seguridad, incluyendo:

- Definición de roles y responsabilidades;
- Controles de acceso físico y lógico;
- Seguridad física de ambientes y sistemas;
- Gestión de copias de seguridad (respaldos);
- Registros de auditoría;
- Respuesta ante incidentes.

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

El procedimiento de control se detalla en los documentos PRO-ECA-03 de control de accesos físicos y lógicos, PRO-ECA-02 de respuesta a incidentes y PL-ECA-01 de gestión de desastres.

13.6. 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**

Todos los sistemas utilizados por Certificaciones Digitales Digicert S.R.L. pasan por revisiones y pruebas de seguridad según los procedimientos establecidos en el SGSI.

Certificaciones Digitales Digicert S.R.L. utiliza software a medida desarrollado y mantenido por terceros para sus propósitos de funcionalidad como ECA. Toda modificación al código, o actualización, y cambio de configuración de los sistemas utilizados pasa por un riguroso proceso de prueba 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 durante todo el ciclo de vida de los sistemas, incluyendo:

- Registro y reporte de acceso físico.
- Registro y reporte de acceso lógico.

Procedimientos de actualización e implementación de sistemas.El procedimiento se detalla en los documentos PRO-ECA-01 de gestión de cambios y pasaje entre ambientes y PRO-ECA-10 de control de Cambios.

13.7. CONTROLES DE SEGURIDAD DE LA RED

El hardware y software para la emisión de certificados por parte de Certificaciones Digitales Digicert S.R.L. están sujetos a estrictos controles de seguridad y únicamente son accesibles desde la red interna.

La red se encuentra segmentada y protegida por firewalls en alta disponibilidad, los sistemas protegidos contra virus y software malicioso, y el acceso de los usuarios a sus cuentas en el sistema está controlado.

La herramienta de SIEM incorporada realiza la centralización de los registros del NIDS, firewall y HIDS y tiene definidas reglas específicas de correlación que generan alarmas ante actividades sospechosas. De esta manera se dispone de un esquema de control y monitoreo en tiempo real de la seguridad de la red.

13.8. CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

Certificaciones Digitales Digicert S.R.L. únicamente utiliza módulos criptográficos con certificación FIPS 140-2 nivel 3.

- **Registro de tiempo**

Los sistemas y servidores de Certificaciones Digitales Digicert S.R.L. se encuentran sincronizados en fecha y hora y guardan registros de todas las actividades.

14. PERFIL DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

14.1. 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 3.
    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, YYMMDDHHMMSSZ (formato UTC Time);

- Fecha de caducidad del Certificado, 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).

14.2. PERFIL DEL CERTIFICADO DE LA ENTIDAD CERTIFICADORA AUTORIZADA (ECA)

1. El formato para el Certificado Digital de Certificaciones Digitales Digicert S.R.L. tendrá los siguientes atributos y contenidos:
   a) Versión (version):
      - El valor del campo es 3.
   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, YYMMDDHHMMSSZ (formato UTC Time);

- Fecha de caducidad del Certificado, formato UTC Time.

f) Nombre suscriptor (subject):
- CN = “Entidad Certificadora Autorizada Digicert”;
- O = “Digicert”;
- 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).

14.3. PERFIL DE LA CRL DE LA ENTIDAD CERTIFICADORA RAÍZ

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

a) Versión (versión):
   - El valor del campo es 2;
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 Autorizada Digicert”;

- O = “Digicert”;
- 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, formato UTC Time.

f) Certificados Revocados (Revoked Certificates):
- Lista de certificados revocados (CRL) 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 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

14.4. PERFIL DEL OCSP

La adhesión en cuanto a definiciones, implementación y formatos, al RFC 5280 “*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*” y RFC 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 todas estas condiciones son verificadas, se devuelve una respuesta. De lo contrario, 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 ser, de acuerdo al RFC 5280:
- Válido (good), existe un certificado digital válido con el número de serie contenido en la consulta;
- Revocado (revoked), el certificado digital con el número de serie indicado está revocado;
- Desconocido (unkown), no se reconoce el número de serie de certificado contenido en la consulta;
c) Período de validez de la respuesta;
d) Extensiones opcionales.

Las respuestas OCSP deben estar firmadas digitalmente por la ECA correspondiente o por una entidad habilitada a tal efecto en el marco de la PKI 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: A completar por Certificaciones Digitales Digicert S.R.L

15. DISPONIBILIDAD DEL SERVICIO

Certificaciones Digitales Digicert S.R.L. implementa un ambiente de contingencia, tanto en su servicio de certificación digital como en el servicio de custodia de certificados digitales para la firma digital remota que le permite contar con alto nivel de disponibilidad operativo del servicio.

Para casos particulares, condiciones adicionales y específicas respecto a la disponibilidad del servicio, deberán ser tratadas contractualmente con los clientes finales.

16. AUDITORÍA DE CONFORMIDAD

16.1. 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.

16.2. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Al margen de la función de auditoría, el auditor y la parte auditada (Certificaciones Digitales Digicert S.R.L) no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

En cumplimiento de lo establecido en la Constitución Política del Estado sobre protección de datos personales y considerando que, para el cumplimiento, por parte del auditor, de los servicios regulados en el contrato será preciso acceder a los datos de carácter personal custodiados por Certificaciones Digitales Digicert S.R.L., el auditor tendrá la consideración de encargado del tratamiento de los datos, lo que le permitirá acceso a los mismos durante el desarrollo de la auditoría.

16.3. COMUNICACIÓN DE LOS RESULTADOS

El auditor comunicará los resultados de la auditoría a la Gerencia y Dirección de Tecnología de Certificaciones Digitales Digicert S.R.L., al igual que al Oficial de Seguridad y a los responsables de las distintas áreas en las que se detecten no conformidades.

17. SUSCRIPTION AL SERVICIO

17.1. SUSCRIPCION PRE PAGO

La suscripción pre pago al servicio es posible, para ello, el suscriptor debe definir el volumen de transacciones/certificados que requerirá y cancelar por adelantado el monto correspondiente a las mismas de acuerdo al tarifario establecido por Certificaciones Digitales Digicert S.R.L.

17.2. SUSCRIPCION POST PAGO

La suscripción post pago al servicio es posible, en este modelo, el suscriptor utiliza el servicio, consumiendo un cierto volumen de transacciones/certificados y al finalizar un cierto periodo de tiempo (mes, por ejemplo) deberá cancelar el monto correspondiente por el consumo realizado de acuerdo al tarifario establecido por Certificaciones Digitales Digicert S.R.L.

18. REQUISITOS COMERCIALES Y LEGALES

18.1. TARIFAS

Serán publicadas en la página web de Certificaciones Digitales Digicert S.R.L.

18.2. POLÍTICA DE CONFIDENCIALIDAD

Toda la recopilación y uso de la información compilada por Certificaciones Digitales Digicert S.R.L. 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.

18.3. 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 Certificaciones Digitales Digicert S.R.L. de la información contenida en su clave pública y el certificado firmado por Certificaciones Digitales Digicert S.R.L.

18.4. 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.

- **Responsabilidades de las autorizadas ante aceptantes**

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.

18.5. 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 Certificaciones Digitales Digicert S.R.L.

En todo caso los ajustes a la documentación requerida por la ATT para la operación de Certificaciones Digitales Digicert S.R.L., 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.

18.6. RESOLUCIÓN DE CONFLICTOS

Toda controversia o diferencia, cualquiera sea su naturaleza, relativas a contratos y a su ejecución, liquidación e interpretación se resolverán por CONCILIACION y/o ARBITRAJE de acuerdo con los Reglamentos del Centro de Conciliación y Arbitraje Comercial de la CAINCO de Santa Cruz de la Sierra-Bolivia, y los siguientes acuerdos.

El número de árbitros será 3 (tres), uno a ser designado por cada parte y el tercero a ser designado por los otros dos. Todos los árbitros deberán ser designados entre los árbitros que se encuentren debidamente inscritos y registrados en las listas de árbitros del Centro de Conciliación y Arbitraje Comercial de la CAINCO. Si cualesquiera de las partes no designa su respectivo árbitro en el plazo de 15 (quince) días calendario, computables a partir de la notificación a cualesquiera de ellas con la intención de la otra de someter la controversia a arbitraje; o en el caso de que los árbitros de parte no designen al tercer árbitro dentro de los 15 (quince) días calendario computables a partir de la designación del último árbitro de parte, el o los árbitros no designados deberá(n) ser designado(s) por el Centro de Conciliación y Arbitraje Comercial de la CAINCO.

La decisión de los árbitros deberá ser debidamente fundamentada, será final, vinculante y exigible contra las partes y la ejecución de cualquier laudo podrá ser sometido a cualquier corte que tenga jurisdicción. Si el incumplimiento de cualquiera de las partes de este contrato de las decisiones de los árbitros requiere que la otra parte recurra a cualquier corte competente para obtener la ejecución del laudo, la parte incumplida deberá compensar a la otra parte por todos los costos de dicho litigio, incluyendo los honorarios de los abogados.

18.7. 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.

18.8. 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.