

## TERMINOS Y CONDICIONES GENERALES DE CONTRATACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL DE DIGICERT

Los Términos y Condiciones para la Provisión de la Certificación Digital contemplan la descripción del servicio que implementa **DIGICERT S.R.L**

### PRIMERA.- DEFINICIONES

**ATT** : Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes

**ECA**: Entidad Certificadora Autorizada.

**AR**: Agencia de registro quien brinda el servicio de recepción de solicitudes de Certificado Digital.

**Signatario**: Es el titular del certificado digital que utiliza el mismo para firmar digitalmente, bajo su exclusivo control.

**Usuario**: Persona natural o jurídica, beneficiario del servicio de certificación digital, que obtiene y/o autoriza la obtención y el uso del servicio para uno o varios signatarios.

**Contacto de Revocación**: Persona designada por el titular quien puede solicitar la suspensión, reactivación o revocación del certificado digital.

**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.

**Clave privada**: Conjunto de caracteres alfanuméricos generados mediante un sistema de cifrado que contiene datos únicos que el signatario emplea en la generación de una firma electrónica digital sobre un mensaje electrónico de datos o documento digital.

**Clave pública**: Conjunto de caracteres de conocimiento público, generados mediante el mismo sistema de cifrado de la clave privada; contiene datos únicos que permiten verificar la firma digital de signatario en el Certificado Digital

**Certificado revocado**: La revocación o la suspensión de un certificado corresponde a revocar o suspender su validez, por algún motivo, antes de su fecha de expiración.

**Emisión de Certificados**: Procedimiento por el cual la ECA, previo al cumplimiento de requisitos del signatario emite el certificado digital respectivo.

### SEGUNDA.- DESCRIPCIÓN Y OTROS ASPECTOS ASOCIADOS

Un certificado digital emitido por DIGICERT le permite al signatario realizar firmas digitales 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.

El servicio de certificación Digital responde a formatos y procedimientos de calidad y estándares reconocidos internacionalmente y fijados por la ATT, conteniendo la información necesaria para la identificación, vigencia y verificación de la firma digital.

### TERCERA.- ALCANCE DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL

La prestación del servicio de certificación digital contempla:

- a) La emisión, suspensión, revocación, reactivación y renovación de Certificados Digitales.
- b) Garantizar la prestación del servicio de forma permanente, confidencial, oportuna y segura.
- c) Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario;
- d) Validar y comprobar cuando corresponda, la identidad y existencia real de la persona natural o jurídica;
- e) Otros servicios relacionados con la prestación de servicios de certificación digital.

#### **3.1.- SUSPENSIÓN DE LA VIGENCIA**

El Decreto Supremo N° 1793, que aprueba el Reglamento a la Ley N° 164 de 8 de agosto de 2011, Ley de Telecomunicación y Tecnologías de Comunicación, establece:

- a) La vigencia de un Certificado Digital será suspendida por la ECA, cuando se verifique alguna de las siguientes circunstancias:
  - A solicitud del titular, usuario del certificado o persona de contacto de revocación, debidamente comunicada a la entidad certificadora;
  - Decisión de la entidad certificadora en virtud de razones técnicas, que será previamente comunicada a los signatarios;
  - Por orden o decisión judicial debidamente fundamentada que determine la suspensión provisional de la vigencia del certificado digital.
- b) En mérito a la suspensión de la vigencia, cesan de forma temporal los efectos jurídicos del Certificado Digital conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.
- c) La suspensión de la vigencia del Certificado Digital será levantada por cualquiera de las siguientes causas:
  - A requerimiento del titular, usuario del certificado o persona de contacto de revocación, cuando la suspensión haya sido solicitada por éste;
  - Cesación de las causas técnicas que motivaron la suspensión a criterio de la entidad certificadora;
  - Por orden o decisión judicial debidamente fundamentada que determine el cese de la suspensión de la vigencia del certificado digital.
- d) En las situaciones descritas en el parágrafo anterior, la ECA habilitará de manera inmediata el certificado digital.
- e) La suspensión de un certificado digital, no producirá, por sí sola, la invalidez jurídica de los actos que al amparo de dicho certificado se hayan realizado con anterioridad.

#### **3.2.- REVOCACIÓN DE UN CERTIFICADO DIGITAL**

El Decreto Supremo N° 1793, que aprueba el Reglamento a la Ley N° 164 de 8 de agosto de 2011, Ley de Telecomunicación y Tecnologías de Comunicación, establece:

- a) Un certificado digital será revocado en los siguientes casos:
  - A solicitud de su titular, usuario o persona de contacto de revocación, debidamente comunicada a la entidad certificadora;
  - Por fallecimiento del titular del certificado;
  - Por disolución o quiebra de la persona jurídica titular del certificado digital, a partir de la comunicación oficial recibida por la entidad certificadora;
  - Por causa judicialmente declarada o por requerimiento de autoridad competente conforme a Ley;
  - Cuando se corrobore que el titular del certificado digital no ha custodiado adecuadamente los mecanismos de seguridad, propios del funcionamiento del sistema de certificación, que le proporcione la entidad certificadora;
  - De comprobarse por parte de la ATT, que se han producido vulneraciones técnicas del sistema de seguridad de la entidad certificadora que afecte la prestación de servicios de certificación digital.
- b) La revocación del certificado digital no exime a su titular del cumplimiento de las obligaciones contraídas durante la vigencia del certificado.

#### **3.3.- CONSERVACIÓN DEL CERTIFICADO DIGITAL**

El Decreto Supremo N° 1793, que aprueba el Reglamento a la Ley N° 164 de 8 de agosto de 2011, Ley de Telecomunicación y Tecnologías de Comunicación, establece:

**I.** La conservación de la información contenida en un mensaje electrónico de datos o documento digital ambos con firma digital, deberá cumplir las siguientes condiciones:

- a) Estar en el formato original con el que haya sido generado, enviado o recibido, demostrando su integridad, la identidad del generador del mensaje electrónico de datos o documento digital, su origen, fecha, hora de creación, destino y otros;
- b) Ser accesible y disponible para posteriores consultas a requerimiento de autoridad competente;
- c) Ser conservada de acuerdo a la naturaleza del mensaje electrónico de datos o documento digital y la normativa vigente.

**II.** Para la conservación de la información contenida en mensajes electrónicos de datos o documentos digitales, la entidad certificadora podrá utilizar el servicio de terceros, garantizando la integridad de los mismos.

**III.** La información que tenga por única finalidad hacer conocer el envío o recepción de un mensaje electrónico de datos o documento digital está exenta de la obligación de conservarse.

Adicionalmente, la ECA y AR aplicará sus respectivos procedimientos y condiciones para la conservación de los documentos físicos y digitalizados, respaldados en normas legales vigentes, procesos institucionales, procesos archivísticos y basados en los requerimientos de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

#### **CUARTA.- VALIDEZ JURÍDICA DE DOCUMENTOS Y FIRMAS DIGITALES**

La Ley N° 164, del 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, establece la validez jurídica y probatoria de:

1. El acto o negocio jurídico realizado por persona natural o jurídica en documento digital y aprobado por las partes a través de firma digital, celebrado por medio electrónico u otro de mayor avance tecnológico.
2. El mensaje electrónico de datos.
3. La firma digital.

La misma ley realiza exclusiones en los siguientes actos y hechos jurídicos de su celebración por medio electrónicos:

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

#### **QUINTA.- MODALIDADES DE PRESTACIÓN DEL SERVICIO**

El servicio de certificación digital, conforme a lo establecido en la normativa vigente, comprende los siguientes tipos de certificados:

- a) Certificado de persona natural.- documento digital que pertenece y contiene los datos de una persona natural y tiene una duración máxima de un año.
- b) Certificado de Persona jurídica.- documento digital que pertenece y contiene los datos de una persona jurídica que figura en representación de una entidad pública o privada y tiene una duración máxima de un año.

#### **SEXTO.- REQUISITOS TÉCNICOS PARA ACCEDER AL SERVICIO**

Para obtener un certificado, el signatario tiene que cumplir los siguientes requisitos:

- a) Dispositivo que permita firmar un documento, donde será almacenado y custodiado el Certificado Digital. En función al tipo de información que utiliza una organización/entidad las claves públicas y privada podrán ser emitidas a:
  - Dispositivo que permita firmar un documento, donde sea almacenado el Certificado Digital y custodiado (*Token o tarjetas inteligentes -smartcards-*) que cumpla con el estándar FIPS 140-2.
  - Software, que cumpla con los requerimientos y niveles de seguridad establecidos en la RAR -DJ-RA TL LP 31/2015, donde sea almacenado el Certificado Digital que permita uno o varios documentos y que cumpla con los sistemas de seguridad reconocidos internacionalmente, garantizando la confiabilidad del mismo a sus usuarios o signatarios.
- b) Documento de solicitud de Certificación Digital y aceptación de términos y condiciones del servicio de certificación digital firmado, en caso de que el SIGNATARIO no fuera el USUARIO.

#### **SEPTIMO.- HABILITACIÓN Y PLAZO PARA LA PROVISIÓN DEL SERVICIO**

La ECA una vez que haya validado y verificado el cumplimiento de los requisitos y se haya registrado el comprobante de pago, procederá a emitir el certificado digital en un máximo de 24 horas.

#### **OCTAVO.- TARIFAS.-**

La estructura tarifaria deberá ser aprobada por la ATT del servicio de certificación digital y se encontrará publicada en el sitio web: <http://www.digicert.bo>.

#### **NOVENA.- OBLIGACIONES Y RESPONSABILIDADES DE LA ECA**

##### **9.1.- OBLIGACIONES DE LA ECA.-**

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**:

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

- h) Revocar el certificado digital al producirse alguna de las causales señaladas en los puntos anteriores;
- i) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación;
- j) Mantener la información relativa a los certificados digitales emitidos, por un período mínimo de cinco (5) años posteriores al periodo de su validez o vigencia;
- k) Facilitar información y prestar la colaboración debida al personal autorizado por la ATT, en el ejercicio de sus funciones, para efectos de control, seguimiento, supervisión y fiscalización del servicio de certificación digital, demostrando que los controles técnicos que emplea son adecuados y efectivos cuando así sea requerido;
- l) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia;
- m) Notificar a la ATT cualquier cambio en la personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos o correo electrónico;
- n) Verificar toda la información proporcionada por el signatario del servicio, bajo su exclusiva responsabilidad;
- o) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;
- p) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidos que administra.

## **9.2.-RESPONSABILIDADES DE LA ECA.-**

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 la emisión de certificados digitales 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.

## **DECIMA.- DERECHOS, OBLIGACIONES Y RESPONSABILIDADES DEL SIGNATARIO Y USUARIO.-**

### **10.1.- DERECHOS DEL SIGNATARIO Y USUARIO.-**

De acuerdo a lo establecido en el Art. 54 de la Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, **el signatario y usuario** tienen los siguientes derechos:

- a) Acceder en condiciones de igualdad, equidad, asequibilidad, calidad, de forma ininterrumpida a los servicios de certificación digital.
- b) Acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de certificación digital, a ser proporcionada por la ECA.
- c) Recibir la factura respectiva por el pago de los servicios de certificación digital.
- d) Exigir respeto a la privacidad e inviolabilidad de sus datos, salvo aquellos casos expresamente señalados por la Constitución Política del Estado y la Ley.
- e) Suscribir contratos de los servicios de certificación digital de acuerdo a los modelos de contratos, términos y condiciones, previamente aprobados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.
- f) Ser informado por la ECA oportunamente, cuando se produzca un cambio de las tarifas.
- g) Recibir el reintegro o devolución de montos que resulten a su favor.
- h) Obtener respuesta efectiva a las solicitudes realizadas a la ECA.
- i) Reclamar ante la ECA y acudir ante las autoridades competentes en aquellos casos que el usuario considere vulnerados sus derechos, mereciendo atención oportuna.
- j) A ser informado, antes de la suscripción del contrato para la emisión de certificados digitales, acerca del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, de las condiciones precisas para la utilización del certificado, de las limitaciones de uso, de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o los que se acordaren;
- k) Solicitar, revocar, renovar certificados digitales para los signatarios autorizados durante la vigencia del certificado.
- l) A que la ECA le proporcione la información sobre todos los medios a los que el signatario/usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del servicio contratado, o la forma en que presentará sus reclamos;

### **10.2.- OBLIGACIONES DEL SIGNATARIO Y USUARIO.-**

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** tienen 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 certificado digital y la generación de la firma digital;
- 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 certificado digital;
- 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.

### **10.3.- RESPONSABILIDAD DEL SIGNATARIO Y USUARIO.-**

- a) Por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como signatario.
- b) Los datos de creación de la firma digital vinculado a cada certificado digital de una persona jurídica, será responsabilidad del usuario, cuya identificación se incluirá en el certificado digital.
- c) El documento con firma digital le otorga a su signatario la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.
- d) Está bajo responsabilidad del signatario el uso de la clave privada, en caso de verse comprometida por cualquier razón dicha clave, el signatario deberá informar a la ECA a la brevedad posible y solicitar su revocatoria.

- e) Todos los efectos o daños que pudieran ocasionarse al signatario o a terceros, en el transcurso comprendido entre la generación de la firma y su revocatoria, son de exclusiva responsabilidad del signatario.

#### **DECIMO PRIMERA.- INFRACCIONES CONTRA LOS DERECHOS DE SIGNATARIO Y USUARIO DE CERTIFICADORAS DIGITALES**

##### **INFRACCIONES.-**

Constituyen infracciones contra el derecho de una SIGNATARIO/USUARIO de certificadoras digitales, sin perjuicio de la restauración que corresponda las siguientes:

- No mantener la confidencialidad de la información proporcionada por los titulares de los certificados digitales, salvo orden judicial o solicitud del titular del certificado digital.
- La copia y/o almacenamiento de la llave privada del usuario.
- Falta de consentimiento del titular de los datos personales, para el procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones de sus datos.
- No informar a los usuarios cuando se ha vulnerado y/o comprometido la seguridad de su información.
- Revocar el certificado digital sin justificación.
- No informar al usuario, previamente, sobre las condiciones de emisión, validación, renovación, baja, suspensión, tarifas y uso de sus certificados digitales.
- Negativa injustificada de la provisión del certificado digital.

Las sanciones serán expuestas de conformidad a la normativa legal vigente y aplicable.

#### **DECIMO SEGUNDA.- ATENCIÓN DE CONSULTAS, RECLAMACIONES Y EMERGENCIAS Y/O SERVICIOS DE INFORMACIÓN Y ASISTENCIA.-**

##### **12.1.- ATENCIÓN DE CONSULTAS Y EMERGENCIAS Y/O SERVICIOS DE INFORMACIÓN.-**

DIGICERT S.R.L atenderá las consultas referentes a los servicios que presta en la cuenta de correo electrónico soporte@digicert.bo, y sistema de consultas establecidos en el sitio web <http://www.digicert.bo>.

Las consultas serán atendidas de Lunes a Viernes, de 08:30 a 12:00 y de 14:30 a 19:00.

##### **12.2.- PROCEDIMIENTO DE RECLAMACIONES.-**

###### **12.2.1.- RECLAMACIÓN DIRECTA.-**

El SIGNATARIO Y/O USUARIO tiene el derecho de recibir por parte de la ECA o AR, a través de las Oficinas definidas para la otorgación del servicio, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación del servicio.

El SIGNATARIO/USUARIO o tercero por él debidamente acreditado, previa identificación, presentará su reclamación, en una primera instancia ante la ECA o AR.

En primera instancia, la Reclamación Directa será presentada en medio escrito, en un lapso no mayor a 30 días calendario contados después del día del hecho que motivo la reclamación.

La ECA o AR resolverá la Reclamación, en un lapso no mayor a 5 días hábiles contados desde el día siguiente de la presentación de su Reclamación. En caso de que la ECA o AR resuelva procedente su Reclamación, adoptará las medidas necesarias para evitarle perjuicios, en un plazo no mayor a 2 días hábiles contados después de la emisión de su pronunciamiento. En caso de que la ECA o AR resuelva improcedente su Reclamación o no la resuelva dentro el plazo de 5 días establecidos, usted podrá presentar una Reclamación Administrativa ante la ATT.

###### **12.2.2.- RECLAMACIÓN ADMINISTRATIVA.-**

El signatario y/o usuario presentará la Reclamación Administrativa de manera escrita, indistintamente en cualquier oficina de la ECA o AR o directamente en la oficina de la ATT, acreditando que con anterioridad realizó la reclamación directa o, en su defecto, expresando las razones por las que realiza su reclamación en esta instancia.

#### **DECIMO TERCERA.- INFRACCIONES CONTRA LAS ATRIBUCIONES DE LA AUTORIDAD REGULADORA DE ENTIDADES CERTIFICADORAS AUTORIZADAS.-**

##### **INFRACCIONES.-**

I. Constituyen infracciones contra las atribuciones de la Autoridad Reguladora, las siguientes relacionadas al servicio:

- Omisión de llevar un registro actualizado de los certificados expedidos.
- Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías, seguimiento, supervisión y fiscalización por parte de la ATT.
- No comunicar inmediatamente, por parte de las entidades certificadoras a la ATT, sobre alguna anomalía o incidente que pueda comprometer la confidencialidad de su clave privada.
- Incumplir con el pago de las obligaciones económicas de acuerdo a normativa vigente.
- La emisión de certificados sin el cumplimiento de las políticas de certificación comprometida y que causen perjuicio al usuario, signatario o tercero, o que incida gravemente la seguridad de los servicios de certificación.

II. Constituyen infracciones contra las atribuciones de la Autoridad Reguladora, las siguientes relacionadas a lo administrativo:

- La falta de notificación de cambio de personería jurídica a la ATT.
- No facilitar los datos requeridos a la ATT en ejercicio de sus funciones.
- No mantener la información relativa a los certificados digitales emitidos, por al menos (5) años posteriores al periodo de validez o vigencia.
- No publicar, mantener o actualizar, los procedimientos de certificación digital y su contenido en un sistema de información de acceso libre.

Las sanciones serán expuestas de conformidad a la normativa legal vigente y aplicable.

#### **DECIMO CUARTO.- CAMBIO O MODIFICACIONES EN LA LEY O REGLAMENTOS DE TELECOMUNICACIONES.-**

Los presentes Términos y Condiciones se encuentran enmarcados en la Ley General de Telecomunicaciones y sus Reglamentos vigentes. Cualquier modificación futura a estas disposiciones legales será de aplicación inmediata en lo concerniente a los Términos y Condiciones.