REGLAMENTO PARA EL DESARROLLO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
ASPECTOS GENERALES

Artículo 1.- (OBJETO). Reglamentar el acceso, uso y desarrollo de las Tecnologías de Información y Comunicación - TIC, en el marco del Título IV de la Ley No 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación.

Artículo 2. - (ÁMBITO DE APLICACIÓN). El presente reglamento se aplicará a personas naturales o jurídicas, públicas o privadas que realicen actividades o presten servicios relacionados con la certificación digital, gobierno electrónico, software libre, correo electrónico y el uso de documentos y firmas digitales en el Estado Plurinacional de Bolivia.

Artículo 3.- (DEFINICIONES). Además de las definiciones técnicas establecidas en la Ley No. 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, para el cumplimiento del presente Reglamento, se adoptan las siguientes definiciones:

I. Respecto al Desarrollo de Contenidos y Aplicaciones.

a) **Contenido digital.** Información digitalizada generada bajo cualquier modo o forma de expresión que puede ser distribuida por cualquier medio electrónico y es parte de un mensaje que el sistema de transferencia o soporte no examina ni modifica, salvo para conversión durante el transporte del mismo;

b) **Desarrollo de Contenido Digital.** Es la creatividad, diseño y producción de contenidos digitales para la obtención de productos y aplicaciones digitales con propósitos específicos;

c) **Aplicaciones digitales.** Programas de software modulares, específicos e interactivos de usuario o multiusuario, utilizados sobre plataformas de prestación de servicios digitales en general o equipos terminales destinados a comunicaciones personales, fines educativos, productivos o de entretenimiento, entre otros.

II. Respecto a software libre.

a) **Programa o software.** Cualquier secuencia de instrucciones finita usada por un dispositivo de procesamiento digital de datos para llevar a cabo una tarea específica o resolver un problema determinado, incluyendo todas las dependencias necesarias para su pleno funcionamiento;

b) **Código fuente o programa fuente.** Conjunto completo de instrucciones y archivos digitales originales, legible para el ser humano, tal y como fue escrito por el

programador, en un lenguaje de programación específico, más todos los archivos digitales de soporte, como tablas de datos, imágenes, especificaciones, documentación y todo otro elemento que sea necesario para producir el programa ejecutable a partir de ellos;

c) **Software libre.** Software licenciado por su autor, bajo una licencia de código fuente abierta, de manera tal que permita a sus usuarios el ejercicio de las siguientes libertades:

- Ejecutar el software, para cualquier propósito, sin restricción alguna.
- Estudiar cómo funciona el software y modificarlo para que cumpla un determinado propósito, a través del acceso al código fuente del mismo y todos los componentes que hacen posible su funcionamiento.
  El acceso al código fuente es una condición necesaria e imprescindible.
- Redistribuir copias del software.
- Distribuir copias de las versiones modificadas a terceros. El acceso al código fuente es una condición necesaria e imprescindible.

d) **Software propietario o Software Privativo.** Todo software que no cumple, parcial o totalmente, con cualquiera de las condiciones mencionadas para el software libre se considera, para los efectos del presente reglamento, software propietario;

e) **Estándar abierto.** Es una especificación técnica o protocolo normalizado:

- Cuyas especificaciones técnicas, completas y coherentes, están sujetas a una evaluación pública completa, se puede usar sin restricciones y está disponible por igual para todos los usuarios y/o partes, sin costo alguno para su uso.
- Que no necesita ningún componente o extensión adicional que tenga dependencias con formatos o protocolos que no cumplan la definición de Estándar Abierto.
- Que está libre de cláusulas legales o técnicas que limiten o restrinjan su utilización por cualquier usuario y/o parte o en cualquier modelo de negocio.
- Que es gestionado y puede ser desarrollado independientemente por cualquier organización en un proceso abierto a la participación equitativa e inclusiva de competidores, usuarios, especialistas del área de aplicación y terceras partes.
- Que esté disponible en al menos una implementación completa, cuya documentación y especificación técnica está disponible para todas las partes con grado de detalles suficientes para un desarrollo correcto y de calidad.

f) **Repositorio Estatal de Software Libre**. Es el sistema informático que contiene los sistemas y aplicaciones libres desarrollados por o para el Estado, de manera directa o a través de terceros.

III. Respecto a firmas y certificados digitales**.**

a) **Autenticación.** Proceso técnico de verificación por el cual se garantiza la identidad del firmante en un mensaje electrónico de datos o documento digital, que contengan firma 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;

e) **Infraestructura nacional de certificación digital.** Es el conjunto de normas, estándares tecnológicos, procedimientos, equipos, redes, bases de datos y programas informáticos y dispositivos de cifrado, preparados para la generación, almacenamiento y publicación del estado, la vigencia y validez de los certificados digitales reconocidos por las entidades certificadoras;

f) **Mensaje electrónico de datos.** Es toda información de texto, imagen, voz, video y datos codificados digitalmente, creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que pueden ser intercambiados por cualquier sistema de comunicación electrónico;

g) **Signatario.** Es el titular de una firma digital que utiliza la misma bajo su exclusivo control y el respaldo de un certificado digital proporcionado por entidades certificadoras autorizadas.

IV. Respecto al Tratamiento de los Datos Personales**.**

a) **Datos personales.** A los fines del presente Reglamento, se entiende como datos personales, a toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable;

b) **Autorización.** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada;

c) **Tratamiento de los datos personales.** Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

V. Respecto a correo electrónico**.**

a) **Correo Electrónico Comercial.** Todo mensaje, archivo, dato u otra información electrónica, enviada por cualquier medio electrónico con el fin de difundir, ofertar y publicitar bienes o servicios;

b) **Correo Electrónico no deseado.** Todo mensaje, archivo, dato u otra información enviada periódicamente, por cualquier medio electrónico dirigido a un receptor con quien el emisor no tiene relación alguna y es enviado sin su consentimiento.

VI. Respecto a la Seguridad Informática**.**

a) **Seguridad Informática.** Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante;

b) **Seguridad de la información.** La Seguridad de la Información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad;

c) **Plan de Contingencia.** Es un instrumento que comprende métodos y el conjunto de acciones para el buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.

VII. Respecto a la Soberanía.

a) **Dependencia tecnológica.** Es la condición a que someten a los usuarios, sean estos personas, naturales o jurídicas, Estados o naciones, las compañías, empresas, naciones o Estados que desarrollan, distribuyen o venden tecnología, al negar el acceso al conocimiento de los contenidos, procedimientos, técnicas y procesos necesarios para el uso, desarrollo y distribución de las mismas, a través de licencias, patentes, restricciones prácticas, restricciones legales y otros; de modo que los usuarios vean restringida la posibilidad de controlar, auditar, usar, modificar o desarrollar dicha tecnología;

b) **Soberanía tecnológica.** Es la posesión del control por parte de una nación y/o Estado sobre la tecnología que utiliza. Se caracteriza por el acceso al conocimiento sobre el contenido y los procedimientos, procesos y técnicas necesarios para el desarrollo y uso de dicha tecnología, el mismo que le permite auditar, mejorar, desarrollar, modificar y ajustar a sus necesidades específicas la misma, sin la intervención ni autorización específica de terceros; de modo que se garantice la total independencia en cuanto al control de la tecnología utilizada por dicha nación o Estado con respecto a compañías, empresas, personas, naciones o Estados;

c) **Descolonización del conocimiento tecnológico e informacional.** Es el proceso social y científico que permite romper los lazos de dependencia tecnológica e informacional de una nación y/o Estado con respecto a terceras personas, empresas, naciones o Estados y desarrollar conocimiento y tecnología propia, acorde a sus necesidades, retos y características, partiendo del diálogo entre los conocimientos locales y universales disponibles. Es un proceso de intercambio cultural, de conocimientos y tecnologías, con otras sociedades, naciones y/o Estados dispuestos a compartir sus propios desarrollos e interiorizar los externos, respetando el derecho de los otros a conocer los contenidos y los procedimientos, procesos y técnicas necesarios para el desarrollo y uso de las tecnologías en general y de las tecnologías de la información y la comunicación en particular. La

descolonización del conocimiento tecnológico e informacional está directamente relacionada con el desarrollo de capacidades científicas e institucionales para garantizar el manejo y aprovechamiento soberano de los recursos naturales y el desarrollo económico del Estado Plurinacional en la construcción del vivir bien.

VIII. Respecto a comercio electrónico

a) **Mensaje de datos.** La información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

b) **Intercambio electrónico de datos**. La transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) **Iniciador de un mensaje de datos.** Toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, exceptuando aquel que actué a título de intermediario;

d) **Destinatario de un mensaje de datos.** La persona designada por el iniciador para recibir el mensaje, exceptuando aquel que actué a título de intermediario;

e) **Intermediario.** Toda persona que actuando por cuenta de otra, envíe, reciba o archive un mensaje de datos o preste algún otro servicio con respecto a él;

f) **Sistema de información.** Todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 4.- (PRINCIPIOS). I. Documentos digitales. Los documentos y mensajes electrónicos ambos con firma digital se regirán por los siguientes principios:

a) **Autenticidad.** La información del documento digital y su firma digital se corresponden con la persona que ha firmado. Esta es una característica intrínseca de la firma digital, en donde el autor del mensaje queda acreditado, puesto que permite verificar la identidad del emisor de un documento digital;

b) **Integridad.** Característica única del mensaje electrónico de datos o documento digital ambos con firma digital, que indica que los mismos no han sido alterados en el proceso de transmisión desde su creación por parte del emisor hasta la recepción por el destinatario;

c) **No repudio.** Es la garantía de que un mensaje electrónico de datos o un documento digital ambos firmados digitalmente, no puedan ser negados en su autoría y contenido.

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

a) **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;

b) **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;

c) **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;

d) **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;

e) **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.

III. Contenidos digitales. Los contenidos digitales se rigen con los siguientes principios:

a) **Prácticos.** Proveer de información práctica y realista;

b) **Accesibles.** Disponibilidad e intercambio de información en todo momento;

c) **Contextualizados.** Deben ser acordes a la circunstancia socio-económica, cultural y lingüística de los usuarios;

d) **Legibles.** Su escritura debe ser concisa, sin ambigüedades, redundancias ni imprecisiones;

e) **Ejemplificativos.** Deben contener situaciones paradigmáticas, tener ejemplos, casos de estudio y escenarios auténticos y relevantes.

IV. Software. El Software a ser utilizado por las entidades públicas debe regirse por los siguientes principios:

a) **Soberanía Tecnológica.** Debe permitir al Estado Plurinacional ejercer pleno control sobre las aplicaciones informáticas o software que utiliza, asegurando la independencia tecnológica del país y la seguridad informática del Estado Plurinacional;

b) **Seguridad Informática del código fuente.** Debe permitir al Estado Plurinacional la

posibilidad de auditar, conocer y modificar el código fuente del mismo sin requerir ningún tipo de autorización, para obtener el comportamiento deseado de parte de ellas y ningún otro no consentido o requerido, precautelando la seguridad, independencia y soberanía tecnológica de Bolivia;

c) **Descolonización del Conocimiento Tecnológico.** Debe permitir al Estado Plurinacional romper los lazos de dependencia tecnológica e informacional con respecto a terceros, garantizando la soberanía tecnológica y seguridad informática; y avanzar en el proceso de desarrollo de capacidades científicas e institucionales que permitan el desarrollo de la economía nacional en la construcción del vivir bien.

CAPÍTULO II
DESARROLLO DE CONTENIDOS Y APLICACIONES

Artículo 5.- (DESARROLLO DE CONTENIDOS Y APLICACIONES TIC). I. El Estado promoverá de manera prioritaria el desarrollo de contenidos y aplicaciones y servicios de las TIC en software libre, utilizando estándares abiertos y velando por la seguridad de la información en las siguientes áreas:

a) En educación, a través de plataformas virtuales de aprendizaje, capacitación e investigación y servicios en todos los niveles educativos y académicos;

b) En salud, a través de plataformas virtuales de información, atención y servicios a la población que asiste a los diferentes centros de salud, velando por la credibilidad de los datos que utilice el sector y promoviendo la asistencia médica a distancia;

c) En la gestión gubernamental, a través de la implementación del gobierno electrónico promoviendo la transparencia y la capacitación de los recursos humanos para garantizar la eficiencia de los sistemas implantados;

d) En lo productivo, a través de plataformas virtuales de información, comercialización y otros servicios, promoviendo entre otros la construcción de comunidades virtuales productivas como motores de desarrollo de las TIC para la industria en el país;

e) En comunicación e Información, a través de plataformas virtuales, promoviendo la creación de espacios de socialización, sensibilización y evaluación de las TIC en el Estado Plurinacional.

II. El desarrollo de contenidos debe considerar los siguientes aspectos:

a) Desarrollo de contenidos accesibles y de fácil manejo por parte de la población y el uso de términos de compresión amplia y de uso común;

b) El uso del castellano, y otros idiomas oficiales reconocidos en la Constitución Política del Estado, a fin de contribuir a la preservación y divulgación de los diferentes idiomas existentes en el Estado Plurinacional;

c) Contenidos de índole social y culturalmente adecuados en relación a los valores y principios relacionados con la construcción del Estado Plurinacional, la descolonización, despatriarcalización y el vivir bien;

d) La generación y uso de contenidos educativos y culturales adecuados a la realidad local;

e) La articulación de las oportunidades de la convergencia tecnológica en función a medios tradicionales y nuevos de TIC para la generación y difusión de contenidos.

Artículo 6.- (OBJETIVOS DEL DESARROLLO DE CONTENIDOS DIGITALES). El desarrollo, diseño e innovación de contenidos digitales tendrán mínimamente los siguientes objetivos:

a) Dar soporte a las TIC en la atención prioritaria a demandas en las áreas de educación, salud, gestión gubernamental, en lo productivo y de comunicación e información;

b) Aprovechar el conjunto de recursos de las TIC y de la convergencia tecnológica en la formación de la sociedad de los saberes y la información;

c) Formar y capacitar en contenidos digitales y su utilización en la red internet o en plataformas de gestión de Tecnologías de Información – TI;

d) Promover la identidad cultural de los pueblos originarios, sus territorios ancestrales, usos y costumbres; para el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades y fomentar el respeto mutuo y el diálogo intracultural, intercultural y plurilingüe;

e) Contribuir a la generación de contenidos accesibles y de fácil manejo por parte de la población en el uso de términos de comprensión amplia de uso común, utilizando en lo posible los idiomas oficiales reconocidos en la Constitución Política del Estado a fin de contribuir a su preservación y divulgación;

f) Incluir contenidos social y culturalmente adecuados en relación a los valores y principios enmarcados en la construcción del Estado Plurinacional, la descolonización, despatriarcalización y el vivir bien, promoviendo la soberanía nacional en la generación, difusión y replicación de contenidos nacionales y locales;

g) Promover estudios de investigación, identificación y análisis de la oferta y la demanda sobre contenidos digitales con los agentes del sector;

h) Favorecer la creación de empresas y de modelos de negocios, que coadyuven al desarrollo económico de Bolivia, enmarcados en la economía plural definida por la Constitución Política del Estado;

i) Coadyuvar a un mayor tránsito del tráfico digital nacional en las comunicaciones de datos, en los servicios de comunicaciones de voz, internet, utilización de contenidos y aplicaciones y servicios digitales de valor agregado;

j) Promover el derecho a la privacidad de la información de los usuarios;

k) Profundizar el proceso de descolonización del conocimiento;

l) Avanzar hacia la soberanía tecnológica del Estado Plurinacional de Bolivia;

m) Fortalecer la seguridad informática del Estado Plurinacional de Bolivia.

Artículo 7.- (DESARROLLO DE APLICACIONES DIGITALES). El desarrollo de aplicaciones digitales por parte de las entidades públicas priorizará el uso de herramientas y plataformas de software libre, las cuales deben permitir a los usuarios y las usuarias: comunicarse entre sí, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse, activar servicios en las redes públicas de comunicaciones y realizar una serie de tareas de manera práctica y desde uno o más tipos de equipos terminales, proceso para el cual se enmarcarán en el uso de Estándares Abiertos, de modo que los contenidos sean democratizados y accesibles para los usuarios.

Artículo 8.- (PLAN DE CONTINGENCIA). Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad.

TÍTULO II
COMITÉ PLURINACIONAL Y CONSEJO SECTORIAL

CAPITULO I
COMITÉ PLURINACIONAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – COPLUTIC

Artículo 9.- (CONFORMACIÓN). I. El COPLUTIC estará conformado por:

a) Un (1) representante del Ministerio de Obras Públicas, Servicios y Vivienda que lo preside;

b) Un (1) representante del Ministerio de Planificación del Desarrollo;

c) Un (1) representante del Ministerio de Comunicación;

d) Un (1) representante del Ministerio de Educación;

e) Un (1) representante de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB.

II. Los representantes deberán tener un rango mínimo de Director, ser designados por su Máxima Autoridad Ejecutiva mediante el instrumento legal correspondiente y no percibirán remuneración o dieta alguna por el ejercicio de las funciones propias del Comité.

III. En el marco del derecho a la participación y control social establecido en el artículo

30 de la Constitución Política del Estado y la Ley N° 341 de Participación y Control Social el COPLUTIC convocará periódicamente a organizaciones de la sociedad civil.

IV. El COPLUTIC se enmarca en los conceptos y principios de la descolonización del conocimiento, la seguridad informática, la soberanía tecnológica del Estado Plurinacional y el uso de software libre y estándares abiertos.

Artículo 10.- (FUNCIONES DEL COPLUTIC). I. Son funciones del Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC las siguientes:

a) Proponer al Órgano Ejecutivo del nivel central planes nacionales de desarrollo que permitan garantizar el acceso universal de todas las bolivianas y bolivianos a las tecnologías de información y comunicación, con el fin de fomentar su uso, apoyando al crecimiento del desarrollo nacional y aumento de la productividad y competitividad del país;

b) Coordinar los proyectos y líneas de acción entre todos los actores involucrados, respecto a la penetración, uso y comportamiento de las tecnologías de información y comunicación;

c) Proponer programas de capacitación, sensibilización y socialización en el uso y aprovechamiento de las TIC;

d) Definir los mecanismos de ejecución y seguimiento a los resultados, para el buen cumplimiento y beneficio de las tecnologías de información y comunicación y acceso al conocimiento en el entorno socioeconómico del Estado Plurinacional;

e) Proponer líneas de acción para la seguridad informática;

f) Generar políticas conducentes a alcanzar la soberanía tecnológica, seguridad informática y descolonización del conocimiento en el área de las TIC;

g) Promover la producción de contenidos nacionales, acorde a las necesidades de la sociedad boliviana y las organizaciones, naciones y pueblos indígena originario campesinos reconocidos en la Constitución Política del Estado;

h) Promover la adaptación y apropiación por parte de la sociedad boliviana de las tecnologías, saberes y conocimientos relacionados a las TIC;

i) Promover la dotación a las organizaciones sociales, naciones y pueblos indígena originario campesinas de herramientas TIC que les permitan conformarse en comunidades y redes de intercambio cultural y de conocimiento para el desarrollo y despliegue tecnológico de las culturas reconocidas por la Constitución Política del Estado;

j) Promover un paradigma cultural y tecnológico alternativo al capitalista, sustentado en los principios y valores comunitarios, de intercambio cultural y de conocimientos para el desarrollo de los pueblos;

k) Proponer normas adecuadas para la protección y defensa de los usuarios de medios, mensajes y recursos informáticos;

l) Las propuestas sectoriales del COPLUTIC deberán ser puestas a consideración de las entidades que lo conforman, para la aprobación por el o los ministerios competentes.

Artículo 11.- (PARTICIPACIÓN). I. Los miembros del COPLUTIC cuando lo determinen podrán requerir la participación de instituciones o entidades públicas o privadas, dependiendo del tema específico a tratarse.

II. El COPLUTIC podrá contar, cuando así lo requiera con la participación de otros expertos, los mismos que brindarán asesoramiento técnico especializado respecto a los temas tratados con carácter de recomendación.

Artículo 12.- (REUNIONES DEL COPLUTIC). I. Las reuniones serán convocadas por el Presidente del Comité y se llevarán a cabo en sus instalaciones o en cualquier otro lugar que se establezca con carácter previo.

II. Las reuniones podrán ser ordinarias o extraordinarias. Las ordinarias se celebrarán de forma trimestral y las extraordinarias cuantas veces se estimen necesarias.

III. Las reuniones se llevarán a cabo cuando asistan por lo menos tres (3) de sus miembros, la decisión se tomará por mayoría simple, en caso de empate, el miembro que preside tendrá voto decisivo.

IV. El Presidente del Comité designará al Secretario de Actas.

CAPITULO II
CONSEJO SECTORIAL DE TELECOMUNICACIONES Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – COSTETIC

Artículo 13.- (CONFORMACIÓN). I. El COSTETIC estará conformado por:

a) Un (1) representante o autoridad competente del sector de cada asociación departamental de municipios;

b) Un (1) representante del Ministerio de Planificación del Desarrollo;

c) Un (1) representante del Ministerio de Economía y Finanzas Públicas;

d) Un (1) representante del Ministerio de Comunicación;

e) Un (1) representante del Viceministerio de Telecomunicaciones;

f) Un (1) representante de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT en calidad de asesor técnico, con derecho a voz y no a voto.

II. En el marco del derecho a la participación y control social establecido en el artículo 30 de la Constitución Política del Estado y la Ley Nº 341 de Participación y Control Social el COSTETIC convocará periódicamente a organizaciones de la sociedad civil.

III. El COSTETIC se enmarca en los conceptos y principios de la descolonización del conocimiento, la seguridad informática, la soberanía tecnológica del Estado Plurinacional y el uso de estándares abiertos.

Artículo 14.- (FUNCIONES DEL COSTETIC). El COSTETIC, en el marco del Artículo 74 de la Ley No 164, General de Telecomunicaciones, Tecnologías de Información y Comunicación, tiene como funciones principales las siguientes:

a) Proponer y coordinar mecanismos necesarios para fomentar el acceso, uso y apropiación social de las tecnologías de información y comunicación;

b) Coordinar y concertar el despliegue y uso de la infraestructura tecnológica;

c) Proponer y concertar servicios y aplicaciones de las tecnologías de información y comunicación en las áreas de educación, salud, gestión gubernamental, en lo productivo, comunicación e información en sus respectivos niveles de gobierno.

Artículo 15.- (REUNIONES). I. Las reuniones del COSTETIC serán convocadas por el Presidente del Consejo a iniciativa de este o a petición de uno de sus miembros.

II. En función a la necesidad de coordinación de asuntos y proyectos sectoriales y su incumbencia territorial, se convocará a los representantes o autoridades designadas por los gobiernos autónomos u organizaciones sociales para su participación en las reuniones.

III. El Presidente del COSTETIC designará al Secretario de Actas.

TÍTULO III
GOBIERNO ELECTRÓNICO Y SOFTWARE LIBRE

CAPÍTULO I
GOBIERNO ELECTRÓNICO

Artículo 16.- (PLAN DE IMPLEMENTACION DEL GOBIERNO ELECTRÓNICO). I. El Ministerio de Planificación del Desarrollo, en coordinación con el Ministerio de Obras Públicas, Servicios y Vivienda a través del Viceministerio de Telecomunicaciones, y la ADSIB, es la instancia responsable de elaborar, promover, gestionar y articular el Plan de Implementación del Gobierno Electrónico en el Estado Plurinacional de Bolivia, así como su permanente actualización.

II. La ejecución del Plan de Implementación del Gobierno Electrónico, estará a cargo de las entidades públicas del Estado.

III. El seguimiento a la ejecución del Plan de Implementación del Gobierno Electrónico estará a cargo de la ADSIB en coordinación con cada entidad de la administración

pública del Estado.

Artículo 17.- (OBJETIVO DEL GOBIERNO ELECTRÓNICO). I. Modernizar y transparentar la gestión pública, otorgando servicios y atención de calidad a la ciudadanía, garantizando el derecho a la información, así como contribuir a la eficiencia y eficacia de los actos administrativos en los procesos internos del Gobierno, mediante el uso de las tecnologías de información y comunicación y otras herramientas.

II. Generar mecanismos tecnológicos de participación y control social, mediante el uso de TIC por parte de los ciudadanos, organizaciones sociales y pueblos y naciones indígena originario campesinas.

Artículo 18.- (LINEAMIENTOS DEL PLAN DE IMPLEMENTACIÓN). El Plan de Implementación del Gobierno Electrónico deberá considerar mínimamente los siguientes lineamientos:

a) Posibilitar a la población en general el derecho a acceder, participar y relacionarse de manera eficiente y transparente con las entidades públicas por medios electrónicos, asegurando credibilidad y confianza en el gobierno en línea;

b) Fortalecer la protección de la información, contenidos y aplicaciones digitales de la población en general, que acceda a la prestación de los servicios en línea;

c) Establecer las condiciones tecnológicas adecuadas para que la población en general pueda acceder y comunicarse con las entidades públicas y hacer uso de los servicios proporcionados por las mismas, en condiciones de igualdad, indistintamente del hardware o software utilizado, la infraestructura de red, el idioma y la localización geográfica;

d) Proponer mecanismos para lograr eficiencia en el uso de los recursos tecnológicos de las entidades públicas, además de la interoperabilidad de los sistemas de información y de servicios gubernamentales desarrollados por cada una de ellas, a través de la aplicación y uso de estándares abiertos;

e) Promover mecanismos de colaboración para generar la integración entre las diferentes entidades públicas que posibiliten ampliar y mejorar el desarrollo conjunto de soluciones y servicios de gobierno en línea, permitiendo una gestión efectiva y de vocación de servicio al público;

f) Promover la capacitación y formación de los recursos humanos de manera de contribuir al uso y aprovechamiento de los diferentes sistemas y aplicaciones de gobierno electrónico a fin de lograr su eficiencia;

g) Promover el acceso a la información pública a través de sistemas informáticos que permitan a la ciudadanía, organizaciones sociales y pueblos y naciones indígena originario campesinas ejercer los derechos a la participación y control social establecidos en la Constitución Política del Estado y la Ley de Participación y Control Social N° 341;

h) Fortalecer los mecanismos de participación de la ciudadanía, organizaciones sociales y pueblos y naciones indígena originario campesinas en la elaboración de las políticas públicas, mediante el uso de TIC.

CAPITULO II
SOFTWARE LIBRE Y ESTANDARES ABIERTOS

Artículo 19.- (PLAN DE IMPLEMENTACIÓN DE SOFTWARE LIBRE Y ESTANDARES ABIERTOS). I. El Ministerio de Planificación del Desarrollo en coordinación con el Ministerio de Obras Públicas, Servicios y Vivienda, a través del Viceministerio de Telecomunicaciones y la ADSIB, es la instancia responsable de elaborar, promover, gestionar y articular el Plan de Implementación de Software Libre y Estándares Abiertos para los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles del Estado Plurinacional de Bolivia, así como de su permanente actualización.

II. El Plan de Implementación de Software Libre y Estándares Abiertos establecerá los mecanismos para el desarrollo comunitario de aplicaciones de Software Libre, transversales a las necesidades del Estado Plurinacional.

III. La ejecución del Plan de Implementación de Software Libre y Estándares Abiertos, estará a cargo de las entidades públicas.

IV. El seguimiento a la ejecución del Plan de Implementación de Software Libre y Estándares Abiertos estará a cargo de la ADSIB en coordinación con cada entidad de la administración pública del Estado

Artículo 20.- (OBJETIVO DEL PLAN). Establecer las condiciones y mecanismos para la implementación, uso, estudio, auditoria, investigación y desarrollo de software libre y estándares abiertos en las entidades públicas.

Artículo 21.- (LINEAMIENTOS DEL PLAN). El Plan de Implementación de Software Libre y Estándares Abiertos, debe considerar mínimamente los siguientes lineamientos:

a) Posibilitar la implementación, uso y desarrollo de Software Libre y Estándares Abiertos en las plataformas informáticas, aplicaciones, ordenadores, redes informáticas, intercambio de datos y publicación de contenidos digitales de los Órganos del Estado Plurinacional;

b) Promover el avance del proceso de descolonización del conocimiento;

c) Promover la formación, especialización y capacitación de recursos humanos en software libre y estándares abiertos en coordinación con los órganos del Estado y entidades de la administración pública;

d) Promover mecanismos de cooperación internacional en materia de software libre y estándares abiertos, en respeto de la soberanía y seguridad informática del Estado Plurinacional;

e) Establecer los mecanismos de seguimiento y control que garanticen la aplicación del presente reglamento y el Plan de Implementación de Software Libre y Estándares Abiertos;

f) Promover el desarrollo de software libre en los sectores público y privado, favoreciendo a los profesionales y empresas bolivianas;

g) Establecer las condiciones y jerarquización para fortalecer las unidades de sistemas de las entidades públicas, de modo que puedan cumplir con los objetivos del reglamento.

Artículo 22.- (REPOSITORIO ESTATAL DE SOFTWARE LIBRE). I. Será utilizado para promover y compartir el software desarrollado por o para el Estado permitiendo la optimización y reutilización de recursos.

II. La ADSIB es la entidad que administra el Repositorio Estatal de Software Libre para el registro, preservación y custodia. Debe publicar en línea la información de todos los sistemas y las aplicaciones que se encuentren en el Repositorio.

III. Las normas técnicas, estándares de desarrollo y licenciamiento de software libre para el registro en el repositorio y uso por parte del Estado, serán establecidos por la ADSIB.

IV. La ADSIB establecerá los mecanismos y procesos de registro consulta y uso del Repositorio Estatal de Software Libre.

V. Las entidades públicas tienen la obligación de registrar los sistemas y las aplicaciones libres usadas y desarrolladas, de manera directa o a través de terceros, en el Repositorio Estatal de Software Libre, conforme a procedimientos establecidos por la ADSIB, con excepción de aquellas consideradas estratégicas por cada institución.

Artículo 23.- (LICENCIAS DE SOFTWARE PRIVATIVO). I. En caso de adquisición o donación, ampliación y/o renovación de Licencias de Software Propietario por parte de las entidades públicas del Estado Plurinacional, la Máxima Autoridad Ejecutiva solicitará la conformidad a la ADSIB acompañada del informe técnico que justifique el uso de dicho software. En el caso de que el software sea utilizado por varias instituciones, será suficiente la solicitud presentada por el coordinador del proyecto.

II. En caso de desarrollo de aplicaciones en plataforma de Software Propietario por parte de las entidades públicas del Estado Plurinacional, la Máxima Autoridad Ejecutiva solicitará la conformidad a la ADSIB acompañada del respectivo informe técnico que justifique el desarrollo de dicho software bajo esa plataforma.

III. Para lo establecido en los Parágrafos I y II, la ADSIB hará conocer su conformidad u oposición, mediante documento de su Máxima Autoridad Ejecutiva, acompañado del respectivo informe técnico, estableciendo las recomendaciones necesarias. La decisión final en estos casos, será asumida por la Máxima Autoridad Ejecutiva de cada entidad.

IV. Toda adquisición de hardware por parte de las entidades públicas del Estado

Plurinacional deberá exigir la compatibilidad del mismo con sistemas de software libre.

V. En caso de que un hardware periférico indispensable requiera de un software insustituible para su funcionamiento, no se aplica lo establecido en el Parágrafo I del presente Artículo para dicho software.

TÍTULO IV
CERTIFICADO Y FIRMA DIGITAL Y ENTIDADES CERTIFICADORAS

CAPÍTULO I
CERTIFICADO Y FIRMA DIGITAL

Artículo 24.- (CERTIFICADO DIGITAL). Los certificados digitales deben ser emitidos por una entidad certificadora autorizada, responder a formatos y estándares reconocidos internacionalmente y fijados por la ATT, contener como mínimo los datos que permitan identificar a su titular, a la entidad certificadora que lo emitió, su periodo de vigencia y contemplar la información necesaria para la verificación de la firma digital.

Artículo 25.- (TIPOS DE CERTIFICADOS). La ATT establecerá mediante Resolución Administrativa, los tipos de certificados digitales que podrán emitir las entidades certificadoras autorizadas, de acuerdo a su uso y conforme a estándares y recomendaciones internacionales aplicables que promuevan la interoperabilidad con otros sistemas.

Artículo 26.- (FUNCIÓN DEL CERTIFICADO DIGITAL). El certificado digital cumple las siguientes funciones:

a) Acredita la identidad del titular de la firma digital;

b) Legitima la autoría de la firma digital que certifica;

c) Vincula un documento digital o mensaje electrónico de datos, con la firma digital y la persona;

d) Garantiza la integridad del documento digital o mensaje electrónico con firma digital.

Artículo 27.- (CARACTERÍSTICAS DEL CERTIFICADO DIGITAL). I. Los Certificados Digitales, deben contener mínimamente las siguientes características:

a) La emisión debe ser realizada por una entidad de certificación autorizada;

b) Contener el número único de serie que identifica el certificado;

c) Responder a formatos estándares reconocidos internacionalmente;

d) Periodo de validez;

e) Ser susceptibles de verificación respecto de su estado de revocación;

f) Acreditar, en los supuestos de representación, las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente;

g) Contemplar la información necesaria para la verificación de la firma;

h) Identificar la política de certificación bajo la cual fue emitido;

i) Contemplar los límites de uso del certificado, si se prevén;

j) Validar la correspondencia jurídica entre el Certificado Digital, la firma digital y la persona;

k) Identificar inequívocamente a su titular y al certificador autorizado que lo emitió.

II. La ATT, mediante Resolución Administrativa establecerá el formato y estructura de los certificados digitales tanto para personas naturales como para personas jurídicas.

Artículo 28.- (OBTENCIÓN DEL CERTIFICADO DIGITAL). I. Para la obtención del certificado digital, las entidades certificadoras deberán suscribir convenio de partes o contratos de prestación de servicios con los usuarios, de acuerdo con los términos y condiciones de esta prestación, previamente aprobados por la ATT.

II. Los requisitos mínimos para la obtención del Certificado Digital serán establecidos por la ATT mediante Resolución Administrativa, de acuerdo al tipo de Certificado.

Artículo 29.- (VIGENCIA DE LOS CERTIFICADOS PARA CARGOS PÚBLICOS). La vigencia de los certificados de firma digital emitidos con relación al ejercicio de cargos públicos no será superior a los dos (2) años y no deberá exceder el tiempo de duración de dicho cargo público a menos que exista prórrogas de funciones en las instituciones, debiendo todo cambio en el cargo, ser comunicado a la entidad certificadora pública inmediatamente.

Artículo 30.- (SUSPENSIÓN DE LA VIGENCIA). I. La vigencia de un certificado digital será suspendida por la entidad certificadora, cuando se verifique alguna de las siguientes circunstancias:

a) A solicitud del titular del certificado, debidamente comunicada a la entidad certificadora;

b) Decisión de la entidad certificadora en virtud de razones técnicas, previa comunicación a los signatarios;

c) Por orden o decisión judicial debidamente fundamentada que determine la suspensión provisional de la vigencia del certificado digital.

II. 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.

III. La suspensión de la vigencia del certificado digital será levantada por cualquiera de las siguientes causas:

a) A requerimiento del titular del certificado digital, cuando la suspensión haya sido solicitada por éste;

b) Cesación de las causas técnicas que motivaron la suspensión a criterio de la entidad certificadora;

c) Por orden o decisión judicial debidamente fundamentada que determine el cese de la suspensión de la vigencia del certificado digital.

IV. En las situaciones descritas en el parágrafo anterior, la entidad certificadora tiene la obligación de habilitar de inmediato el certificado digital de que se trate.

V. La suspensión de un certificado digital, no producirá, por si sola, la invalidez jurídica de los actos que al amparo de dicho certificado se hayan realizado con anterioridad.

Artículo 31.- (REVOCACIÓN DE UN CERTIFICADO DIGITAL). I. Un certificado digital será revocado por la entidad certificadora en los siguientes casos:

a) A solicitud de su titular, debidamente comunicada a la entidad certificadora;

b) Por fallecimiento del titular del certificado;

c) Por disolución o quiebra de la persona jurídica titular del certificado digital, a partir de la comunicación oficial recibida por la entidad certificadora;

d) Sentencia condenatoria ejecutoriada en contra del titular del certificado digital, por la comisión de delitos en los que se haya utilizado como instrumento la firma digital;

e) Sentencia judicial que declare la ausencia o interdicción del titular del certificado digital;

f) Por requerimiento de autoridad competente conforme a Ley;

g) 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 autorizada;

h) 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;

i) Por incumplimiento de las causas pactadas entre la entidad certificadora con el titular del certificado digital.

II. La revocación del certificado digital no exime a su titular del cumplimiento de las obligaciones contraídas durante la vigencia del certificado.

Artículo 32.- (CONSERVACIÓN). 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, siempre y cuando se garantice 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.

IV. La ATT mediante Resolución Administrativa determinará el procedimiento y las condiciones que deberán cumplir las entidades certificadoras para la conservación de los documentos físicos y digitalizados, asegurando el almacenamiento de los mismos en servidores ubicados en el territorio y bajo la legislación del Estado Plurinacional de Bolivia.

Artículo 33.- (CARACTERÍSTICAS DE LA FIRMA DIGITAL). Debe cumplir mínimamente las siguientes condiciones:

a) Estar vinculada a un certificado digital de manera que cualquier alteración subsiguiente en el mismo sea detectable;

b) Haber sido creada durante el periodo de vigencia del certificado digital válido del firmante;

c) Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable;

d) Ser creada por medios que el firmante pueda mantener bajo su exclusivo control y la firma sea controlada por la persona a quien pertenece;

e) Contener información vinculada exclusivamente a su titular;

f) Permitir verificar unívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación;

g) Que el método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual fue generado un registro de creación de la firma;

h) Que los datos sean susceptibles de verificación por terceros;

i) Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del signatario;

j) Que la firma digital sea controlada por la persona a quien pertenece.

Artículo 34.- (VALIDEZ DE LA FIRMA DIGITAL). I. Cuando una Firma Digital ha sido inscrita en un documento digital o mensaje electrónico de datos, se presume la voluntad del titular de la firma digital para acreditar ese documento digital o mensaje electrónico de datos, y se adscribe y vincula con el contenido de la información de los mismos.

II. Los mensajes electrónicos de datos o documentos digitales ambos con firma digital adquieren plena validez jurídica probatoria bajo las siguientes condiciones:

a) Ser individual y estar vinculada exclusivamente a su titular;

b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante procedimientos de autenticación y de seguridad y esté conforme a la normativa vigente;

c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;

d) Que al momento de creación de la firma digital, los datos con los que se creare se hallen bajo control exclusivo del signatario;

e) Que la firma sea controlada por la persona a quien pertenece.

III. Una firma digital pierde validez cuando la vigencia del certificado digital ha expirado o éste haya sido revocado.

Artículo 35.- (USO DE LA FIRMA DIGITAL EN EL SISTEMA DE PAGOS NACIONAL).
Para el uso y aceptación de la firma digital en el sistema de pagos nacional, las instancias competentes podrán establecer las condiciones para otorgar seguridad a las transferencias electrónicas en el sistema financiero. Todos los participantes del sistema de pagos nacional para poder efectuar operaciones, además de observar lo establecido en el presente Reglamento, deberán cumplir la regulación establecida por estas instancias.

CAPITULO II
INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN DIGITAL

Artículo 36.- (JERARQUÍA NACIONAL DE CERTIFICACIÓN DIGITAL). Establece los

niveles de la Infraestructura Nacional de Certificación Digital, donde existe una entidad certificadora de nivel superior encargada de regular y fiscalizar los procesos de certificación.

Artículo 37.- (ESTRUCTURA JERÁRQUICA). La organización de la Infraestructura Nacional de Certificación Digital, tiene los siguientes niveles:

1. Primer nivel: 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 pública y privadas subordinadas.

2. Segundo nivel: Entidades Certificadoras. Son las entidades certificadoras pública o privadas subordinadas de la Entidad Certificadora Raíz. La entidad certificadora pública es la ADSIB y las entidades certificadoras privadas, son todas aquellas autorizadas por ATT a prestar Servicios de Certificación, cumpliendo los requisitos exigidos para la autorización de prestación del servicio.

3. Tercer nivel: Agencia de Registro. Es la agencia dependiente de una entidad certificadora, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además es quién se encarga de solicitar la aprobación o revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital.

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

Artículo 38.- (FUNCIONES DE LA AUTORIDAD). Para el cumplimiento de las atribuciones establecidas en la Ley Nº 164, General de Telecomunicaciones, Tecnologías de Información y Comunicación, la ATT tendrá las siguientes funciones:

a) Autorizar la operación de entidades de certificación;

b) Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad;

c) Definir los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación;

d) Evaluar las actividades desarrolladas por las entidades de certificación de acuerdo a los estándares definidos en los reglamentos técnicos;

e) Revocar o suspender la autorización para operar como entidad de certificación;

f) Requerir en cualquier momento a las entidades de certificación información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren;

g) Verificar la calidad de prestación del servicio público de certificación y firma digital;

h) Imponer sanciones a las entidades de certificación por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio;

i) Ordenar la revocación o suspensión de certificados digitales cuando la entidad de certificación los hubiere emitido sin el cumplimiento de las formalidades legales;

j) Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones;

k) Emitir certificados digitales en relación con las firmas digitales de las entidades de certificación.

Artículo 39.- (FUNCIONES DE LA ENTIDAD CERTIFICADORA). Las entidades certificadoras tendrán las siguientes funciones:

a) Emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales;

b) Facilitar servicios de generación de firmas digitales;

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) Reconocer y validar los certificados digitales emitidos en el exterior;

f) Otras funciones relacionadas con la prestación de servicios de certificación digital.

Artículo 40.- (FUNCIONES DE LA AGENCIA DE REGISTRO). Las funciones de la Agencia de Registro son las siguientes:

a) La recepción de las solicitudes de emisión de certificados;

b) Comprobar la identidad y autenticación de los datos de los titulares de certificados;

c) Comprobar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la entidad certificadora;

d) La remisión de las solicitudes aprobadas a la entidad certificadora con la que se encuentre operativamente vinculada;

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la entidad certificadora con la que se vinculen;

f) La identificación y autenticación de los solicitantes de revocación de certificados;

g) El archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la entidad certificadora;

h) El cumplimiento de las normas y recaudos establecidos para la protección de los datos personales;

i) El cumplimiento de las disposiciones que establezca la política de certificación y el manual de procedimiento de la entidad certificadora con la que se encuentre vinculada.

Artículo 41.- (SERVICIO DE CERTIFICACIÓN DIGITAL). Las entidades certificadoras deberán prestar los siguientes servicios:

a) **Servicio de Certificación Digital**: Consiste en emitir, revocar y administrar los certificados digitales utilizados para generar Firmas Digitales;

b) **Servicio de Registro:** Consiste en comprobar y validar la identidad del solicitante de un certificado digital, y otras funciones relacionadas al proceso de expedición y manejo de los certificados digitales;

c) Otros servicios relacionados a la certificación digital.

Artículo 42.- (TARIFAS POR LA PRESTACIÓN DEL SERVICIO DE CERTIFICACIÓN DIGITAL). Las entidades certificadoras autorizadas establecerán sus tarifas considerando criterios sustentados y orientados en costos del servicio de certificación digital, previa presentación de su estructura tarifaria a la ATT para su aprobación y registro.

Artículo 43.- (OBLIGACIONES DE LAS ENTIDADES CERTIFICADORAS). Para garantizar la publicidad, seguridad, integridad y eficacia de la firma y certificado digital, las entidades certificadoras están obligadas a:

a) Cumplir con la normativa vigente y los estándares técnicos emitidos por la ATT;

b) Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT;

c) Informar a los usuarios de las condiciones de emisión, validación, renovación, baja, suspensión, tarifas y uso acordadas de sus certificados digitales a través de una lista que deberá ser publicada en su sitio web 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 los certificados digitales emitidos 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) Las entidades certificadoras que derivan de la certificadora raíz (ATT) deberán mantener un sistema de información con las mismas características mencionadas en el punto anterior, ubicado en territorio y bajo legislación del Estado Plurinacional de Bolivia;

h) Revocar el certificado digital al producirse alguna de las causales establecidas en el presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la Revocatoria deben ser estipuladas en los contratos de los titulares;

i) Mantener la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso;

j) Mantener la información relativa a los certificados digitales emitidos, por un 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 solicitante del servicio, bajo su exclusiva responsabilidad;

o) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia;

p) Contar con plataformas tecnológicas de alta disponibilidad, que garanticen mantener la integridad de la información de los certificados y firmas digitales emitidos que administra.

Artículo 44.- (RESPONSABILIDAD DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS ANTE TERCEROS). I. Las entidades certificadoras autorizadas serán responsables por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios.

II. Las entidades certificadoras autorizadas privadas deberán rendir una caución que será utilizada para responder por las eventuales consecuencias civiles contractuales o extracontractuales de su actividad. Esta caución será rendida por medio de una Póliza de Seguro expedida por una Entidad de Seguros debidamente establecida en el Estado Plurinacional de Bolivia, tomando en consideración los riesgos y responsabilidades inherentes a la labor de certificación digital. El monto de la caución será fijada por la ATT anualmente mediante Resolución Administrativa, conforme a categorías que se determinarán de acuerdo con la cantidad de certificados emitidos.

III. La entidad certificadora autorizada se liberará de responsabilidades si demuestra que actuó con la debida diligencia y no le son atribuibles los errores y omisiones objeto de las reclamaciones.

IV. Las entidades certificadoras autorizadas deberán responder por posibles perjuicios que se causen al signatario o a terceros de buena fe por el retraso en la publicación de la información sobre la vigencia de los certificados digitales.

Artículo 45.- (GARANTÍA). I. Las entidades certificadoras deberán obtener y mantener vigente una boleta de garantía de cumplimiento de contrato, por el siete por ciento (7%) de sus ingresos brutos de la gestión inmediata anterior, o sobre sus proyecciones para el primer año, que respalde su actividad durante la vigencia de la autorización para prestación de servicios de certificación digital.

II. El incumplimiento de este requisito dará lugar a las acciones correspondientes en el marco de las competencias de la ATT.

Artículo 46.- (AUDITORÍAS). I. Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.

II. La ATT podrá implementar el sistema de auditoría, que debe como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, el cumplimiento de los estándares nacionales e internacionales sobre certificación y firma digital, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento de las políticas de certificación definidas por la autoridad, su declaración de prácticas de certificación y los planes de seguridad y de contingencia aprobados.

CAPÍTULO III
AUTORIZACIÓN A LA ENTIDAD CERTIFICADORA

Artículo 47.- (AUTORIZACIÓN PARA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN DIGITAL). La ATT mediante la firma de un contrato, otorgará la autorización para la prestación de servicios de Certificación Digital, con una vigencia de cinco (5) años, renovables por periodos similares, a personas naturales o jurídicas que así lo soliciten, previo cumplimiento de los requisitos y condiciones establecidos en Resolución Administrativa por la ATT.

Artículo 48.- (PAGO DE DERECHO). I. Las entidades certificadoras pagarán a la ATT de manera anual, el uno por ciento (1%) de sus ingresos brutos de operación del

servicio de certificación digital correspondiente al año anterior, como tasa de fiscalización y regulación.

II. Para el primer año de operación, la entidad certificadora cancelará por adelantado la tasa de fiscalización y regulación, en base a la proyección de sus ingresos brutos.

Artículo 49.- (TRANSFERENCIA DE MONTOS RECAUDADOS). La recaudación por concepto de la tasa de fiscalización y regulación, así como sus intereses y multas por mora, serán depositados por la ATT de manera semestral hasta los diez (10) días del mes siguiente, vencido el semestre, a la Cuenta Única del Tesoro (CUT).

Artículo 50.- (REVOCATORIA DE LA AUTORIZACIÓN). I. La ATT podrá revocar la autorización para la prestación de servicios de certificación digital otorgada a favor de la entidad certificadora, por las siguientes causales:

a) Cuando la entidad certificadora autorizada transfiera, ceda, arriende o realice cualquier acto de disposición de su autorización para prestación de servicios de certificación digital, sin contar con la autorización expresa de la ATT;

b) Por petición expresa de la entidad certificadora autorizada;

c) Quiebra de la entidad certificadora legalmente declarada;

d) Cuando la entidad certificadora autorizada no haya iniciado la provisión de servicios a los solicitantes durante los doce meses posteriores a la otorgación de la autorización para prestación de servicios de certificación digital;

e) Cuando la entidad certificadora preste un servicio distinto o modifique el objeto para el cual obtuvo la autorización para prestación de servicios de certificación digital, sin permiso de la ATT;

f) Cuando la entidad certificadora autorizada, luego de haber recibido una notificación de la ATT, sobre el incumplimiento de disposiciones contractuales, legales, técnicas y reglamentarias, no las corrija o subsane en los plazos que señale el contrato o la normativa aplicable;

g) En caso de que la entidad certificadora autorizada incumpla el pago de derecho por la prestación de servicios de certificación digital;

h) Por incurrir en cualquier otra causal establecida en su contrato.

II. De producirse la revocatoria, la ATT deberá prever el resguardo y transferencia a otra entidad certificadora de los certificados digitales y la información brindada por los titulares, quedando facultada para ello a intervenir la entidad certificadora antes de la notificación con revocatoria, en caso de ser necesario.

Artículo 51.- (TRANSFERENCIA DE LA ENTIDAD CERTIFICADORA AUTORIZADA). I. Para la transferencia de la autorización para prestación de servicios de certificación digital a otra entidad certificadora autorizada, la entidad certificadora deberá comunicar tal situación a los titulares de los certificados digitales por ella emitidos, con una

antelación de por lo menos dos (2) meses, señalando al titular 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 entenderá que el usuario ha consentido en la transferencia de los mismos.

II. En caso de revocatoria de una autorización, la entidad certificadora cuya autorización hubiere sido revocada, deberá comunicar inmediatamente a los titulares de certificados digitales esta situación para el traspaso de los certificados digitales a otra entidad certificadora autorizada.

III. La entidad certificadora comunicará a la ATT, con al menos dos (2) meses de anticipación sobre el destino que dará a los datos de los certificados digitales emitidos.

TÍTULO V
TITULAR DEL CERTIFICADO DIGITAL

CAPÍTULO I
DERECHOS Y OBLIGACIONES
DE LOS TITULARES DEL CERTIFICADO DIGITAL

Artículo 52.- (TITULAR DEL CERTIFICADO DIGITAL). Son titulares de la firma digital y del Certificado Digital las personas naturales y las personas jurídicas a través de sus representantes legales, que han solicitado por sí y para sí una certificación que acredite su firma digital.

Artículo 53.- (RESPONSABILIDAD DEL TITULAR). I. El titular será responsable por la falsedad, error u omisión en la información proporcionada a la entidad de certificación y por el incumplimiento de sus obligaciones como titular.

II. Los datos de creación de la firma digital vinculado a cada certificado digital de una persona jurídica será responsabilidad del representante legal, cuya identificación se incluirá en el certificado digital.

III. El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.

Artículo 54.- (DERECHOS DEL TITULAR DEL CERTIFICADO). El titular del certificado digital tiene los siguientes derechos:

a) A ser informado por la entidad certificadora, de las características generales, de los procedimientos de creación y verificación de firma digital, así como de las reglas sobre prácticas de certificación y toda información generada que guarde relación con la prestación del servicio con carácter previo al inicio del mismo, así como de toda modificación posterior;

b) A la confidencialidad de la información proporcionada a la entidad certificadora;

c) A recibir información de las características generales del servicio, con carácter previo al inicio de la prestación del mismo;

d) 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;

e) A que la entidad certificadora le proporcione la información sobre su domicilio legal en el país y sobre todos los medios a los que el titular pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del servicio contratado, o la forma en que presentará sus reclamos;

f) A ser informado, al menos con dos meses de anticipación, por la entidad certificadora del cese de sus actividades, con el fin de hacer valer su aceptación u oposición al traspaso de los datos de sus certificados a otra entidad certificadora.

Artículo 55.- (OBLIGACIONES DEL TITULAR). I. El titular de la firma digital mediante el Certificado Digital correspondiente tiene las siguientes obligaciones:

a) Proporcionar información fidedigna y susceptible de verificación a la entidad certificadora;

b) Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado;

c) Observar las condiciones establecidas por la entidad certificadora para la utilización del certificado digital y la generación de la firma digital;

d) Notificar oportunamente a la certificadora 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;

e) 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;

f) Comunicar a la entidad certificadora, cuando exista el riesgo de que los datos de su firma digital sean de conocimiento no autorizado de terceros, por el titular y pueda ser utilizada indebidamente;

g) 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.

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

CAPÍTULO II

TRATAMIENTO DE LOS DATOS PERSONALES

Artículo 56.- (PROTECCIÓN DE DATOS PERSONALES). A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado Plurinacional;

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.

TÍTULO VI
COMUNICACIONES PUBLICITARIAS POR MEDIO DE CORREO ELECTRÓNICO

CAPÍTULO ÚNICO
COMUNICACIONES COMERCIALES PUBLICITARIAS

Artículo 57.- (**COMUNICACIONES COMERCIALES PUBLICITARIAS).** Las comunicaciones por medio de correo electrónico u otro medio de comunicación digital equivalente que tengan por finalidad la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una

actividad comercial, industrial, artesanal o profesional, deberán cumplir las siguientes condiciones:

a) Deberán publicitar los servicios, caracterizando los mismos sobre la base de términos técnicos y de tecnología, incluyendo características técnicas, económicas, comerciales, tarifas, aspectos legales, respecto de todos los servicios, así como los mecanismos de suscripción y conclusión de la suscripción a dicho tipo de servicios;

b) En los textos publicitarios que se refieran a los servicios, las condiciones y características, y promociones así como en la publicidad de acceso a contenidos y aplicaciones digitales, deben utilizar redacciones de difusión que resalten las facilidades y bondades del servicio;

c) En caso de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, se deberá asegurar, además del cumplimiento de los requisitos establecidos en los incisos anteriores del presente artículo, que sean claramente identificadas como tales y que las condiciones de acceso, y en su caso de participación, se expresen de forma clara e inequívoca, así como las autorizaciones de las autoridades competentes;

d) Deberá indicar la forma como el destinatario puede aceptar o rechazar el envío de futuras comunicaciones del remitente, para que los usuarios puedan habilitarse o deshabilitarse en el caso de que no deseen continuar recibiendo estos mensajes o correos;

e) Deberán ser claramente identificables los remitentes y datos del mismo, indicando la persona natural o jurídica en nombre de la cual se realizan;

f) En la publicidad y acceso interactivo a los sitios web del proveedor a través de equipo terminal, el simple registro comercial de ingreso no conlleva a un enlace comercial del proveedor de difusión posterior, sino que esta debe ser explícita y manifiestamente aceptada por suscripción;

g) Las ofertas de productos o servicios deberán proporcionar información clara, precisa y veraz concordante con sus prestaciones.

TÍTULO VII
COMERCIO ELECTRÓNICO

CAPÍTULO ÚNICO

Artículo 58.- (COMERCIO ELECTRÓNICO). Las TIC, se utilizarán como un instrumento que permita promover el Comercio Electrónico, entre el Oferente y el Demandante de Bienes y Servicios.

Artículo 59.- (OBJETIVOS DEL COMERCIO ELECTRÓNICO). El comercio electrónico tendrá mínimamente los siguientes objetivos:

a) Facilitar el comercio electrónico en el interior y exterior del Estado Plurinacional;

b) Validar las operaciones efectuadas por medio de las nuevas TIC;

c) Fomentar y estimular la aplicación de nuevas tecnologías de la información;

d) Apoyar las nuevas prácticas comerciales.