POLÍTICA DE CERTIFICACIÓN DE PERSONA JURÍDICA

Certificaciones Digitales Digicert S.R.L

Tabla de Contenido

0. GESTIÓN DEL DOCUMENTO

FIRMA		FIRMA		FIRMA	
Elaborado por		**Revisado por**		**Aprobado por**	
Nombre		**Nombre**		**Nombre**	
Cargo		**Cargo**		**Cargo**	
Fecha		**Fecha**		**Fecha**	

1. CONTROL DE CAMBIOS

1.1. CAMBIOS A LA POLÍTICA DE CERTIFICACIÓN DE PERSONA JURÍDICA

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

1.2. DETALLE DE CAMBIOS

Revisión	Fecha	Detalle de modificaciones
0	2016-11-30	Versión inicial del documento
1	2018-02-28	Revisión – Observaciones ATT

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 Transportes y Telecomunicaciones.
CP: (Certificate Policy) Política de Certificación.
CPS: (Certification Practice Statement) Declaración de Prácticas de Certificación.

TIC: Tecnologías de Información y Comunicación.
ISO: (International Organization for Standardization) Organización Internacional de Normalización.
OID: (Object Identifier) Identificador de Objeto.
SGSI: Sistema de Gestión de Seguridad de la Información.

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 conforma su identidad. El certificado digital es válido únicamente dentro del período de vigilancia, 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) **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.

3 INTRODUCCIÓN

3.1 DESCRIPCIÓN GENERAL

El presente documento constituye la Política de Certificación (*Certificate Policy*) de Persona Jurídica de Certificaciones Digitales Digicert S.R.L (a partir de ahora CP de Persona Jurídica), emitida en cumplimiento a las Resoluciones Administrativas Regulatorias **ATT-DJ-RA TL LP 31/2015**, ATT-DJ-RA TL LP 32/2015 y ATT-DJ-RA TL LP 1538/2015 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 a Personas Jurídicas. De esta manera se pretende dar transparencia al conjunto de tareas relacionadas con la provisión de estos servicios. **Cabe mencionar que lo establecido en este documento no excluye lo definido en CP-ECA-01 "Política de certificación de Persona Natural".**

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 de Persona Jurídica**".

Se publicará 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 firmará su certificado y emitirá 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.

3.3.4 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 terciarizado, que está sujeta 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 el Estándar vigente de Agencias de Registro.

3.3.5 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.

3.3.6 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 del certificado de Persona jurídica está limitado a:

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

Cabe destacar que los usos definidos serán en representación de una persona jurídica 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 serán aplicable un proceso penal establecido en el Código Penal, Artículo 363 (alteración, acceso y uso indebido de datos informáticos).

Adicionalmente, le será revocado el certificado digital y el usuario contratante asume la responsabilidad de indemnizar a 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 persona jurídica no pueden ser utilizados en remplazo de los certificados de persona natural o de cargo público, en particular no se pueden firmar documentos como una persona natural o como servidor público con un certificado de persona jurídica.

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 es 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 mantiene 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: info@certificacionesdigitales.bo
Teléfono: (591)(3)3339093

3.5.2 Procedimiento de aprobación

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

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

4 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 anunciara en la página web de la Entidad Certificadora.

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

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

5 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

5.1 REGISTRO DE NOMBRES

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 en determinadas atribuciones;
- **O =** Razón social de la empresa o institución a la que representa la persona jurídica;
- **OU =** Unidad Organizacional de la que depende (opcional);
- **C =** Estándar de acuerdo a ISO 3166 {BO};
- **serialNumber =** Tipo, numero de documento de identidad y el lugar de emisión.

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

5.2 VALIDACIÓN DE LA IDENTIDAD INICIAL

5.2.1 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 o en el navegador web del mismo si el proceso es en línea.

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

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

5.2.2. 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:

- Cédula de Identidad vigente o Documento de Identidad extranjero; y
- Autorización original de la persona jurídica firmada por su Representante Legal.

El Agente de Registro de Certificaciones Digitales Digicert S.R.L, comprueba los datos relativos a la constitución y personalidad jurídica, extensión y vigencia de las facultades de representación del solicitante.

Certificaciones Digitales Digicert S.R.L guarda copia de la documentación presentada por el solicitante.

5.2.3 Autenticación de la identidad de un individuo

El derecho de solicitud de certificados definido en la presente Política de Certificación se encuentra limitado a personas jurídicas. Por tanto, no se considera necesaria la identificación de un individuo en calidad de persona natural.

- 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 del nombramiento o certificado laboral del solicitante firmado por el Representante Legal de la empresa u organización solicitante.
- Autorización original de la persona jurídica solicitada por el Representante Legal.

5.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE CLAVE

5.3.1 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.

5.3.2Identificación 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.

5.4 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:

5.4.1 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

5.4.2 Telemática. Mediante la firma electrónica del formulario de revocación ubicado en el área personal de servicios de certificación.

5.4.3 Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico habilitado para tal fin.

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.

6 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 solicitante del certificado que desee que le sea emitido un Certificado de Persona Jurídica de acuerdo con esta política de certificación debe presentarse para solicitarlo en una Agencia de Registro Autorizada de Certificaciones Digitales Digicert S.R.L y presentar la documentación que se exige en el punto 3.2. de la presente política, bajo el título "Autenticación de la identidad de una organización".

El listado de agencias de registro autorizadas se encuentra en la URL www.certificacionesdigitales.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 recibirá 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 la 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 entrega 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 1.4 de esta Política de Certificación.

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 y teléfono del suscriptor.

Revocación y suspensión de certificados

1. <u>Circunstancias para la revocación</u>

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 AR o 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:

3.1 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.

3.2 Telemático. Existe un formulario de solicitud de revocación de certificados en la web de Certificaciones Digitales Digicert S.R.L, en la URL www.certificacionesdigitales.bo, dentro del área personal de servicios de certificación.

3.3 Telefónico. Mediante llamada telefónica al número de soporte telefónico de Certificaciones Digitales Digicert S.R.L al (591)(3) 3339093.

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

Sólo se suspende un certificado si así lo dispone una autoridad jurídica, por el tiempo que la misma establezca.

Certificaciones Digitales Digicert S.R.L no soporta la suspensión de certificados como operación independiente sobre sus certificados.

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) 3339093.

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 produce 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 www.certificacionesdigitales.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 quedará 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.

7 CONTROLES OPERACIONALES O DE GESTIÓN

7.1 CONTROLES DE SEGURIDAD FÍSICA

7.1.1 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.

7.1.2 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.

7.1.3 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 produce 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.

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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.

7.1.8 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.

7.2 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.

7.2.1 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).

7.2.2 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.

7.2.3 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.

7.3 CONTROLES DE SEGURIDAD DE PERSONAL

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.3.4 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 toman medidas disciplinarias. Se consideran 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.

7.3.5 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.

7.3.6 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.

7.3.7 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

7.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

7.4.1 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.

7.4.2 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.

7.4.3 Período de retención para los registros de auditoría

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

7.4.4 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.

7.4.5 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.

7.4.6 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.

7.4.7 Notificación al sujeto causante del evento

No estipulado.

7.4.8 Análisis de vulnerabilidades

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

7.5 ARCHIVOS DE INFORMACIÓN Y REGISTROS

7.5.1 Tipos de información y eventos registrados

Certificaciones Digitales Digicert S.R.L archiva 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.

7.5.2 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.

7.5.3 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.

7.6 CAMBIO DE CLAVE

No estipulado.

7.7 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.

7.8 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 y además cuenta con un plan de cese de actividades de acuerdo al artículo 51 del reglamento para el desarrollo de las TIC, decreto supremo Nr. 1793. Certificaciones Digitales Digicert S.R.L tiene contemplado en la eventualidad que ocurra un cese de operaciones, los siguientes supuestos:

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

8 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 6.1 de la Declaración de Prácticas de Certificación (CPS) de Certificaciones Digitales Digicert S.R.L.

8.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

8.1.1 Generación del par de claves

Los pares de claves para los certificados emitidos bajo esta Política de Certificación pueden generarse de las siguientes formas:

Navegador Web: Durante el trámite iniciado en el sitio web de Certificaciones Digitales Digicert S.R.L se puede optar por generar de forma local el par de claves en el PC utilizado por el solicitante.
Solicitud PKCS#10: El solicitante genera por sus propios medios el par de claves y adjunta el request PKCS#10 en el formulario de solicitud web.
En dispositivo criptográfico TOKEN: El par de claves se genera durante la inicialización de un dispositivo criptográfico TOKEN entregado durante el trámite presencial.

8.1.2 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.

8.1.3 Hardware y software de generación de claves

Los dispositivos criptográficos entregados en la modalidad de generación del par de claves en TOKEN son certificados FIPS 140-2 nivel 2.

8.2 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.

8.2.1 Estándares para los módulos criptográficos

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

8.2.2 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.

8.2.3 Custodia de la clave privada

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

8.2.4 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.

8.2.5 Archivo de la clave privada

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

8.2.6 Introducción de la clave privada al módulo criptográfico

Si la opción de solicitud es en TOKEN USB la clave privada se genera durante la entrega del dispositivo TOKEN al solicitante.

8.2.7 Método de activación de la clave privada

Si la opción de solicitud es en TOKEN USB la clave privada es activada luego de realizado el proceso de inicialización del dispositivo TOKEN durante la entrega al solicitante.

Si la opción de solicitud es en navegador web la clave privada es activada luego de la generación en PC utilizado por el suscriptor.

Si la opción es avanzada PKCS#10, la clave privada es activada durante la generación realizada por el suscriptor.

8.2.8 Método de desactivación de la clave privada

No aplica.

8.2.9 Método de destrucción de la clave privada

Para una destrucción de la clave privada almacenada en un dispositivo criptográfico TOKEN o HSM debe inicializarse nuevamente el dispositivo.

Para una destrucción de la clave privada generada en archivo por el navegador web u otro medio, la destrucción debe realizarse mediante un borrado seguro del archivo.

8.2.10 Clasificación de los módulos criptográficos

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

8.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

8.3.1 Archivo de la clave pública

Si la opción de solicitud es en TOKEN USB la clave pública se encuentra almacenada en el dispositivo criptográfico junto con el certificado.

Si la opción de solicitud es en navegador web la clave pública se encuentra almacenada en el repositorio de claves del equipo junto con el certificado.

Si la opción es avanzada PKCS#10, la clave pública se encuentra almacenada junto con la clave privada generada por el suscriptor.

8.3.2Período 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.

8.4 DATOS DE ACTIVACIÓN

8.4.1 Generación de los datos de activación

Los datos de activación de la clave privada consisten en un PIN ingresado por el suscriptor durante la generación del par de claves tanto en el navegador web como dispositivo criptográfico TOKEN.

8.4.2 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.

8.4.3 Otros aspectos de los datos de activación

No estipulado.

8.5 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 coloca a disposición de la ATT, el repositorio de todos los certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos.

8.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

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

8.6.1Controles 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.

La entidad no realiza desarrollo *in-house* pero utiliza software a medida desarrollado y mantenido por terceros. 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.

8.6.2 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.

8.6.3 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.

8.7 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.

8.8 CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

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

8.8.1 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.

9 PERFILES DE CERTIFICADO, CRL Y OSCP

9.1 PERFIL DE CERTIFICADO

9.1.1 Formato del certificado

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

a) Versión (version)
   El valor del campo es 2.
b) Número de Serie (serialNumber):
   Número asignado por la ECA.
c) Algoritmo de firmas (signatureAlgorithm):
   OID: 1.2.840.113549.1.15 (SHA256withRSA).
d) Nombre del Emisor (issuer):
   CN = "Entidad Certificadora Certificaciones Digitales Digicert S.R.L";
   O = "Certificaciones Digitales Digicert S.R.L";
   C = BO, de acuerdo a ISO3166.
e) Periodo de validez (validity):
   Fecha de emisión del Certificado, YYYYMMDDHHMMSSZ (formato UTC Time);
   Fecha de caducidad del Certificado, formato UTC Time.
f) Nombre suscriptor (subject):
   CN = Nombres y Apellidos del representante legal autorizado para representar a la persona jurídica en determinadas atribuciones;
   O = Razón social de la empresa o institución a la que representa la persona jurídica;
   OU = Unidad Organizacional de la que depende (opcional);
   T = Cargo del representante legal;
   C = estándar de acuerdo a ISO 3166 {BO};
   dnQualifier = Tipo de documento {CI/CE};
   uidNumber = Número de documento {numeral};
   uid = Número de complemento {alfanumérico} (opcional);
   serialNumber = Número de NIT {numeral} (opcional).
g) Clave pública del suscriptor (subjectPublicKey):
   Algoritmo: RSA;
   Longitud: mínimo 2048 bits.

9.1.2 Extensiones del certificado

Las extensiones del Certificado Digital de una Persona Jurídica son las siguientes:

a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier):
   Valor de la Extensión subjectKeyIdentifier del certificado de la ECA emisora.
b) Identificador de la clave del suscriptor (subjectKeyIdentifier):
   Función Hash (SHA1) del atributo subjectPublicKey.
c) Uso de Claves (keyUsage):
   digitalSignature = 1;

nonRepudiation = 1;
keyEncipherment = 1;
dataEncipherment = 1;
keyAgreement = 0;
keyCertSign = 0;
cRLSign = 0;
encipherOnly = 0;
decipherOnly = 0.

d) Uso de Claves Extendido (Extended Key Usage):
clientAuth;
EmailProtection;
codeSigning.

e) Política de Certificación (certificatePolicies):
URI: (archivo en formato de texto).

f) Restricciones Básicas (basicConstraints):
CA = FALSE.

g) Punto de distribución de las CRL (cRLDistributionPoints):
URI: (.crl).

h) Información de Acceso de la ECA (authorityInformationAccess):
URI:(.crt).

i) Nombre Alternativo del Suscriptor (subjectAlternativeName):
E = Correo electrónico del suscriptor.

9.1.3 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.

El campo cn del subject name se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra “Ñ” por la “N” y la letra “Ç” por la “C”. Esta característica se da únicamente en el atributo CommonName.

9.1.4 Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

9.2 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 Certificaciones Digitales Digicert S.R.L”;
   O = “Certificaciones Digitales Digicert S.R.L”;
   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.

9.3 PERFIL DE OSCP

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

10 ADMINISTRACIÓN DOCUMENTAL

10.1 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 desee una modificación en la presente política debe realizar la solicitud a la ATT con la correspondiente justificación, la ATT evalúa la solicitud y en caso de aprobarla, realiza la modificación y posterior publicación de la nueva versión.

10.1 Procedimientos de publicación y notificación

La ATT publica en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos remplazados junto con la publicación de la nueva versión.

Certificaciones Digitales Digicert S.R.L debe notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación. De la misma forma, Certificaciones Digitales Digicert S.R.L debe publicar en su sitio web cualquier modificación aprobada por la ATT y notificar a los usuarios finales de los cambios realizados en caso de ser necesario.

ANEXO 1
Plan de Cese de actividades

1. Introducción

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) presentó la Resolución Administrativa RAR -DJ-RA TL LP 32/2015 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 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: certificacionesdigitales.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 esta 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 RAR -DJ-RA TL LP 32/2015 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 TIC's, 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

A ser acordado una vez se realicen las revisiones necesarias.

1.2.5 Sitio web de consulta

El sitio web de consulta es: certificacionesdigitales.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. 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 "*.

6. 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.