

REGLAMENTO DE LA LEY N° 164, DE 08 DE AGOSTO DE 2011- LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN SOBRE DESARROLLO CONTENIDOS Y APLICACIONES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

**CAPITULO I
DISPOSICIONES GENERALES**

**ARTÍCULO 1. (OBJETO)
ARTÍCULO 2. (DEFINICIONES)**

**CAPÍTULO II
COMITÉ PLURINACIONAL DE TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIÓN – COPLUTIC**

**ARTÍCULO 3. (CONFORMACIÓN)
ARTÍCULO 4. (PARTICIPACIÓN)
ARTÍCULO 5. (FUNCIONAMIENTO)**

**CAPÍTULO III
CONSEJO SECTORIAL DE TELECOMUNICACIONES Y
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - COSTETIC**

**ARTÍCULO 6. (CONFORMACIÓN)
ARTÍCULO 7. (FUNCIONES)
ARTÍCULO 8. (FUNCIONAMIENTO)**

**CAPÍTULO IV
DEL GOBIERNO ELECTRÓNICO**

**ARTÍCULO 9. (OBJETO)
ARTÍCULO 10. (INSTANCIA RESPONSABLE)
ARTÍCULO 11. (LINEAMIENTOS)**

**CAPÍTULO V
DEL SOFTWARE LIBRE**

**ARTÍCULO 12. (INSTANCIA RESPONSABLE)
ARTÍCULO 13. (LINEAMIENTOS DEL PLAN)
ARTÍCULO 14. (PRESERVACIÓN DE SOFTWARE PÚBLICO)
ARTÍCULO 15. (EXCEPCIONES)**

**CAPÍTULO VI
GENERALIDADES DE DOCUMENTOS, FIRMAS Y CERTIFICADOS DIGITALES**

**ARTÍCULO 16. (EQUIVALENCIA FUNCIONAL)
ARTÍCULO 17. (CONSERVACIÓN)
ARTÍCULO 18. (UTILIZACIÓN DE FIRMAS ELECTRÓNICAS)**

CAPÍTULO VII

DE LA ENTIDAD CERTIFICADORA Y LA CERTIFICACIÓN DIGITAL

- ARTÍCULO 19. (ENTIDAD CERTIFICADORA)**
- ARTÍCULO 20. (ENTIDAD CERTIFICADORA PÚBLICA)**
- ARTÍCULO 21. (FUNCIONES)**
- ARTÍCULO 22. (PRECIO POR LOS SERVICIOS PRESTADOS)**
- ARTÍCULO 23. (OBLIGACIONES)**
- ARTÍCULO 24. (RESPONSABILIDAD DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS ANTE TERCEROS)**
- ARTÍCULO 25. (GARANTÍA)**
- ARTÍCULO 26. (CESE DE LA ENTIDAD CERTIFICADORA AUTORIZADA)**
- ARTÍCULO 27. (CONVENIO DE PARTES)**

CAPÍTULO VIII

DE LA AUTORIZACIÓN A LA ENTIDAD CERTIFICADORA

- ARTÍCULO 28. (REQUISITOS PARA LA AUTORIZACIÓN)**
- ARTÍCULO 29. (PROCEDIMIENTO PARA AUTORIZACION)**
- ARTÍCULO 30. (REVOCATORIA)**
- ARTÍCULO 31. (TASA)**
- ARTÍCULO 32. (INFRACCIONES Y SANCIONES)**
- ARTÍCULO 33. (RESOLUCIÓN DE CONTROVERSIAS)**
- ARTÍCULO 34. (FISCALIZACIÓN)**

CAPÍTULO IX

DE LA FIRMA DIGITAL

- ARTÍCULO 35. (CARACTERÍSTICAS)**
- ARTÍCULO 36. (FUNCIONES)**
- ARTÍCULO 37. (DEL TITULAR DE LA FIRMA Y DEL CERTIFICADO DIGITAL)**
- ARTÍCULO 38. (OBLIGACIONES DEL TITULAR)**
- ARTÍCULO 39. (INVALIDEZ DE LA FIRMA DIGITAL)**

CAPÍTULO X

DEL CERTIFICADO DIGITAL

- ARTÍCULO 40. (FUNCIÓN)**
- ARTÍCULO 41. (CAPACIDAD DEL SOLICITANTE)**
- ARTÍCULO 42. (CONTENIDO)**
- ARTÍCULO 43. (PERIODO DE VALIDEZ DEL CERTIFICADO DIGITAL)**
- ARTÍCULO 44. (SUSPENSIÓN DE LA VIGENCIA)**
- ARTÍCULO 45. (REVOCACIÓN)**

CAPÍTULO XI

DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE LA CERTIFICACIÓN DIGITAL

- ARTÍCULO 46. (DERECHOS DEL TITULAR DEL CERTIFICADO)**
- ARTÍCULO 47. (OBLIGACIONES DEL TITULAR DEL CERTIFICADO)**

**CAPÍTULO XII
DEL TRATAMIENTO DE LOS DATOS PERSONALES**

ARTÍCULO 48. (PROTECCIÓN DE DATOS PERSONALES)

**CAPÍTULO XIII
DEL SISTEMA DE AUDITORÍA**

ARTÍCULO 49. (AUDITORIAS)

**CAPÍTULO XIV
COMERCIO ELECTRÓNICO**

ARTÍCULO 50. (RÉGIMEN TÉCNICO DEL COMERCIO ELECTRÓNICO)

ARTÍCULO 51. (OFERTA ELECTRÓNICA DE BIENES Y SERVICIOS)

ARTÍCULO 52. (INFORMACIÓN SOBRE LAS CARACTERÍSTICAS Y COSTOS DE LOS BIENES Y/O SERVICIOS OFRECIDOS).

**CAPÍTULO XV
DEL CORREO ELECTRÓNICO**

ARTÍCULO 53. (CORREO ELECTRÓNICO PERSONAL)

ARTÍCULO 54. (CORREO ELECTRÓNICO LABORAL)

ARTÍCULO 55. (CARACTERÍSTICAS DE LAS COMUNICACIONES COMERCIALES PUBLICITARIAS)

ARTÍCULO 56. (PROHIBICIÓN DE COMUNICACIONES COMERCIALES NO SOLICITADAS)

REGLAMENTO DE LA LEY N° 164, DE 08 DE AGOSTO DE 2011- LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN SOBRE DESARROLLO CONTENIDOS Y APLICACIONES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

CAPITULO I DISPOSICIONES GENERALES

ARTÍCULO 1. (OBJETO) El presente Reglamento tiene por objeto regular el desarrollo de contenidos y aplicaciones de tecnologías de información y comunicación, la utilización de firmas digitales, el régimen de la certificación digital, la autorización, regulación, fiscalización y control de las entidades que prestan el servicio de certificación digital, aspectos del gobierno electrónico, software libre, comercio electrónico y correo electrónico en el Estado Plurinacional de Bolivia.

ARTÍCULO 2. (DEFINICIONES) En adición a las definiciones que constan en la Ley N° 164 – Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, se definen los siguientes términos técnicos:

I. Respecto a software libre.

1. Programa o software. Conjunto de instrucciones, reglas, procedimientos y documentos almacenados electrónicamente de manera tal que un dispositivo de procesamiento pueda utilizarlos para llevar a cabo una tarea específica o resolver un problema determinado.

2. Software libre. Software licenciado por su autor de manera tal que se ofrezcan a sus usuarios las siguientes libertades total o parcialmente:

a) Libertad de ejecutar el programa con cualquier propósito, sin discriminar personas o grupos, ni imponer restricciones a las actividades para las que el programa puede ser utilizado. La licencia del software no incluye restricciones al número de usuarios que pueden ejecutarlo, número de equipos en que se puede instalar, ni propósitos para los que se puede utilizar.

b) Libertad de estudiar la manera como opera el programa, incluyendo la realización de cualquier tipo de pruebas técnicas y la publicación de los resultados, sin restricciones, y la posibilidad de adaptarlo a las necesidades particulares.

c) Libertad para redistribuir copias del programa, incluido su código fuente a quien desee, bajo las mismas libertades que le fueron otorgadas.

d) Libertad para mejorar el software y distribuirlo públicamente bajo las mismas condiciones que le fueron otorgadas con el programa original.

3. Software propietario. Es el software cuyo autor no otorga las libertades de ejecutar, estudiar, redistribuir y mejorar el software, ni total ni parcialmente, sin autorización o licencia del autor.

4. Estándar abierto. Un estándar abierto hace referencia a un formato o protocolo que:

a) Esté sujeto a una evaluación pública completa, se pueda usar sin restricciones y esté disponible por igual para todas las partes.

b) No necesite ningún componente o extensión adicional que tenga dependencias con formatos o protocolos que no cumplan la definición de un estándar abierto.

c) Esté libre de cláusulas legales o técnicas que limiten su utilización por cualquier parte o en cualquier modelo de negocio.

d) Esté gestionado y pueda ser desarrollado independientemente por cualquier compañía en un proceso abierto a la participación equitativa por parte de competidores y terceras partes.

e) Esté disponible en varias implementaciones completas por compañías en competencia o como una implementación completa disponible para todas las partes.

II. Respecto a firmas y certificados digitales.

1. Agente automatizado. Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana.

2. Ambiente confiable. Conjunto de equipos, aplicaciones informáticas, sistemas, procedimientos e infraestructura utilizados para prestar los servicios de certificación de documentos y firmas digitales y otros relacionados con estas actividades, que cumplan con prácticas de seguridad establecidas en reglamentos específicos y estándares internacionalmente aceptados.

3. Autenticación. Proceso técnico por el cual se comprueba el vínculo entre la identidad de la persona que emite un documento digital firmado digital o electrónicamente, vinculándolo con dicho mensaje/documento.

4. 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 el período de vigencia, indicado en el certificado digital.

5. Documento Digital. Es toda representación digital de actos, hechos o datos jurídicamente relevantes, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

6. Firma Digital. Es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alternación.

7. Firma Electrónica. Datos en forma electrónica que puedan ser utilizados para identificar al signatario en relación con el mensaje electrónico de datos e indicar que el signatario aprueba la información recogida en el mismo.

8. Clave Privada. Clave generada bajo un sistema de encriptación que se emplea en la generación de una firma digital sobre un documento digital y es mantenida en reserva por el titular de la misma.

9. Clave Pública. Clave generada bajo un sistema de encriptación que es conocida y usada por el destinatario del documento digital para verificar la autenticidad de la firma digital puesta en dicho documento.

10. Integridad. Característica única de un documento digital que indica que el mismo no ha sido alterado en el proceso de transmisión desde su creación por parte del emisor hasta la recepción por el destinatario.

11. No repudio. Relación de una persona natural o jurídica con el documento digital de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones del mismo.

12. Mensaje electrónico de datos. Es la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos, digitales o similares.

13. Signatario. Persona titular de la firma digital que actúa en nombre propio o de una persona jurídica a la que representa legalmente.

III. Respecto a correo electrónico.

1. Correo Electrónico. Es un servicio de red que permite a las usuarias y usuarios enviar y recibir mensajes y archivos, mediante sistemas de comunicación electrónicos.

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

3. Correo Electrónico no solicitado. Todo mensaje, archivo, dato u otra información enviada por cualquier medio electrónico dirigido a un receptor con quien el emisor no tiene una relación comercial o personal existente y es enviado sin que medie un pedido expreso del receptor o sin su consentimiento.

4. Proveedor de servicio de correo electrónico. Persona natural o jurídica que provee a los usuarios registrados la capacidad para enviar o recibir correo electrónico y que actúa como intermediario en el envío o la recepción de dicho correo electrónico.

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

ARTÍCULO 3. (CONFORMACIÓN) I. El Comité Plurinacional de Tecnologías de Información y Comunicación - COPLUTIC estará conformado por:

- a) Un representante del Ministerio de Obras Públicas, Servicios y Vivienda que lo preside
- b) Un representante de TIC del Ministerio de Planificación del Desarrollo
- c) Un representante de TIC del Ministerio de Comunicación
- d) Un representante de TIC del Ministerio de Educación

- e) Un representante de TIC de la Agencia de Desarrollo para la Sociedad de la Información en Bolivia – ADSIB

Los representantes deberán tener un rango mínimo de Director General y ser designados mediante el instrumento legal correspondiente.

II. Los miembros del Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC no percibirán remuneración o dieta alguna por el ejercicio de las funciones propias del Comité.

ARTÍCULO 4. (PARTICIPACIÓN) I. A objeto de cumplir con la finalidad de su creación, los miembros del Comité Plurinacional de Tecnologías de Información y Comunicación - COPLUTIC podrán requerir la participación de funcionarios públicos, instituciones civiles y representantes de los actores involucrados del sector público y privado previa determinación del Comité, en sus reuniones dependiendo del tema específico a tratarse.

II. El Comité Plurinacional de Tecnologías de Información y Comunicación - COPLUTIC podrá contar con asesores técnicos ad-honorem, quienes emitirán opiniones técnicas especializadas respecto a los temas tratados con carácter de recomendación.

ARTÍCULO 5. (FUNCIONAMIENTO) I. Las reuniones del Comité Plurinacional de Tecnologías de Información y Comunicación - COPLUTIC serán convocadas por el representante del Ministerio de Obras Públicas, Servicios y Vivienda y se llevarán a cabo en instalaciones del mencionado Ministerio o en cualquier otro lugar que se considere pertinente.

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 de sus miembros y cuando existan temas cuya aprobación deban ser sometida a votación, la decisión se tomará por mayoría simple, en caso de empate, el que presida tendrá voto decisivo.

IV. Los miembros del Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC tienen derecho a voz y voto en las reuniones y su participación será obligatoria por sí o a través de su suplente. Los asesores e invitados tendrán derecho a voz, pero no a voto.

V. El representante de la institución que preside el Comité designará al miembro que hará las veces de Secretario de la reunión, quién redactará el Acta de la reunión correspondiente y, antes de su aprobación leerá la misma para su posterior aprobación por los miembros del Comité en la misma sesión.

VI. Si existiera un voto en contra, el mismo tendrá que ser justificado y constar en acta.

VII. La convocatoria y orden del día de las reuniones tanto ordinarias como extraordinarias serán realizadas por el representante del Ministerio de Obras Públicas, Servicios y Vivienda y serán comunicadas a los demás miembros a través de correo electrónico con

diez días hábiles de anticipación tratándose de reuniones ordinarias y de cinco días hábiles, si se trata de reuniones extraordinarias.

VIII. Los miembros del Comité podrán solicitar por escrito al Presidente que convoque a sesiones extraordinarias para tratar asuntos urgentes que deberán mencionarse en su petición.

IX. Cada año se debatirá y aprobará un informe de las actuaciones realizadas durante el periodo y se propondrá iniciativas para mejorarlas. El informe para su seguimiento será presentado al Presidente del Estado Plurinacional de Bolivia

CAPITULO III CONSEJO SECTORIAL DE TELECOMUNICACIONES Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - COSTETIC

ARTÍCULO 6. (CONFORMACIÓN) El Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación - COSTETIC estará conformado por:

- a) Ministro cabeza del sector de Telecomunicaciones y Tecnologías de Información y Comunicación (Ministro de Obras Públicas, Servicios y Vivienda) o un representante que lo preside
- b) Viceministro de Telecomunicaciones o un representante.
- c) Director General Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT o un representante.
- d) Director de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB o un representante.
- e) Un representante o autoridad competente debidamente designado por los Gobiernos Autónomos departamentales.
- f) Un representante o autoridad competente debidamente designado por los Gobiernos Autónomos municipales.
- g) Un representante o autoridad competente debidamente designado por los Gobiernos Autónomos de las naciones y pueblos indígena originario campesinos

ARTÍCULO 7. (FUNCIONES) El Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación - COSTETIC, como instancia consultiva de proposición y concertación entre el nivel central del Estado y los gobiernos autónomos (departamentales, municipales e indígenas originario campesinas), tiene como funciones principales las siguientes:

- Proponer y coordinar mecanismos necesarios para fomentar el acceso, uso y apropiación social de las tecnologías de información y comunicación;
- Desplegar y usar la infraestructura tecnológica;
- Promocionar y desarrollar contenidos, aplicaciones y servicios 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.

ARTÍCULO 8. (FUNCIONAMIENTO) I. Las reuniones del Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación - COSTETIC serán convocadas por Ministro la cabeza del sector o su representante y se llevaran a cabo en

instalaciones del Ministro de Obras Públicas, Servicios y Vivienda o en cualquier otro lugar que se considere pertinente.

II. Se reunirán por lo menos una vez al año de manera presencial y tantas veces como sea necesario a convocatoria por el Ministro la cabeza del sector o su representante a través de videoconferencias o fonconferencias.

III. El Ministro cabeza del sector o su representante de la institución que preside el Consejo designará al miembro que hará las veces de Secretario de la reunión, quién redactará el Acta de la reunión correspondiente y, antes de su aprobación leerá la misma para su posterior aprobación por los miembros del Consejo en la misma sesión.

VI. Si existiera un voto en contra, el mismo tendrá que ser justificado y constar en acta.

VII. La convocatoria y orden del día de las reuniones tanto ordinarias como extraordinarias serán realizadas por el Ministro cabeza del sector o su representante de la institución que preside el Consejo y serán comunicadas a los demás miembros a través de correo electrónico con diez días hábiles de anticipación tratándose de reuniones ordinarias y de cinco días hábiles, si se trata de reuniones extraordinarias.

VIII. Los miembros del Consejo podrán solicitar por escrito al Ministro cabeza del sector o su representante de la institución que preside el Consejo que convoque a sesiones extraordinarias para tratar asuntos urgentes que deberán mencionarse en su petición.

IX. Cada año se debatirá y aprobará un informe de las actuaciones realizadas durante el periodo y se propondrá iniciativas para mejorarlas. El informe para su seguimiento será presentado al Presidente del Estado Plurinacional de Bolivia

CAPITULO IV DEL GOBIERNO ELECTRÓNICO

ARTÍCULO 9. (OBJETO) Se entenderá por Gobierno Electrónico el uso de tecnologías de información y comunicación orientada a modernizar la gestión pública, en términos de mejorar la calidad de los servicios, perfeccionar la calidad de atención a la ciudadanía, la eficiencia y eficacia, transparencia e interoperabilidad de los actos administrativos, eliminación de la discrecionalidad de acciones funcionarias, participación e interacción de la ciudadanía con los diferentes Órganos y niveles autonómicos del Estado Plurinacional.

ARTÍCULO 10. (INSTANCIA RESPONSABLE) El Ministerio de Planificación del Desarrollo, es la instancia responsable de impulsar la implementación del Gobierno electrónico en Bolivia.

ARTÍCULO 11. (LINEAMIENTOS) Para la incorporación del Gobierno Electrónico a los procedimientos gubernamentales, a la prestación de sus servicios y a la difusión de información, se disponen los siguientes lineamientos:

a) Elaborar, diseñar e implementar un Plan Nacional de Gobierno Electrónico con todos los actores involucrados.

b) Definir y establecer las políticas de seguridad informática para el gobierno electrónico.

c) Definir y establecer los estándares tecnológicos de interoperabilidad entre los diferentes sistemas de información del Estado en todos sus niveles, entre ellos y con los ciudadanos.

d) Organizar los distintos sistemas de información de los órganos del Estado y niveles de la administración pública.

CAPITULO V DEL SOFTWARE LIBRE

ARTÍCULO 12. (INSTANCIA RESPONSABLE) Se determina que el Viceministerio de Ciencia y Tecnología, dependiente del Ministerio de Educación es la instancia responsable de elaborar el plan de implementación de software libre y estándares abiertos, en coordinación con el nivel central del Estado y los gobiernos autónomos, conforme lo dispone el Artículo 77 de la Ley N° 164 de 8 de agosto de 2011.

ARTÍCULO 13. (LINEAMIENTOS DEL PLAN) El plan de implementación de software libre y estándares abiertos, deberá tomar en cuenta los siguientes lineamientos:

a) Definir los sistemas de información que utilizan los órganos y niveles del Estado para alcanzar y permitir la integridad, oportunidad, confidencialidad, disponibilidad, interoperabilidad e independencia tecnológica de todos los procesos y procedimientos administrativos.

b) Analizar la factibilidad del cambio o migración de los sistemas de información utilizados.

c) Definir un plan de formación de recursos humanos para el desarrollo e implementación del software libre.

d) Incentivar a las Universidades y otras entidades públicas y privadas en los procesos de investigación y desarrollo de aplicaciones que utilicen estándares abiertos.

e) Promover la cooperación internacional en materia de software libre.

ARTÍCULO 14. (PRESERVACIÓN DE SOFTWARE PÚBLICO) I. Los estándares de desarrollo, preservación, acopio, registro, transferencia y licenciamiento de software libre desarrollado por el Estado de manera directa o a través de terceros, serán determinados por el COPLUTIC. Para esta finalidad se creará un repositorio estatal bajo cuya responsabilidad se encontrará su protección.

II. El COPLUTIC definirá que entidad pública se encontrará a cargo del repositorio en el marco de la soberanía y seguridad nacional.

ARTÍCULO 15. (EXCEPCIONES) La utilización de software propietario será permitido en las siguientes circunstancias:

a) Cuando no se disponga de programas de software libre adecuados para cumplir una determinada labor, debiendo estar técnicamente justificado.

b) Cuando la utilización del software libre pueda causar incompatibilidad operacional con otros programas utilizados en el sector público.

CAPITULO VI GENERALIDADES DE DOCUMENTOS, FIRMAS Y CERTIFICADOS DIGITALES

ARTÍCULO 16. (EQUIVALENCIA FUNCIONAL) Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma digital que cumplan con las disposiciones de la Ley N° 164 de 8 de agosto de 2011 y del presente Reglamento serán válidos de la misma manera y producirán los mismos efectos que los actos y contratos celebrados por escrito, con firma autógrafa y en soporte físico.

ARTÍCULO 17. (CONSERVACIÓN) I. La conservación es un requisito para la equivalencia funcional del documento digital.

II.- La conservación de la información contenida en un documento digital, deberá cumplir las siguientes condiciones:

a) Ser conservada en el formato original con el que haya sido generada, enviada o recibida que demuestre su integridad y la identidad del generador del documento digital, su origen, fecha y hora de creación, destino y otros, por un plazo no menor a 5 años.

b) Ser accesible y estar disponible para posteriores consultas a requerimiento de autoridad competente.

III. Para la conservación de información contenida en documentos digitales se podrá utilizar el servicio de terceros autorizados.

IV. La información que tenga por única finalidad hacer conocer el envío o recepción de un documento digital privado está exenta de la obligación de conservarse.

ARTÍCULO 18. (UTILIZACIÓN DE FIRMAS ELECTRÓNICAS) Las disposiciones contenidas en el presente Reglamento no limitan la utilización de firmas electrónicas, las cuales serán válidas en el marco del acuerdo de las partes.

CAPITULO VII DE LA ENTIDAD CERTIFICADORA Y LA CERTIFICACIÓN DIGITAL

ARTÍCULO 19. (ENTIDAD CERTIFICADORA) I. Es la persona jurídica de derecho público o privado que tiene la capacidad económica, técnica, legal y administrativa para prestar servicios de certificación digital y otros relacionados, previo derecho de autorización otorgada por la ATT a través de la suscripción del contrato correspondiente.

II. Cuando en el presente Reglamento se mencione entidad certificadora o entidad certificadora autorizada se entenderá que se está refiriendo tanto a la entidad certificadora pública como a la privada.

ARTÍCULO 20. (ENTIDAD CERTIFICADORA PÚBLICA) Conforme lo determinado en la Ley N° 164 – Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB será la entidad certificadora pública que prestará los servicios de certificación digital para el sector público y la población en general, cumpliendo los requisitos técnicos, económicos y legales, fijados por la ATT para la correcta prestación del servicio.

ARTÍCULO 21. (FUNCIONES) I. Las entidades certificadoras tendrán las siguientes funciones:

- a) Emitir, validar, renovar, denegar, suspender o revocar certificados digitales.
- b) Homologar certificados digitales emitidos por entidades certificadoras extranjeras.
- c) Facilitar servicios de generación de firmas digitales.
- d) Garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario.
- e) Otras funciones relacionadas con la certificación digital.

ARTÍCULO 22. (PRECIO POR LOS SERVICIOS PRESTADOS) El precio o importe por los servicios prestados por las entidades certificadoras será establecido en el marco del régimen general de tarifas y precios regulados por la ATT.

ARTÍCULO 23. (OBLIGACIONES) Para garantizar la publicidad, seguridad, integridad y eficacia de la firma y certificado digital, las entidades certificadoras están obligadas a:

- a) Cumplir con el marco normativo aplicable a la prestación del servicio de certificación digital, el que está conformado por la Ley N° 164, el presente Reglamento, las normas y disposiciones técnicas emitidas por la ATT y demás normas aplicables.
- b) Prestar los servicios de certificación digital conforme a estándares internacionales y los procedimientos a ser aprobados por la ATT.
- c) Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las políticas de protección de la información y lineamientos establecidos por la ATT.
- d) Informar a los usuarios de las condiciones de emisión, validación, renovación, revocación, suspensión, y uso acordadas de sus certificados digitales.
- e) 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.

f) Mantener el control, reserva y cuidado sobre la clave pública que le es confiada por el signatario.

g) 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 fecha de emisión, vigencia y restricciones aplicables, así como el detalle de los certificados digitales suspendidos.

h) Revocar el certificado digital al producirse alguna de las causales establecidas en el Artículo 45 del presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la cancelación deben ser estipuladas en los contratos de los titulares y suscriptores.

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) Informar a la ATT de la validación de certificados digitales emitidos por entidades extranjeras.

l) 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.

m) Demostrar que los controles técnicos que emplea son adecuados y efectivos cuando así sea requerido.

n) Mantener domicilio legal en el territorio del Estado Plurinacional de Bolivia.

o) Notificar a la ATT cualquier modificación en sus procedimientos, personería jurídica, accionar comercial, o cualquier cambio administrativo, dirección, teléfonos, correo electrónico dentro los diez (10) días hábiles siguientes de producida la modificación o cambio.

p) Verificar toda la información proporcionada por el solicitante del servicio, bajo su exclusiva responsabilidad.

q) Contar con personal profesional, técnico y administrativo con conocimiento especializado en la materia.

r) Contar con plataformas tecnológicas de alta disponibilidad, que permita mantener la integridad de la información de los certificados y firmas digitales emitidos que administra, incluso en caso de producirse desastres naturales, fuerza mayor o casos fortuitos.

ARTÍCULO 24. (RESPONSABILIDAD DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS ANTE TERCEROS) I. La entidad certificadora autorizada será responsable por la emisión de certificados digitales con errores y omisiones que causen

perjuicio a sus signatarios frente a reclamaciones de terceros.

II. La Entidad Certificadora Autorizada del servicio 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.

ARTÍCULO 25. (GARANTIA) I. Para prestar el servicio de certificación digital y afrontar los riesgos que puedan surgir como resultado del cumplimiento de sus funciones, las entidades certificadoras deberán obtener y mantener vigente una garantía que respalde su actividad durante la vigencia de su autorización.

II. La ATT establecerá la cuantía mínima de la póliza de seguro o garantía bancaria y determinará los criterios para el cumplimiento de este requisito.

III. El incumplimiento de este requisito dará lugar a la revocatoria de la autorización otorgada.

ARTÍCULO 26. (CESE DE LA ENTIDAD CERTIFICADORA AUTORIZADA) I. La entidad certificadora cesa en la prestación del servicio, en los siguientes casos:

a) Por decisión unilateral comunicada a la ATT.

b) Por revocación de la autorización para su funcionamiento.

c) Por quiebra declarada judicialmente.

d) Por disolución de la persona jurídica.

e) Por decisión de la ATT, mediante Resolución motivada como consecuencia del incumplimiento de los requerimientos exigidos para la prestación del servicio.

II. Para el supuesto del inciso a), 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 meses y señalando al titular que de no existir objeción a la transferencia de los certificados digitales a otra entidad certificadora autorizada, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos.

III. Asimismo, deberá comunicar este hecho a la ATT, con al menos un mes de anticipación, informándole sobre el destino que dará a los datos de los certificados digitales emitidos.

IV. La revocación de la autorización deberá comunicarse inmediatamente a los titulares de certificados digitales. En caso que la entidad certificadora esté en situación de efectuar el traspaso de los certificados digitales a otra entidad certificadora debidamente autorizada, deberá informar tal situación en la forma y plazo señalado en el parágrafo II. Si el titular se opone a la transferencia, el certificado digital quedará sin efecto sin más trámite.

ARTÍCULO 27. (CONVENIO DE PARTES) La relación entre la entidad certificadora que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren. Este modelo de Contrato será previamente aprobado por la ATT.

CAPÍTULO VIII DE LA AUTORIZACIÓN A LA ENTIDAD CERTIFICADORA

ARTÍCULO 28. (REQUISITOS PARA LA AUTORIZACIÓN) El procedimiento de solicitud de autorización para la prestación de servicio de entidad certificadora se inicia con la presentación de nota dirigida a la ATT, acompañada de la siguiente documentación:

- a) Nombre y apellido del representante legal.
- b) Testimonio de Constitución y Poder de Representación, debidamente inscritos en FUNDEMPRESA, cuando corresponda
- c) Matrícula de Comercio emitida por FUNDEMPRESA, cuando corresponda.
- d) Número de Identificación Tributaria.
- e) Estados financieros debidamente auditados
- f) Declaración Jurada con la descripción detallada de la infraestructura e instalaciones suficientes, políticas de seguridad, operación y otras para el uso adecuado de los certificados digitales emitidos y procedimientos para la certificación y otros dispuestos por la ATT.
- g) Documentos respaldatorios que acrediten que cuenta con la capacidad tecnológica conforme a estándares internacionales para la prestación del servicio de certificación digital.
- h) Proyecto de modelo de contrato a suscribirse con los usuarios.
- i) El comprobante de pago por derecho de solicitud de autorización.
- j) Plan de Inversión para los siguientes 5 años.
- k) Otros documentos que a criterio de la ATT sean requeridos.

ARTÍCULO 29. (PROCEDIMIENTO PARA AUTORIZACION) I. Recibida la solicitud, la ATT procederá a determinar la admisibilidad de la misma mediante la verificación de los antecedentes presentados, dentro de los tres (3) días hábiles siguientes.

II. Admitido el trámite, la ATT evaluará la documentación técnica, económica y legal presentada y en caso de evidenciarse el cumplimiento de los requisitos exigidos procederá a emitir la correspondiente Resolución Administrativa otorgando la autorización y disponiendo la suscripción del contrato respectivo.

III. En caso de que la ATT determine que el solicitante no cumple con los requisitos exigidos para la prestación del servicio, requerirá al interesado la presentación de documentación, técnica, legal o económica, adicional que requiera, otorgándole un plazo prudencial que no excederá de cinco (5) días hábiles, cumplido el mismo y no habiéndose recibido la documentación requerida la solicitud será rechazada.

IV. Durante el proceso de autorización, la ATT podrá realizar las inspecciones o verificaciones técnicas que considere necesarias.

ARTÍCULO 30. (REVOCATORIA) I. La ATT podrá revocar la autorización otorgada a favor de la entidad certificadora y terminará el contrato, conforme a las siguientes causales:

- a) Cuando la entidad certificadora autorizada transfiera, ceda, arriende o realice cualquier acto de disposición de su autorización para la prestación de servicio, debidamente aprobados por la ATT, a un tercero.
- 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.
- e) Cuando la entidad certificadora preste un servicio distinto o modifique el objeto para el cual obtuvo la autorización, sin autorización 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 provisión de servicios.

II. De producirse la revocación 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.

III. La ATT podrá revocar la autorización otorgada en caso de verificarse el incumplimiento de los requerimientos exigidos para la prestación del servicio o por pérdida de las condiciones técnicas, económicas o legales que sirvieron de fundamento a su autorización o fraude declarado judicialmente.

ARTÍCULO 31. (TASA) I. La ATT por medio de la resolución administrativa correspondiente fijará anualmente la tasa y los costos de mantenimiento de la autorización, los mismos que serán pagados por la entidad certificadora por un monto del uno por ciento (1%) de sus ingresos brutos de operación del año anterior del servicio de certificación.

II. Para el primer año de operación, la entidad certificadora cancelará por adelantado la tasa y los costos de mantenimiento de la autorización, en base a la proyección efectuada en su propuesta económica.

ARTÍCULO 32. (INFRACCIONES Y SANCIONES) El incumplimiento a las disposiciones contenidas en el presente Reglamento será sancionado conforme a lo dispuesto en el Reglamento de Infracciones y Sanciones.

ARTÍCULO 33. (RESOLUCIÓN DE CONTROVERSIAS) I. La interpretación, validez y cumplimiento de las condiciones del contrato y de todas aquellas obligaciones derivadas del servicio se regirán por las leyes del Estado Plurinacional de Bolivia.

II. Cualquier acción o procedimiento iniciado para resolver una controversia derivada de las presentes condiciones del servicio se someterá al procedimiento de los recursos administrativos dispuestos en la Ley No. 2341, de fecha 23 de abril de 2002 y su reglamento aprobado mediante DS. 27113 de fecha 23 de julio de 2003.

ARTÍCULO 34. (FISCALIZACIÓN) I. En función de las atribuciones que constan en la Ley N° 164 – General de Telecomunicaciones, Tecnologías de Información y Comunicación, la ATT cumplirá su función fiscalizadora mediante la realización de inspecciones ordinarias y extraordinarias a las entidades certificadoras. La inspección ordinaria consiste en la facultad de practicar una visita anual a las instalaciones de la entidad certificadora. La inspección extraordinaria será practicada de oficio o por denuncia motivada sobre la prestación del servicio, ordenada mediante resolución fundamentada.

II. La ATT requerirá toda información técnica, financiera o de cualquier otra naturaleza que considere necesaria dentro del ámbito de su competencia sin que la entidad certificadora pueda negarse a dicho requerimiento.

CAPÍTULO IX DE LA FIRMA DIGITAL

ARTÍCULO 35. (CARACTERÍSTICAS) La firma digital presenta las siguientes características mínimas:

- a) Se genera al cifrar el código de verificación de un documento digital usando la clave privada del titular del certificado digital.
- b) Es única para el titular de la firma digital y en cada documento digital firmado por éste.
- c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
- d) Su generación está bajo el control exclusivo del titular de la firma digital.
- e) Está añadida o asociada lógicamente al documento digital de tal manera que es posible detectar su alteración.

ARTÍCULO 36. (FUNCIONES) La firma digital cumple las siguientes funciones:

- a) Acredita la identidad del titular de la firma digital que consta en el documento digital confirmando que fue firmado con la clave privada.
- b) Garantiza la integridad del documento digital firmado.
- c) Garantiza que el titular de la firma digital no pueda repudiar o desconocer un documento digital que ha sido emitido por él y usando su clave privada.

ARTÍCULO 37. (DEL TITULAR DE LA FIRMA Y DEL CERTIFICADO DIGITAL) I. El documento con firma digital le otorga a su titular la responsabilidad sobre los efectos jurídicos generados por la utilización del mismo.

II. Tratándose de personas naturales, éstas son titulares de la firma digital y del certificado. Se incluye la firma digital que es generada a través de agentes automatizados.

III. Las personas jurídicas son titulares de la firma digital y del certificado digital a través de sus representantes legales.

ARTÍCULO 38. (OBLIGACIONES DEL TITULAR) I. El titular de la firma digital 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 (clave privada), 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.

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.

ARTÍCULO 39. (INVALIDEZ DE LA FIRMA DIGITAL) Una firma digital pierde validez si es utilizada cuando el periodo de validez de su certificado digital ha expirado.

CAPÍTULO X DEL CERTIFICADO DIGITAL

ARTÍCULO 40. (FUNCIÓN) El certificado digital cumple la función de legitimar la autoría de la firma digital que certifica y con esta la integridad del documento digital.

ARTÍCULO 41. (CAPACIDAD DEL SOLICITANTE) El solicitante de un certificado digital, deberá:

a) Tratándose de personas naturales tener capacidad de obrar.

b) Tratándose de personas jurídicas acreditar su personería jurídica a través de su registro en FUNDEMPRESA vigente.

ARTÍCULO 42. (CONTENIDO) Los certificados digitales deberán contener, al menos, las siguientes menciones:

I. PERSONAS NATURALES:

a) Código de Identificación Único del certificado con numeración de secuencia correlativa.

b) Identificación de la entidad certificadora que contenga: denominación o razón social, número de Matrícula de Comercio, Número de Identificación Tributaria, domicilio legal de la Entidad Certificadora, dirección de correo electrónico, número de Resolución Administrativa y contrato de autorización.

- c) Firma digital de la entidad certificadora.
- d) Plazo de vigencia.
- e) Fecha y hora de emisión del certificado
- f) Nombre completo y cédula de identidad del titular
- g) Dirección de correo electrónico del titular
- h) Otros datos de seguridad que se considere necesarios

II. PERSONAS JURÍDICAS:

- a) Código de Identificación Único del certificado, con numeración de secuencia correlativa.
- b) Identificación de la entidad certificadora que contenga: denominación o razón social, número de Matrícula de Comercio, Número de Identificación Tributaria, domicilio legal de la Entidad Certificadora, dirección de correo electrónico, número de Resolución Administrativa y contrato de autorización.
- c) Firma digital de la entidad certificadora.
- d) Plazo de vigencia.
- f) Fecha y hora de emisión del certificado
- g) Razón social o denominación de la persona jurídica titular
- h) Matrícula de comercio FUNDEMPRESA de la persona jurídica titular.
- i) Número de identificación tributaria de la persona jurídica titular
- j) Dirección oficial de correo electrónico de la persona jurídica titular
- k) Nombre completo del representante legal
- l) Número de cédula de identidad del representante legal
- m) Dirección de correo electrónico vigente del representante legal
- n) Otros datos de seguridad que se considere necesarios

ARTÍCULO 43. (PERÍODO DE VALIDEZ DEL CERTIFICADO DIGITAL) I. El certificado digital será válido dentro del período de su vigencia, el mismo que no podrá exceder de dos (2) años.

II. La entidad certificadora no deberá emitir certificados digitales cuya vigencia sea mayor a la vigencia de su autorización otorgada

ARTÍCULO 44. (SUSPENSIÓN DE LA VIGENCIA) I. La vigencia de un certificado digital podrá ser suspendida cuando se verifique alguna de las siguientes circunstancias:

- 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 judicial.

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 terminará 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 Judicial.

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

ARTÍCULO 45. (REVOCACIÓN) I. Un certificado digital podrá quedar sin efecto:

- 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 recepcionada por la Entidad Certificadora
- d) Fallo judicial ejecutoriado
- e) Por requerimiento de autoridad competente conforme a Ley.
- f) Si 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.
- g) 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 del servicio.
- h) Las demás 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.

CAPÍTULO XI DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE LA CERTIFICACIÓN DIGITAL

ARTÍCULO 46. (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. Para ello, la entidad de certificación debe emplear los elementos técnicos disponibles para otorgar seguridad y privacidad a la información aportada. Los signatarios tendrán derecho a recibir información de las características generales de dichos elementos, con carácter previo al inicio de la prestación del servicio.

c) 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.

d) 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.

e) 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 47. (OBLIGACIONES DEL TITULAR DEL CERTIFICADO) El titular del certificado digital deberá cumplir con las siguientes obligaciones:

a) 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.

b) 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.

c) Solicitar la suspensión inmediata del certificado digital cuando tome conocimiento del uso indebido de su firma digital.

d) Proporcionar los datos de su identidad personal y otra información requerida a ser objeto de certificación, brindando declaraciones exactas y completas.

e) 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.

f) Cumplir con las obligaciones establecidas en la Ley, el presente Reglamento y las normas técnicas que emita la ATT.

CAPÍTULO XII DEL TRATAMIENTO DE LOS DATOS PERSONALES

ARTÍCULO 48. (PROTECCIÓN DE DATOS PERSONALES) I. La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado.

II. El tratamiento de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, grabación, conservación, elaboración, modificación, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del consentimiento previo, expreso e informado del titular, el que será brindado por escrito o por 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.

III. 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 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.

IV. 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.

V. El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativas 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.

VI. Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales se desarrollarán en una norma específica.

CAPÍTULO XIII DEL SISTEMA DE AUDITORÍA

ARTÍCULO 49. (AUDITORIAS) I. Las entidades certificadoras podrán ser sometidas a auditorías técnicas y tecnológicas por la ATT.

II. La ATT podrá implementar el sistema de auditoría. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados.

CAPÍTULO XIV COMERCIO ELECTRÓNICO

ARTÍCULO 50. (RÉGIMEN TÉCNICO DEL COMERCIO ELECTRÓNICO) Las personas naturales o jurídicas que oferten y demanden servicios de comercio electrónico deberán cumplir con las condiciones establecidas en la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, el presente Reglamento y otras de carácter técnico emitidas por ATT, en lo que respecta a la utilización de firmas y certificados digitales emitidos por entidades certificadoras.

ARTÍCULO 51. (OFERTA ELECTRÓNICA DE BIENES Y SERVICIOS). La oferta de bienes, servicios e informaciones realizadas por medios digitales deberán contener:

- a) las condiciones generales del contrato y la descripción precisa de los procedimientos para su celebración, su conservación y accesibilidad, en caso de ser necesario;
- b) los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido;
- c) los procedimientos para que el adquirente reciba el comprobante de la operación o factura en su caso.

ARTÍCULO 52. (INFORMACIÓN SOBRE LAS CARACTERÍSTICAS Y COSTOS DE LOS BIENES Y/O SERVICIOS OFRECIDOS). I. El oferente de bienes y servicios deberá proporcionar información precisa y suficiente sobre las características de los bienes o servicios que ofrece y toda la información relativa a los productos ofrecidos, incluyendo especialmente cualquier advertencia sobre peligros o limitaciones relativos a su uso o consumo.

II. Asimismo, proporcionará información precisa y suficiente sobre el precio de los bienes o servicios que ofrece, incluyendo todos los costos adicionales.

CAPÍTULO XV DEL CORREO ELECTRÓNICO

ARTÍCULO 53. (CORREO ELECTRÓNICO PERSONAL) De conformidad con lo establecido en la Ley N° 164 - Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, el correo electrónico personal se encuentra dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado.

ARTÍCULO 54. (CORREO ELECTRÓNICO LABORAL) De conformidad con lo establecido en la Ley N° 164 - Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, el correo electrónico laboral se sujetará a los siguientes parámetros:

a) El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales.

b) El ejercicio de estas facultades por parte del empleador, así como las condiciones de uso y acceso al correo electrónico laboral, deberá ser notificado por medio fehaciente al empleado, al momento de poner a su disposición el correo electrónico o en cualquier oportunidad posterior, como requisito previo a su ejercicio.

c) El empleador deberá asimismo, notificar fehacientemente al empleado, su política respecto del acceso y uso de correo electrónico personal en el lugar de trabajo.

ARTÍCULO 55. (CARACTERÍSTICAS DE LAS COMUNICACIONES COMERCIALES PUBLICITARIAS) I. Toda comunicación que tenga 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, deberá cumplir las siguientes condiciones:

- a. Deberán ser previamente aceptadas por el destinatario de manera explícita.
- b. En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación digital equivalente incluirán al comienzo del mensaje la palabra "publicidad" o cualquier otro término que identifique claramente la intención de la comunicación, de manera tal que el destinatario pueda tener conocimiento de su naturaleza, incluso antes de abrir o acceder al texto del mensaje.
- c. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior, 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.
- d. Deberá indicar la forma como el destinatario puede rechazar el envío de futuras comunicaciones del remitente. El prestador de servicios comerciales a través de Internet que, mediando rechazo de futuras comunicaciones, intencionalmente

reenvíe un mensaje, envíe un nuevo mensaje y/o utilice otra dirección de correo electrónico para volver a contactar al destinatario que ha rechazado su comunicación incurrirá en falta grave.

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

ARTÍCULO 56. (PROHIBICIÓN DE COMUNICACIONES COMERCIALES NO SOLICITADAS) Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente o autorizadas por los destinatarios de las mismas.