POLÍTICA DE CERTIFICACIÓN

Certificaciones Digitales Digicert S.R.L.

Tabla de Contenido

0. GESTIÓN DEL DOCUMENTO 7
1. CONTROL DE CAMBIOS 7
1.1. CAMBIOS A LA POLÍTICA DE CERTIFICACIÓN DE PERSONA NATURAL 7
1.2. DETALLE DE CAMBIOS 7
2. DEFINICIONES Y ABREVIATURAS 8
2.1. ABREVIATURAS 8
2.2. DEFINICIONES 8
3. INTRODUCCIÓN 9
3.1. DESCRIPCIÓN GENERAL Y OBJETIVO 9
3.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO 9
3.3. PARTICIPANTES DE LA PKI BOLIVIA 9
3.3.1. PRIMER NIVEL: ENTIDAD CERTIFICADORA RAÍZ 10
3.3.2. SEGUNDO NIVEL: ENTIDAD DE CERTIFICACIÓN 10
3.3.3. TERCER NIVEL: AGENCIA DE REGISTRO 10
3.3.4. CUARTO NIVEL: SIGNATARIOS 10
3.3.5. OTROS: TERCEROS ACEPTANTES 10
3.4. USO DE LOS CERTIFICADOS 10
3.4.1. USOS TÍPICOS 11
3.4.2. USOS PROHIBIDOS 11
3.4.3. FIABILIDAD DE LA FIRMA DIGITAL A LO LARGO DEL TIEMPO 11
3.5. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN 12
3.5.1. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN 12
3.5.2. PROCEDIMIENTO DE APROBACIÓN 12
4. CONCEPTOS GENERALES 12
4.1. CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA 12
4.2. CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA 12
4.2.1. CONTINUIDAD DEL SERVICIO 12
4.3. ALCANCE DEL SERVICIO DE CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA 13
4.4. COMUNIDAD DE USUARIOS Y AMBITO DE LA APLICACIÓN 13
4.4.1. SUSCRIPTORES 13

4.4.2. TERCEROS ACEPTANTES 13
4.4.3. AMBITO DE LA APLICACIÓN 13
5. POLITICA DEL SERVICIO 13
5.1. VISTA GENERAL 13
5.2. IDENTIFICACION DE LA POLITICA 13
5.3. APLICACIONES DEL SERVICIO 14
5.4. COMUNIDAD DE USUARIOS, APLICABILIDAD, LIMITACIONES Y PROHIBICIONES 14
5.4.1. COMUNIDAD DE USUARIOS 14
5.4.2. USOS PERMITIDOS 14
5.4.3. LIMITES DE USO 14
5.4.4. PROHIBICIONES DE USO 14
6. OBLIGACIONES Y RESPONSABILIDADES 15
6.1. OBLIGACIONES 15
6.1.1. OBLIGACIONES CON LOS SUSCRIPTORES 15
6.1.2. OBLIGACIONES CON LA ATT 15
6.1.3. OBLIGACIONES DE LOS SUSCRIPTORES 16
6.2. RESPONSABILIDADES 17
6.2.1. RESPONSABILIDADES DE LOS PROVEEDORES DE SERVICIO 17
6.2.2. RESPONSABILIDAD FINANCIERA 17
6.2.3. EXONERACION DE RESPONSABILIDAD 17
7. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS 17
8. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS 18
8.1. REGISTRO DE NOMBRES 18
8.2. VALIDACIÓN DE LA IDENTIDAD INICIAL 18
8.2.1. MÉTODOS DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA 19
8.2.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN 19
8.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE CLAVE 20
8.3.1. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN RUTINARIAS 20
8.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN CON CAMBIO DE CLAVE PRIVADA 20
8.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE CLAVE 20
9. REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS 20

10. REQUERIMIENTOS DE LOS PROVEEDORES DE SERVICIO 25
10.1. DECLARACION DE PRACTICAS DEL SERVICIO 25
10.1.1. GESTION DE LOS MODULOS CRIPTOGRAFICOS HSM 25
10.1.2. DEL PAR DE CLAVES 26
10.1.3. CSR Y CERTIFICADOS DIGITALES 26
10.1.4. USO DE LOS CERTIFICADOS DIGITALES ALMACENADOS 26
10.2. GESTION DEL CICLO DE VIDA DEL MODULO CRIPTOGRAFICO USADO PARA EL SERVICIO 26
10.3. CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA 27
10.4. OPERACIÓN Y GESTION DE LOS PROVEEDORES DE SERVICIO 27
10.5. ESQUEMA ORGANIZATIVO 27
10.6. REQUISITOS COMERCIALES LEGALES 27
10.6.1. TARIFAS 28
10.6.2. CAPACIDAD FINANCIERA 28
10.6.3. NOTIFICACIONES 28
10.6.4. RESOLUCION DE CONFLICTOS 28
11. CONTROLES OPERACIONALES O DE GESTIÓN 28
11.1. CONTROLES DE SEGURIDAD FÍSICA 28
11.1.1. UBICACIÓN Y CONSTRUCCIÓN 28
11.1.2. ACCESO FÍSICO 29
11.1.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO 29
11.1.4. EXPOSICIÓN AL AGUA 29
11.1.5. PROTECCIÓN Y PREVENCIÓN DE INCENDIOS 29
11.1.6. SISTEMA DE ALMACENAMIENTO 29
11.1.7. ELIMINACIÓN DE RESIDUOS 29
11.1.8. COPIA DE SEGURIDAD 30
11.2. CONTROLES DE PROCEDIMIENTOS 30
11.2.1. ROLES DE CONFIANZA 30
11.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA 30
11.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 30
11.3. CONTROLES DE SEGURIDAD DE PERSONAL 30
11.3.1. REQUERIMIENTOS DE CALIFICACIÓN, EXPERIENCIA Y ACREDITACIÓN 30
11.3.2. REQUERIMIENTOS DE FORMACIÓN 31

11.3.3. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS 31
11.3.4. SANCIONES POR ACCIONES NO AUTORIZADAS 31
11.3.5. REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL Y CONTROLES PERIÓDICOS DE CUMPLIMIENTO 31
11.3.6. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL 32
11.3.7. FINALIZACIÓN DE LOS CONTRATOS 32
11.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 32
11.4.1. TIPOS DE EVENTOS REGISTRADOS 32
11.4.2. FRECUENCIA DE PROCESADO DE REGISTROS 32
11.4.3. PERÍODO DE RETENCIÓN PARA LOS REGISTROS DE AUDITORÍA 33
11.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA, SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA, NOTIFICACIÓN AL SUJETO, CAUSA DEL EVENTO, ANÁLISIS DE VULNERABILIDADES 33
11.4.5. PROCEDIMIENTOS DE COPIA DE SEGURIDAD DE LOS REGISTROS DE AUDITORÍA 33
11.4.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA 33
11.4.7. NOTIFICACIÓN AL SUJETO CAUSANTE DEL EVENTO 33
11.4.8. ANÁLISIS DE VULNERABILIDADES 33
11.5. ARCHIVOS DE INFORMACIÓN Y REGISTROS 33
11.5.1. TIPOS DE INFORMACIÓN Y EVENTOS REGISTRADOS 33
11.5.2. PERÍODO DE RETENCIÓN PARA EL ARCHIVO 34
11.5.3. SISTEMA DE RECOGIDA DE INFORMACIÓN PARA AUDITORÍA, PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA 34
11.6. CAMBIO DE CLAVE 34
11.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE 34
11.8. CESE DE LA ECA 34
12. CONTROLES DE SEGURIDAD TÉCNICA 35
12.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 35
12.1.1. GENERACIÓN DEL PAR DE CLAVES 35
12.1.2. TAMAÑO DE LAS CLAVES 35
12.1.3. HARDWARE Y SOFTWARE DE GENERACIÓN DE CLAVES 35
12.2. PROTECCIÓN DE LA CLAVE PRIVADA 35
12.2.1. ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS 35
12.2.2. CONTROL MULTI-PERSONA DE LA CLAVE PRIVADA 36
12.2.3. CUSTODIA DE LA CLAVE PRIVADA 36

12.2.4. COPIA DE SEGURIDAD DE LA CLAVE PRIVADA 36
12.2.5. ARCHIVO DE LA CLAVE PRIVADA 36
12.2.6. INTRODUCCIÓN DE LA CLAVE PRIVADA AL MÓDULO CRIPTOGRÁFICO 36
12.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA 36
12.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA 36
12.2.9. MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA 36
12.2.10. CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS 36
12.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 36
12.3.1. ARCHIVO DE LA CLAVE PÚBLICA 37
12.3.2. PERÍODO DE USO DE LAS CLAVES 37
12.4. DATOS DE ACTIVACIÓN 37
12.4.1. GENERACIÓN DE LOS DATOS DE ACTIVACIÓN 37
12.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 37
12.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 37
12.5. CONTROLES DE SEGURIDAD INFORMÁTICA 37
12.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 38
12.6.1. CONTROLES DE DESARROLLO DE SISTEMAS 38
12.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD 38
12.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA DE LOS SISTEMAS 38
12.7. CONTROLES DE SEGURIDAD DE LA RED 38
12.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS 38
12.8.1. REGISTRO DE TIEMPO 38
13. PERFILES DE CERTIFICADO, CRL Y OSCP 39
13.1. PERFIL DE CERTIFICADO DE SIGNATARIO 39
13.1.1. CERTIFICADO DE PERSONA JURIDICA CUSTODIADO EN NUBE PARA FIRMA DIGITAL AUTOMATICA 39
13.1.2. CERTIFICADO DE PERSONA JURIDICA CUSTODIADO EN NUBE PARA FIRMA DIGITAL SIMPLE 40
13.1.3. CERTIFICADO DE PERSONA JURIDICA PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA 41
13.1.4. CERTIFICADO DE PERSONA JURIDICA PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL SIMPLE 42
13.1.5. CERTIFICADO DE PERSONA JURIDICA PKCS12 (SOFTWARE) PARA FIRMA DIGITAL AUTOMATICA 43
13.1.6. CERTIFICADO DE PERSONA JURIDICA PKCS12 (SOFTWARE) PARA FIRMA DIGITAL SIMPLE ... 44

13.1.7. CERTIFICADO DE PERSONA NATURAL EN NUBE PARA FIRMA DIGITAL AUTOMATICA 45
13.1.8. CERTIFICADO DE PERSONA NATURAL EN NUBE PARA FIRMA DIGITAL SIMPLE 46
13.1.9. CERTIFICADO DE PERSONA NATURAL PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA 47
13.1.10. CERTIFICADO DE PERSONA NATURAL PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA 48
13.1.11. CERTIFICADO PARA LAS TSUS 49
13.2. PERFIL DE CRL 50
13.3. PERFIL DE OCSP 51
14. AUDITORIA DE CONFORMIDAD 52
14.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD 52
14.2. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA 52
14.3. COMUNICACIÓN DE LOS RESULTADOS 52
15. ADMINISTRACION DOCUMENTAL 52
15.1. PROCEDIMIENTO PARA CAMBIO DE ESPECIFICACIONES 53
15.2. PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN 53
ANEXO 1: PLAN DE CESE DE ACTIVIDADES 54
ANEXO 2: POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES 58

0. GESTIÓN DEL DOCUMENTO

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	2023-11-23	**Fecha**	2023-11-23	**Fecha**	2023-11-23

Firmado digitalmente por Miguel Angel Gutierrez Blanco 24/11/2023 16:01 AST

Firmado digitalmente por Robin Caballero 24/11/2023 17:03 AST

Firmado digitalmente por Jose Luis Morón 24/11/2023 16:59 AST

1. CONTROL DE CAMBIOS

1.1. CAMBIOS A LA POLÍTICA DE CERTIFICACIÓN DE PERSONA NATURAL

La Política de Certificación de Persona Natural es revisada con una periodicidad anual por el Comité de Control 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	Cambios Realizados	Detalle de modificaciones
0	2016-11-30		Versión inicial del documento
1	2018-02-28		Revisión – Observaciones ATT
2	2019-08-14		Revisión – según norma ATT-DJ-RAR-TL LP 209/2019
3	2019-12-24		Tercera Auditoría-Un solo documento Persona Física y Jurídica
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	2020-09-25	Se añadió el perfil del certificado para una TSU (13.1.11.)	Modificación para la habilitación del servicio de TSA
6	2023-11-07		Actualizar Representante Legal

7	2023-11-23	Actualización de contenido	

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 firmado 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 o 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 del 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 alguno 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. DESCRIPCIÓN GENERAL Y OBJETIVO

El presente documento constituye la Política de Certificación (*Certificate Policy*) para todos los perfiles de certificados emitidos por Certificaciones Digitales Digicert S.R.L., emitida 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.

El alcance y objetivo del presente documento está limitado a la descripción de las políticas, prácticas y procedimientos empleados por Certificaciones Digitales Digicert S.R.L., para brindar Servicios de Certificación Digital a Personas Naturales y Jurídicas en las diferentes modalidades existentes: PKCS11, PKCS12 y haciendo uso de un servicio de custodia de certificado digital en la nube. De esta manera se pretende dar transparencia al conjunto de tareas relacionadas con la provisión de estos servicios.

Esta CP 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 CP 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.

3.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

El presente documento lleva como título "**Política de Certificación**".

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

3.3. 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.

3.3.1. 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 firma su certificado y emite certificados digitales a las entidades certificadoras públicas y privadas subordinadas.

3.3.2. SEGUNDO NIVEL: ENTIDAD DE CERTIFICACIÓN

La CPS de Certificaciones Digitales Digicert S.R.L. especifica su actuación 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 firma digital es 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.

3.3.3. 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.

3.3.4. 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.

3.3.5. 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.

3.4. USO DE LOS CERTIFICADOS

3.4.1. 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 esta CP.

3.4.2. 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.

3.4.3. 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.

3.5. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

3.5.1. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

La administración de la presente Política 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

3.5.2. PROCEDIMIENTO DE APROBACIÓN

El sistema documental y de organización de la CP 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 Política de Certificación y de las especificaciones de servicios que están relacionados.

La aprobación de esta Política 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 presente 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. OBLIGACIONES Y RESPONSABILIDADES

6.1. OBLIGACIONES

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.2. RESPONSABILIDADES

6.2.1. RESPONSABILIDADES DE LOS PROVEEDORES DE SERVICIO

De acuerdo a lo establecido en el Art. 44 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, la ECA tiene las siguientes responsabilidades:

a) Será responsable por el Servicio de Custodia de Certificados Digitales para la Firma Digital Remota y/o en la Nube, con errores y omisiones que causen perjuicio a sus signatarios y/o usuarios.
b) La entidad certificadora se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.
c) Será responsable 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.

Se exceptúa de responsabilidad a DIGICERT S.R.L en el evento de caso fortuito o fuerza mayor en los términos establecidos en el Código Civil.

6.2.2. RESPONSABILIDAD FINANCIERA

Certificaciones Digitales Digicert S.R.L. cuenta con la solvencia financiera necesaria para garantizar la continuidad del servicio.

6.2.3. EXONERACION DE RESPONSABILIDAD

Certificaciones Digitales Digicert S.R.L. se exonera de responsabilidades en caso de haber actuado con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones. Así también, se exceptúa de responsabilidad a DIGICERT S.R.L en el evento de caso fortuito o fuerza mayor en los términos establecidos en el Código Civil.

7. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

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 anuncia 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 dedica sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 2 horas.

Por información adicional consultar el mismo apartado en la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

8. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

8.1. REGISTRO DE NOMBRES

La norma vigente define que el nombre para las personas naturales 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

La norma vigente define que el nombre para las personas jurídicas se compone de:

- **CN =** Nombres y apellidos del representante legal autorizado para representar a la persona jurídica simple o automática en determinadas atribuciones;
- **O =** Razón social de la empresa o institución a la que representa la persona jurídica simple o automática;
- **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

Por información adicional consultar el mismo apartado en la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

8.2. VALIDACIÓN DE LA IDENTIDAD INICIAL

8.2.1. 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. El par de claves para el certificado es generado por la Agencia de Registro en el token del solicitante una vez validada su identidad.

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 procede a la suspensión y/o revocación de la firma digital luego de las validaciones correspondientes.

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

8.2.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN

Persona Natural

8.2.2.1. Autenticación de la identidad de un individuo

El derecho de solicitud de certificados definido en la presente Política de Certificación para personas naturales, no se considera necesaria la identificación de ninguna organización.

La autenticación de la identidad del solicitante de un certificado para persona natural se realiza mediante su presentación personal ante un Agente de Registro, acreditándose mediante:

- Fotocopia simple de carnet de identidad o carnet extranjero del solicitante.
- Fotocopia de la última factura de pago de luz, agua o teléfono que permita verificar la dirección actual del solicitante.

Persona Jurídica

8.2.2.2. Autenticación de la identidad de una organización

La autenticación de la identidad de una organización o entidad se realiza mediante el apersonamiento del solicitante del certificado de entidad (administrador, representante legal o voluntario con poder suficiente) ante una Agencia de Registro habilitada para la emisión de este tipo de certificados, acreditando su identidad personal y aportando la siguiente documentación:

- Formulario de solicitud
- Fotocopia del simple del 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.
- Fotocopia simple del carnet de identidad o carnet de extranjero del representante legal de la empresa u organización solicitante.

- Fotocopia simple del poder de nombramiento del representante legal de la empresa.
- Fotocopia simple del poder de nombramiento del representante legal de la empresa.

Certificaciones Digitales Digicert S.R.L. únicamente garantiza que la dirección de correo que consta en el certificado fue la aportada por el suscriptor en el momento de la formalización de su solicitud.

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

8.3.1. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN RUTINARIAS

Se realiza a través de la cuenta del usuario utilizada durante la solicitud del certificado. 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.

8.3.2. 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 es la misma que para el registro inicial, o bien se emplea algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

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

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

Presencial. Es el mismo que para el registro inicial descrito en el punto 3.2, bajo el título "Autenticación de la identidad de un individuo", de esta Política de Certificación
Telemática. Mediante la firma electrónica del formulario de revocación ubicado en el área personal de servicios de certificación.
Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico.

Certificaciones Digitales Digicert S.R.L. o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

9. REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

Solicitud de certificados

El ciudadano que desee que le sea emitido un certificado de acuerdo con esta política de certificación debe presentarse para solicitarlo en una Agencia de Registro Autorizada de Certificaciones Digitales Digicert S.R.L. con su Cédula de Identidad (CI) o pasaporte vigente.

El listado de agencias de registro autorizadas se encuentra en la URL www.digicert.bo.

Es atribución de la Agencia de Registro de Certificaciones Digitales Digicert S.R.L., el determinar la adecuación de un tipo de certificado a las características del solicitante, en función de las disposiciones de la Política de Certificación aplicable, y de este modo acceder o denegar la gestión de la solicitud de certificación del mismo.

En el caso de denegación de la solicitud de certificación por parte de la Agencia de Registro, el solicitante recibe información de los motivos del rechazo de la misma.

Tramitación de la solicitud de certificados

Compete a la Agencia de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el documento de comparecencia. Una vez completa la solicitud, la Agencia de Registro la remite a Certificaciones Digitales Digicert S.R.L.

Emisión de certificados

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 evidencia sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

La emisión del certificado tiene 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 esta Política de Certificación.

Cuando Certificaciones Digitales Digicert S.R.L. emita un certificado de acuerdo con una solicitud de certificación válida, envía una copia del mismo al individuo que remitió la solicitud y otra al repositorio de Digicert S.R.L.

Es tarea de Digicert S.R.L. notificar al subscriptor de un certificado la emisión del mismo y proporcionarle una copia, o en su defecto, informarle del modo en que puede conseguirla.

Aceptación de certificados

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.

El Contrato de Certificación es un documento que debe ser firmado manualmente por el solicitante y por la persona adscrita al registro de usuarios, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El

formulario del Contrato de Certificación se le entregara al solicitante y puede ser descargado de la web de Certificaciones Digitales Digicert S.R.L.

Uso del par de claves y del certificado

El Solicitante puede utilizar el certificado y su par de claves únicamente para los fines descriptos en la sección 3.4 de esta Política de Certificación.

En ninguna circunstancia el Solicitante puede extraer su clave privada del dispositivo que la contiene ni compartir el PIN que la protege. En caso de que el Solicitante haya extraviado o sospeche del compromiso del dispositivo o del PIN, debe solicitar la revocación inmediata del certificado

Renovación de certificados

El procedimiento, en todos sus aspectos, es idéntico al de emisión de un nuevo certificado.

Renovación de claves

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

Modificación de certificados

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

Revocación y suspensión de certificados

1. Circunstancias para la revocación

Un certificado se revoca cuando:

1.1 El subscriptor del certificado o sus claves o las claves de sus certificados se han comprometido por:

a. El robo, pérdida, revelación, modificación u otro compromiso o sospecha de compromiso de la clave privada del usuario.
b. 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.

1.2 Se produce la emisión defectuosa de un certificado debido a:

c. Que no se ha satisfecho un prerrequisito material para la emisión del certificado.
d. Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
e. Un error de entrada de datos u otro error de proceso.

1.3 El par de claves generado por un usuario final se revela como “débil”

1.4 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

1.5 Una solicitud de revocación válida se recibe de un usuario final

1.6 Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo, una orden judicial

1.7 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

Certificaciones Digitales Digicert S.R.L., acepta solicitudes de revocación por los siguientes procedimientos:

Presencial. Mediante la presentación e identificación del suscriptor en una Agencia de Registro y la cumplimentación y firma, por parte del mismo, del "Formulario de Solicitud de Revocación" que se le proporciona y se encuentra publicado en la web de Certificaciones Digitales Digicert S.R.L.
Telefónico. Mediante llamada telefónica al número de soporte telefónico de Certificaciones Digitales Digicert S.R.L. al (591)(3) 3340104.

El mecanismo de verificación que se emplea es el envío a la dirección de correo electrónico vinculada al certificado a revocar de un mensaje advirtiendo del proceso de revocación en curso. Si el legítimo suscriptor del certificado deseara anular dicho proceso debe enviar una respuesta al mensaje de correo expresando este deseo.

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

4. Periodo de gracia de la solicitud de revocación

La revocación se realiza 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 jurídica, 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. puede ser solicitada por la propia Digicert o por una autoridad jurídica.

3. Procedimiento para la solicitud de suspensión

La suspensión de un certificado debe 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 es normalmente de 15 días, salvo que la resolución judicial o administrativa que lo dictamine imponga un plazo superior o inferior, para lo cual, se aplica el mismo.

Frecuencia de emisión de CRLs

Certificaciones Digitales Digicert S.R.L. actualiza la Lista de Certificados Revocados (CRL) cuando ocurra al menos uno de los siguientes acontecimientos:

a) Se produzca la revocación de un certificado, con un margen de tiempo de 2 horas luego de la revocación; o
b) Transcurran como máximo 48 horas luego de la última emisión de CRL.

Requisitos de comprobación de CRLs

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 deben 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.

Disponibilidad de comprobación de estado on-line

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

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.

Otras formas de divulgación de información de revocación disponibles

Además de la consulta de revocados por medio de Listas de Revocación de Certificados (CRL) y por medio del servicio OCSP, es posible comprobar la validez de los certificados por medio de un formulario web. Este formulario se encuentra en el sitio web de la Autoridad de Certificación en la URL ww.digicert.bo

Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado.

Requisitos especiales de renovación de claves comprometidas

El procedimiento que aplica al cambio de claves asociadas a un certificado es el de Emisión de certificado. Por lo tanto, cuando un suscriptor sospeche el compromiso de sus claves debe re-emitir el certificado asociado a las mismas.

Servicios de comprobación de estado de certificados

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

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.

Finalización de la suscripción

Certificaciones Digitales Digicert S.R.L. informa al firmante, mediante correo electrónico firmado digitalmente, en un momento previo a la publicación del certificado en la CRL, acerca de la suspensión o revocación de su certificado, especificando los motivos, la fecha y la hora en que su certificado queda sin efecto, y comunicándole que no debe continuar utilizándolo.

Depósito y recuperación de claves

Certificaciones Digitales Digicert S.R.L., no realiza depósito de las claves asociadas a los certificados de los suscriptores.

10. REQUERIMIENTOS DE LOS PROVEEDORES DE SERVICIO

10.1. DECLARACION DE PRACTICAS DEL SERVICIO

10.1.1. 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.

10.1.2. DEL PAR DE CLAVES

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).

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.

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.

10.1.3. CSR Y CERTIFICADOS DIGITALES

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.

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.

10.1.4. 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.

10.2. GESTION DEL CICLO DE VIDA DEL MODULO CRIPTOGRAFICO USADO PARA EL SERVICIO

Los HSMs utilizados para el servicio de custodia son inicializados de manera conjunta, durante el ciclo de vida de los mismos mantienen su información sincronizada, y al finalizar la vida útil de los mismos dentro de la solución los mismos pueden ser inicializados nuevamente (para que no contengan información alguna de su periodo de vida) si es que aún se encuentran funcionales.

Los HSMs serán sustituidos cuando se encuentren falla irreparable en los mismos, sin descartar una posible sustitución por mejora en la infraestructura.

10.3. CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

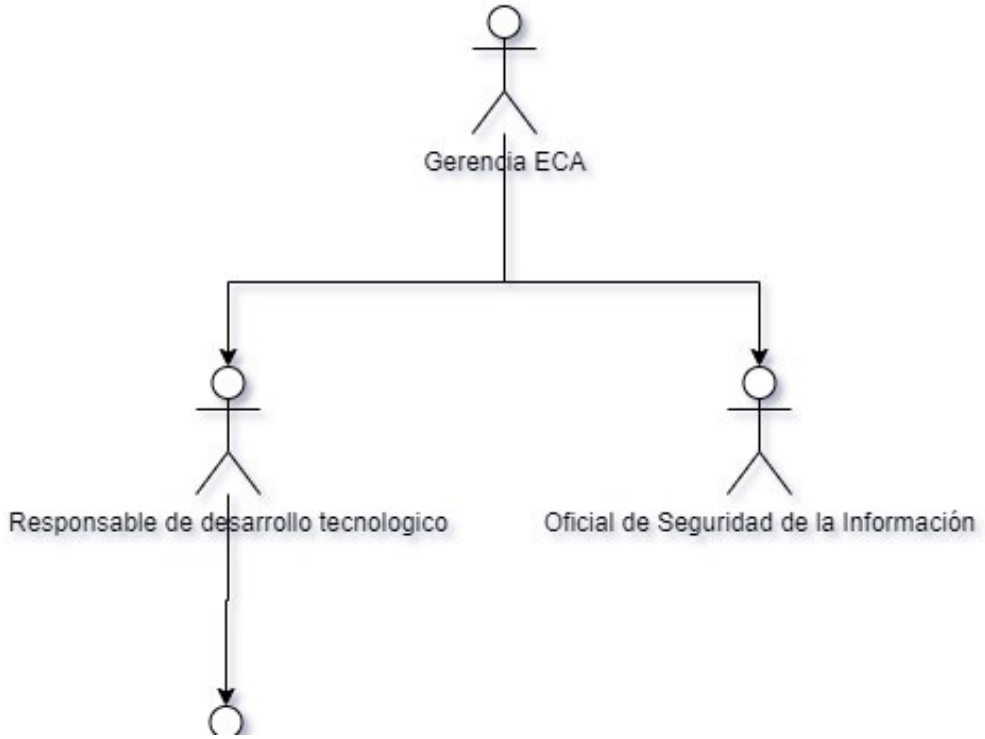
Para el servicio de custodia de certificados digitales para la firma digital remota se utilizan HSMs nCipher (en cumplimiento de FIPS 140-2 nivel 3) en ambos ambientes, producción y contingencia, los cuales son inicializados dentro de un mismo "Security World" (framework de seguridad desarrollado por 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.

10.4. OPERACIÓN Y GESTION DE LOS PROVEEDORES DE SERVICIO

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.

10.5. ESQUEMA ORGANIZATIVO



10.6. REQUISITOS COMERCIALES LEGALES

10.6.1. TARIFAS

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

10.6.2. CAPACIDAD FINANCIERA

Certificaciones Digitales Digicert S.R.L. cuenta con la solvencia financiera necesaria para garantizar la continuidad de los servicios prestados en el marco de lo expresado en su plan de negocio.

10.6.3. NOTIFICACIONES

Ante cualquier eventualidad, Certificaciones Digitales Digicert S.R.L. notificará a sus usuarios a través de los medios de comunicación correspondientes.

10.6.4. RESOLUCION 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.

11. CONTROLES OPERACIONALES O DE GESTIÓN

11.1. CONTROLES DE SEGURIDAD FÍSICA

11.1.1. 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.

11.1.2. 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.

11.1.3. 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.

11.1.4. 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.

11.1.5. 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.

11.1.6. 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.

11.1.7. 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.

11.1.8. 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.

11.2. 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.

11.2.1. ROLES DE CONFIANZA

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

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

11.2.2. 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.

11.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todos los usuarios autorizados de Certificaciones Digitales Digicert S.R.L. se identifican mediante certificados digitales auto firmados y 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.

11.3. CONTROLES DE SEGURIDAD DE 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. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

11.4.1. 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. 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.

11.4.2. 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.

11.4.3. PERÍODO DE RETENCIÓN PARA LOS REGISTROS DE AUDITORÍA

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

11.4.4. 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 emite 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.

11.4.5. 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.

11.4.6. 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.

11.4.7. NOTIFICACIÓN AL SUJETO CAUSANTE DEL EVENTO

No estipulado.

11.4.8. ANÁLISIS DE VULNERABILIDADES

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

11.5. ARCHIVOS DE INFORMACIÓN Y REGISTROS

11.5.1. 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

11.5.2. 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.

11.5.3. 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.

11.6. CAMBIO DE CLAVE

No estipulado.

11.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE

Certificaciones Digitales Digicert S.R.L. cuenta con un plan de continuidad de negocio y recuperación 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.

11.8. CESE DE LA ECA

Certificaciones Digitales Digicert S.R.L. tiene establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones. 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.

12. CONTROLES DE SEGURIDAD TÉCNICA

En este punto se hace referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 7.1 de la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

12.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

12.1.1. GENERACIÓN DEL PAR DE CLAVES

Los pares de claves para los certificados emitidos bajo esta Política de Certificación se generan en el dispositivo criptográfico (TOKEN) del usuario y nunca abandonarán el mismo.

12.1.2. TAMAÑO DE LAS CLAVES

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación nunca es inferior a 2.048 bits.

12.1.3. HARDWARE Y SOFTWARE DE GENERACIÓN DE CLAVES

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

12.2. PROTECCIÓN DE LA CLAVE PRIVADA

En este punto se hace referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

12.2.1. ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los dispositivos criptográficos, TOKEN, empleados en la emisión de los certificados adscritos a esta Política de Certificación soportan el estándar PKCS#11.

12.2.2. CONTROL MULTI-PERSONA DE LA CLAVE PRIVADA

Las claves privadas para los certificados de firma emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos.

12.2.3. CUSTODIA DE LA CLAVE PRIVADA

No se custodian claves privadas de firma digital de los suscriptores de los certificados definidos por la presente política.

12.2.4. COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

No existe una copia de seguridad de la clave privada asociada al certificado y clave pública del solicitante.

12.2.5. ARCHIVO DE LA CLAVE PRIVADA

La clave privada se encuentra siempre en posesión del suscriptor quedando a responsabilidad del mismo su resguardo.

La clave privada se encuentra almacenada en dispositivos de hardware criptográfico USB TOKEN.

12.2.6. INTRODUCCIÓN DE LA CLAVE PRIVADA AL MÓDULO CRIPTOGRÁFICO

La clave privada se genera durante la entrega del dispositivo TOKEN al solicitante.

12.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada es activada luego de realizado el proceso de inicialización del dispositivo TOKEN durante la entrega al solicitante.

12.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

No aplica.

12.2.9. MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Para una destrucción de la clave privada deberá inicializarse nuevamente el dispositivo criptográfico TOKEN.

12.2.10. CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS

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

12.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

12.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La clave pública se encuentra almacenada en el dispositivo criptográfico junto con el certificado generado.

12.3.2. PERÍODO DE USO DE LAS CLAVES

Los certificados emitidos al amparo de la presente política tienen una validez de un (1) año.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de un (1) año.

12.4. DATOS DE ACTIVACIÓN

12.4.1. GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada consisten en el PIN del dispositivo criptográfico TOKEN que la contiene.

La elección del PIN del TOKEN la realiza el subscriptor al momento de inicializarlo en la Agencia de Registro previo a que se le haga entrega del dispositivo.

12.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

El suscriptor del certificado es el responsable de la protección de los datos de activación de su clave privada.

12.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulado.

12.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Certificaciones Digitales Digicert S.R.L. tiene establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones. 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.

12.6. 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 y ATT-DJ-RAR-TL LP 211/2018 emitida por la ATT.

12.6.1. 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.

12.6.2. 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.

12.6.3. 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.

12.7. 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.

12.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

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

12.8.1. 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.

13. PERFILES DE CERTIFICADO, CRL Y OSCP

13.1. PERFIL DE CERTIFICADO DE SIGNATARIO

13.1.1. CERTIFICADO DE PERSONA JURIDICA CUSTODIADO EN NUBE PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.2.0.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular **title, Title:** Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.2. CERTIFICADO DE PERSONA JURIDICA CUSTODIADO EN NUBE PARA FIRMA DIGITAL SIMPLE

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.2.0.0 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular **title, Title:** Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional)

	serialNumber, Serial number (in DN): Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.3. CERTIFICADO DE PERSONA JURIDICA PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.1.0.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular

	title, Title: Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.4. CERTIFICADO DE PERSONA JURIDICA PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL SIMPLE

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.1.0.0 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl

	CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular **title, Title:** Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.5. CERTIFICADO DE PERSONA JURIDICA PKCS12 (SOFTWARE) PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection

Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.0.0.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular **title, Title:** Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** NORMAL
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.6. CERTIFICADO DE PERSONA JURIDICA PKCS12 (SOFTWARE) PARA FIRMA DIGITAL SIMPLE

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0

	Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.0.0.0 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **O, Organization:** Razón Social de la institución a la que pertenece el titular **OU, Organizational Unit:** Área de trabajo del titular **title, Title:** Cargo de trabajo del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** NORMAL
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.7. CERTIFICADO DE PERSONA NATURAL EN NUBE PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1

	Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.2.1.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria (opcional) **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.8. CERTIFICADO DE PERSONA NATURAL EN NUBE PARA FIRMA DIGITAL SIMPLE

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits

Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.2.1.0 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.9. CERTIFICADO DE PERSONA NATURAL PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3
Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación	Algoritmo: RSA

de claves	Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.1.1.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.10. CERTIFICADO DE PERSONA NATURAL PKCS11 (TOKEN/HSM) PARA FIRMA DIGITAL AUTOMATICA

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3

Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 1 Non-repudiation: 1 Key encipherment: 1 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Client Authentication Code Signing Email Protection
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.1.1.0 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name:** Nombres y Apellidos del titular **C, Country (ISO 3166):** BO **dnQualifier, DN Qualifier:** Tipo de documento **uidNumber:** Número de documento de identidad **UID, Unique Identifier:** Número de complemento (opcional) **serialNumber, Serial number (in DN):** Número de Identificación Tributaria **description, Description:** ALTO
Subject Alternative Name	**RFC 822 Name (e-mail address) (RFC822NAME):** Correo electrónico del titular

Formato de nombres

Los certificados emitidos por Certificaciones Digitales Digicert S.R.L. contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500.

13.1.11. CERTIFICADO PARA LAS TSUS

A continuación, se detallan los campos que se utilizan para un certificado digital del presente perfil:

Versión X.509	3

Algoritmo de Firma	SHA256WithRSA
Algoritmo de generación de claves	Algoritmo: RSA Longitud ideal de clave: 2048 bits Longitud mínima de clave: 2048 bits
Key Usage	Digital Signature: 1 Data encipherment: 0 Non-repudiation: 1 Key encipherment: 0 CRL sign: 0 Key agreement: 0 Encipher only: 0 Key certificate sign: 0 Decipher only: 0
Extended Key Usage	Time Stamping
Certificate Policies	Certificate Policy OID: 2.16.68.0.0.0.1.14.1.2.0.2.2.1.2.1 CPS URI: http://www.digicert.bo/ecpdigicert.pdf
Basic Constraints	Subject Type: End Entity
CRL Distribution Points	CRL Distribution Point URI: http://www.digicert.bo/crl CRL Issuer: CN=Entidad Certificadora Autorizada Digicert,O=Digicert,C=BO
Authority Information Access	OCSP Service Locator URI: http://www.digicert.bo/ocsp/ CA issuer URI: http://www.digicert.bo/digicert.pem
Subject DN Attributes	**CN, Common name (CN):** Autoridad de Sellado de Tiempo Digicert **O, Organization (O):** Digicert **C, Country (ISO 3166) (C):** BO

13.2. PERFIL DE CRL

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

a) Versión (versión):
   El valor del campo es 1 (corresponde a la versión 2 del estándar);
b) Algoritmo de firma (signatureAlgorithm):
   Identificador de Objeto (OID) del algoritmo utilizado por la Entidad Certificadora Pública para firmar la Lista de Certificados Revocados;
c) Nombre del Emisor (Issuer):
   CN = “Entidad Certificadora 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 son, 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.

13.3. PERFIL DE 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

14. AUDITORIA DE CONFORMIDAD

14.1. 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.

14.2. 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.

14.3. 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.

15. ADMINISTRACION DOCUMENTAL

15.1. PROCEDIMIENTO PARA CAMBIO DE ESPECIFICACIONES

Certificaciones Digitales Digicert S.R.L. cuenta con procedimientos internos para la administración de los cambios sobre la presente Política de Certificación.

En caso de que Certificaciones Digitales Digicert S.R.L. realice una modificación mayor en la presente política como respuesta a una modificación a la normativa, notificar a ATT sobre el cambio.

15.2. PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN

Certificaciones Digitales Digicert S.R.L. publica en su sitio web las modificaciones (nuevas versiones) aprobadas y realizadas a la presente Política de Certificación.

Certificaciones Digitales Digicert S.R.L. debe notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación.

ANEXO 1: PLAN DE CESE DE ACTIVIDADES

1. Introducción

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) presentó la Resolución Administrativa ATT-DJ-RAR-TL LP 202/2019 que establece los requisitos, condiciones legales, económicas y técnicas para la autorización de la prestación de servicio de Firma y Certificación Digital. El artículo 12 inciso b de esta Resolución establece como requisito la presentación del Plan de Cese de actividades.
El presente anexo tiene como objetivo cumplir con los lineamientos establecidos para el plan de cese de actividades.

2. Supuestos para el cese de actividades

El cese de actividades de Digicert S.R.L. como Entidad Certificadora se producirá siempre y cuando se revoque el permiso que otorga a la institución la atribución del servicio de certificación digital. Mientras tanto, Digicert S.R.L. tiene establecido un período de vigencia u operación en virtud de la Ley 164 de Telecomunicaciones.

3. Sujetos involucrados en el proceso de cese de actividades

El cese de actividades de Digicert S.R.L. como Entidad Certificadora involucra directamente a todos los titulares de los certificados digitales. Digicert S.R.L. toma una serie de recaudos para minimizar el impacto de la finalización de sus servicios, que son descritos en el procedimiento siguiente.

4. Procedimiento

La función del Plan de Cese de actividades de la Entidad Certificadora es asegurar que la transición de funciones a otra entidad se realice de manera ordenada, resguardando la información generada durante el período de actividad. El período de implementación del Plan se realiza desde la declaración de Cese de Actividades hasta la inhabilitación lógica y física de la Autoridad Certificante, la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes. A partir del cese de actividades, Digicert S.R.L. ya no emite nuevos certificados, solo se remite a publicar la lista de certificados revocados. Digicert S.R.L. en todo este período vela por minimizar el impacto de los titulares de los certificados digitales, a través de estrategias y procedimientos delineados a continuación.

4.1. Publicación

Ante la declaración del cese de los servicios de certificación, la primera tarea es publicar la información en el sitio web: ww.digicert.bo.
Esta publicación debe realizarse con dos meses de antelación. Si es que hubiese suscriptores a nivel nacional, también se debe publicar en un medio de difusión nacional.

4.2. Notificación

Digicert S.R.L. notifica a todos los y las suscriptores de los certificados digitales del cese de actividades cuyos certificados permanezcan en vigencia. La misma se lleva a cabo con una antelación mínima de dos (2) meses. La notificación se realiza mediante correo electrónico firmado digitalmente y la página web de la institución, por el transcurso del tiempo que dure la transición del servicio a otra entidad. Las mismas indican la fecha precisa del cese de actividades, señalando además que, de no existir objeción a la transferencia de los certificados digitales, dentro del plazo de quince (15) días hábiles, contados desde la fecha de la comunicación, se entiende que el usuario ha consentido la transferencia de los mismos. Si se hubiese emitido certificados a nivel nacional, debe publicarse en un medio de prensa.

4.3. Solicitud del certificado

Una vez anunciado el cese de actividades de Digicert S.R.L. como Entidad Certificadora, se rechaza la solicitud de emisión de un nuevo certificado, de cualquier tipo, por parte de un suscriptor dentro de los sesenta (60) sesenta días calendarios anteriores a la fecha prevista para el cese. Digicert S.R.L. también rechazará toda solicitud de renovación de un certificado por parte de un suscriptor de los sesenta (60) días corridos anteriores a la fecha prevista para el cese.

4.4. Revocación de Certificados y Lista de Certificados Revocados

Digicert S.R.L. debe proceder de la siguiente manera para la revocación de los certificados.

a) Se puede revocar certificados de suscriptores hasta el mismo día y hora del cese de actividades. Solamente puede efectuar revocaciones a solicitud de sus suscriptores. Si los suscriptores, después de haber sido notificados del cese de actividades de la Entidad Certificadora, dentro del plazo de quince (15) días contados de la fecha de la notificación, se entiende que el usuario ha consentido la transferencia del certificado digital.
b) Coloca a disposición de la ATT los certificados que se encuentre vigentes, hasta tanto se produzca el vencimiento de la totalidad de los certificados emitidos por la Digicert S.R.L.
c) Actualiza la lista del repositorio de los certificados digitales.
d) Emite una lista de certificados revocados (CRL) hasta la fecha prevista de cese de actividades.
e) Inmediatamente de revocados los certificados, Digicert S.R.L. emite una última lista de certificados revocados.
f) La última lista CRL está disponible para consultas, como mínimo hasta el último día del cese de funciones.

4.5. Desactivación y custodia de los equipos

A partir del cese de actividades, los equipos de Digicert S.R.L., incluidos los que soporta a la clave privada, quedan desafectados de la emisión y revocación de certificados. No obstante, permanecen en custodia de Digicert S.R.L., para:

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

Después, del periodo de custodia, Digicert S.R.L. puede disponer libremente de los equipos que hubiese dispuesto para el servicio de la certificación digital.
En forma previa a la desactivación se generan copias de respaldo de toda la información disponible. Los equipos de publicación de CRL continúan prestando el servicio hasta la finalización del último día de la fecha del cese de actividades de Digicert S.R.L. como Entidad Certificadora, según lo mencionado en el punto "4.4.- Revocación de Certificados y Lista de Certificados Revocados".

4.6. Transferencia de certificados

Al producirse el cese de sus actividades, se admite que Digicert S.R.L. realice una transferencia de los certificados emitidos a sus suscriptores a favor de otra entidad certificadora, establecido en la Ley 164. Para ello se requiere un acuerdo previo entre ambas entidades certificadoras, con aprobación de la ATT, Certificadora Raíz, que deberá ser firmado por las máximas autoridades respectivas.
Dicho acuerdo debe indicar que la Autoridad Certificante continuadora toma a su cargo la administración de la totalidad de los certificados emitidos por Digicert.S.R.L. que cesa sus actividades, que no hubieran sido revocados a la fecha de la transferencia. Se envían copias del mencionado acuerdo a la ATT para su archivo.
Asimismo, Digicert S.R.L. transfiere a la Autoridad Certificante continuadora toda la documentación que obre en su poder y que hubiera generado en el proceso de emisión y administración de certificados, así como la totalidad de los archivos y copias de resguardo, en cualquier formato y toda otra documentación referida a su operatoria.
Digicert S.R.L. informa acerca de la transferencia en las publicaciones y notificaciones que efectúe referidas al cese de sus actividades mencionadas en los apartados 4.1 y 4.2. Además, cumple con la totalidad de los procedimientos indicados en el mismo.

4.7. Procedimientos

Una vez anunciada la fecha del cese de funciones de Digicert S.R.L. como Entidad Certificadora, se lo comunica a todo el personal y cada uno de los roles debe proceder de acuerdo a los descrito en este Plan. Para este efecto, se distribuye una copia de este documento a todo el personal directamente o indirectamente involucrado.
El Comité de Gestión de Calidad de la Entidad Certificadora ejerce la supervisión de las operaciones relacionadas, tomando en cuenta el resguardo de la información generada, y velando por la minimizar el impacto del servicio a los suscriptores.

4.8. Resguardo de información histórica

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

- Los archivos de documentación presentada por solicitantes y suscriptores;
- La documentación relacionada con pedidos de revocación;
- La documentación generada en las ceremonias digitales.

También guarda una copia de la información generada mientras Digicert S.R.L. estuvo activa:

- La última lista de certificados revocados;
- El backup de los servidores y de su configuración;
- Los libros de Actas.

5. Modificaciones al Plan de cese de Actividades

Toda modificación a las previsiones de este plan se hace con intervención del Comité de Gestión de Calidad de la Firma digital. Antes de su puesta en vigencia, el documento modificado es sometido a la aprobación de la Autoridad Certificadora Raíz, la ATT.

ANEXO 2: POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

1. Introducción

1.1. Descripción general

Descripción del servicio

Un certificado digital emitido por Digicert S.R.L. le permite al cliente realizar firmas digitales avanzadas y autenticar su identidad con la validez legal, vincula un documento digital o mensaje electrónico de datos y garantiza la integridad del documento digital o mensaje electrónico con firma digital. La certificación que emite Digicert S.R.L., contempla: personas jurídicas y personas naturales.
La Firma Digital consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos digitales. La clave privada siempre se encuentra en posesión del firmante y es la utilizada para realizar firmas. La pública se divulga y es la utilizada para verificar una firma de otro sujeto.
Todo lo descrito se encuentra validado por la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.

1.2. Identificación y nombre del documento

1.2.1 Políticas de Protección de Datos

La Entidad Certificadora considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que cursan a través de las TICs, para otorgar seguridad y protección a la intimidad del usuario que navega en la red.

1.2.2 Nombre

El presente documento lleva como título “Contenido mínimo de las políticas de certificación para una entidad certificadora. Políticas de certificación. Anexo 2. Política de Protección de Datos Personales”.

1.2.3 Versión de fecha de elaboración

Elaborado desde el 16 de Febrero hasta el 14 de Marzo del año 2018.

1.2.4 Fecha de actualización

Revisado y actualizado en fecha 23-nov-2023.

1.2.5 Sitio web de consulta

El sitio web de consulta es: ww.digicert.bo

2. Conceptos fundamentales:

a) Archivo o Banco de Datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento físico, electrónico, magnético o informático, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
b) Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada.
c) Cesión de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.
d) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.
e) Datos personales: toda información de cualquier tipo referida a personas individuales o colectivas determinadas o determinables.
f) Datos sensibles: datos personales que revelen filiación política o filosófica, credo religioso, ideología, afiliación sindical e informaciones referentes a origen racial y étnico, salud u orientación sexual.
g) Destinatario: persona individual o colectiva, pública o privada, que reciba cesión de datos, se trate o no de un tercero.
h) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.
i) Encargado del tratamiento: persona individual o colectiva, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable del archivo o banco de datos o del tratamiento.
j) Tercero: la persona individual o colectiva, pública o privada, distinta del titular del dato, del responsable del archivo o banco de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.
k) Responsable del tratamiento: persona individual o colectiva, pública o privada, propietaria del archivo o banco de datos o que decida sobre la finalidad, contenido y uso del tratamiento.
l) Titular de los datos: es la persona natural o jurídica a quien se refiere la información que reposa en un archivo o banco de datos.
m) Tratamiento de datos personales: Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
n) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en un archivo o banco de datos propio o a través de conexión con los mismos.
o) Fuentes accesibles al público: aquellos archivos o banco de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.
p) Firma Digital: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.
q) Protección de datos personales: Toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable.
r) Servicio de certificación digital: Consiste en emitir, revocar y administrar los certificados digitales utilizados para generar firmas digitales.
s) Servicio de registro: Consiste en comprobar y validar la identidad del solicitante de un certificado

3. Principios

Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios:

Principio de Finalidad.

La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;

Principio de Veracidad.

La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;

Principio de Transparencia.

Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;

Principio de Seguridad.

Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;

Principio de Confidencialidad.

Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

4. Derechos de los Titulares de Datos

Los titulares de los datos, tendrán los siguientes derechos:

- Derecho de información y contenido de la información.
- Derecho de conocer los datos registrados.
- Derecho de rectificación, actualización, inclusión o eliminación.
- Datos sensibles: Ninguna persona puede ser obligada a proporcionar datos sensibles, como ser: Ideología, religión, salud, origen racial o étnico y otros. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular y/o cuando medien razones de interés general autorizadas por ley, o cuando la Entidad Certificadora tenga mandato legal para hacerlo.

5. Información que es recopilada

La información que es recopilada desde la plataforma web esta en función al tipo de persona que requiere los servicios, es decir si es persona Natural o Jurídica y se solicitan la siguiente información:

a) Personas Naturales
Ciudad de Ingreso de la Solicitud
Nombres del titular
Apellido Paterno del titular
Apellido Materno del titular
Fecha de Nacimiento del titular
Numero de celular del titular
Correo electrónico
Tipo de documento
Nro de documento de identidad
Complemento (si corresponde)
Expedición del documento de identidad
Dirección del domicilio
Adjunto: Copia del anverso del documento de identidad
Adjunto: Copia del reverso del documento de identidad
Adjunto: Aviso de cobranza de servicios publico (agua o luz)

b) Personas Jurídicas

Ciudad de Ingreso de la Solicitud
Nombres del titular
Apellido Paterno del titular
Apellido Materno del titular
Fecha de Nacimiento del titular
Numero de celular del titular
Correo electrónico
Tipo de documento
Nro de documento de identidad
Complemento (si corresponde)
Expedición del documento de identidad
Numero de Identificación Tributaria
Nombre de la Organización
Unidad Organizacional (opcional)
Cargo en la Organización
Dirección del domicilio (representante legal)
Dirección de ubicación de la Organización
Adjunto: Copia del anverso del documento de identidad (titular)
Adjunto: Copia del reverso del documento de identidad (titular)
Adjunto: Carta de autorización
Adjunto : Copia del Numero de Identificación Tributaria
Adjunto: Copia del anverso del documento de identidad (representante legal)
Adjunto: Copia del reverso del documento de identidad (representante legal)
Adjunto: Poder del representante Legal

6. Como usamos la información provista por el Titular de los Datos

Los datos personales registrados e información adjunta descritos en el punto anterior se utilizan para las siguientes finalidades:

a) Para realizar las validaciones y contrastaciones de datos con el Segip para garantizar veracidad de los datos ingresados.
b) Para la generación de los contratos entre el titular y Certificaciones Digitales Digicert.
c) Para el procesamiento de la generación y emisión del certificado digital
d) Para el procesamiento de la generación de firmas de documentos adjuntados por el Titular
e) Para la emisión de las correspondiente facturación por el uso del servicio
f) Para que nuestros operadores internos puedan revisar , observar o aprobar toda la información enviada
g) Para contactar al titular de los datos en el momento que se lo requiera.
h) Para el envío de la información procesada referente a contratos generados, formularios, certificado emitido, documentos firmados.

7. Modificación o Actualización de los Datos Registrados

Referente a la Modificación o Actualización de los Datos Registrados son procesados acorde a los dos siguientes escenarios:

- Cuando esta en proceso de emisión del certificado.- Mientas no este emitido el certificado ni generado el contrato es posible poder hacer correcciones o actualizaciones de los datos ingresados.
- Cuando ya fue emitido el certificado.- Después de emitido el certificado solamente podrá actualizarse el correo electrónico para el reenvío de alguna información requerida por el titular, previo envío de carta de solicitud.

8. Conservación de los datos provistos por el Titular de los Datos

Retenemos los datos personales e información recopilada a través de los formularios de registro desde la plataforma web, para fines operativos , de registro , validaciones y legales. Retendremos los datos personales durante el periodo necesario para cumplir con los fines descritos en esta Política.

9. Marco legal nacional para el tratamiento de los datos personales en materia de telecomunicaciones

La Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información Y Comunicación, en su Art. 56 (Inviolabilidad y Secreto de las Telecomunicaciones) señala*: "En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma"*.

Por otro lado, el Art. 56 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, a fin de garantizar los datos personales y la seguridad informática de los mismos, adopta 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.

c) 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;

d) 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;

e) 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, las 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.

El Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, en el Art. 176 establece:

Artículo 176.- (Protección de los Datos Personales).

I. El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.
II. Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los usuarios del servicio, salvo en los siguientes casos:

a) De existir una orden judicial específica;
b) Con consentimiento previo, expreso y por escrito del usuario titular;
c) En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de

información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo.

III. El operador o proveedor de servicios deberá coadyuvar en la identificación de los presuntos responsables de vulneraciones a la inviolabilidad, secreto de las comunicaciones, protección de los datos personales y la intimidad de los usuarios, que su personal pudiera cometer en las instalaciones del operador o proveedor.

IV. La ATT aprobará los procedimientos y medidas utilizadas por los operadores y proveedores para salvaguardar la inviolabilidad y secreto de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

V. Queda prohibido que los operadores y proveedores de servicios permitan el acceso a registros o bases de datos de sus usuarios, ya sea de manera individual o a través de listas de usuarias, usuarios o números, con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita de la usuaria o usuario que desee recibir dicha publicidad.

Asimismo, de conformidad a lo establecido en el artículo 43 inciso i) del D.S 1793, la Entidad Certificadora mantendrá 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.
Finalmente, el Art. 43 inciso b) del Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013, señala:
"*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*".

10. Marco jurídico aplicable:

Asimismo, las disposiciones legales y reglamentarias que regulan la protección de datos, son:
- Constitución Política del Estado
- Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación, de fecha 08 de agosto de 2011.
- Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013.
- Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, de fecha 24 de octubre de 2012.
- Decreto Supremo N° 28168, que garantiza el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo, de fecha 17 de mayo de 2005.
- Estándares Técnicos emitidos por la ATT.