Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 876/2016

La Paz, 27 de diciembre de 2016

Abog. Nikesti Fernanda Peña Barriga
ANALISTA LEGAL
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

VISTOS:

El Informe Técnico ATT-DTL TIC-INF TEC LP 1149/2016 de 09 de diciembre de 2016 y Anexos; el Informe Jurídico ATT-DJ-INF-JUR LP 2685/2016 de 27 de diciembre de 2016; las normas aplicables y todo lo que convino ver y se tuvo presente;

CONSIDERANDO 1: (Antecedentes).-

El Informe Técnico ATT-DTLTIC-INF TEC LP 1149/2016 de 09 de diciembre de 2016, emitido por el Analista de Tecnologías de Información vía el Supervisor de Regulación de Tecnologías de la Información y el Director Técnico Sectorial de Telecomunicaciones y Tecnologías de la Información y Comunicación de la Dirección Técnica Sectorial de Telecomunicaciones y Tecnologías de la Información y Comunicación – TIC, señala que se ha analizado los estándares respectivos y la normativa internacional disponible, elaborándose el primer documento "ESTÁNDAR TÉCNICO PARA EL FUNCIONAMINETO DEL SERICIO DE SELLADO DE TIEMPO", por lo que con el objetivo de perfeccionar el documento a adoptarse por nuestro país, se remitieron notas a veinticinco entidades privadas y públicas a fin de que emitan sus observaciones, mismas que fueron tomadas en cuenta en la elaboración del documento final, así como se tomaron en cuenta distintos estándares descritos en ese informe. Asimismo, señala que la institución que proporciona la hora oficial en el país, y que cuenta con acuerdos internacionales necesarios para ser fuente fiable de tiempo, para el servicio de sellado de tiempo es el Instituto Boliviano de Metrología - IBMETRO. Por lo que de acuerdo a la Disposición Transitoria Primera del Reglamento a la Ley N° 164 de 08 de agosto de 2011 para el Desarrollo de Tecnologías de Información y Comunicación recomiendan dar cumplimiento al artículo 38, inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo N° 1793, debiéndose aprobar el "ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO DE SELLADO DE TIEMPO" (Versión 2); y al tratarse de un Instrumento regulatorio con alcance nacional deberá publicarse el correspondiente edicto en un Matutino de circulación Nacional, así como en el portal WEB de la Institución.

Que el Informe Jurídico ATT-DJ-INF-JUR LP 2685/2016 de 22 de diciembre de 2016, emitido por la Dirección Jurídica señala que: *"En virtud a los antecedentes citados y las disposiciones de orden legal mencionadas, se considera que la solicitud de aprobación del "ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO SELLADO DE TIEMPO", realizada a través del Informe Técnico ATT-DTLTIC-INF TEC LP 1149/2016 por la Dirección Técnica Sectorial de Telecomunicaciones y TIC, se ajusta a la actual normativa vigente, por lo tanto, se recomienda emitir la correspondiente Resolución Administrativa Regulatoria por la que se disponga aprobar el documento "ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO SELLADO DE TIEMPO" y su correspondiente publicación en un Matutino de Circulación Nacional y en la página WEB de la Institución".*

DIRECCIÓN JURÍDICA J.C.Z. A.T.T.

DIRECTOR EJECUTIVO V°B° R.A.M.S.O. A.T.T.

CONSIDERANDO 2: (Marco normativo aplicable).-

El Parágrafo II del Artículo 103 de la Constitución Política del Estado establece que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 876/2016

El Decreto Supremo N° 0071 de 9 de abril de 2009, creó la Autoridad de Fiscalización y Control Social de Transportes y Telecomunicaciones – ATT con personalidad jurídica y patrimonio propio, con independencia administrativa, financiera, legal y técnica, supeditada al Ministerio cabeza de Sector (Ministerio de Obras Publicas Servicios y Vivienda - MOPSV), con el objetivo de regular las actividades que realicen las personas naturales y jurídicas, privadas, comunitarias, mixtas y cooperativas en los sectores de Transportes y Telecomunicaciones.

Este mismo cuerpo legal establece en el Artículo 19 que son atribuciones del Director Ejecutivo como Máxima Autoridad Ejecutiva de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), entre otras: "*a) Ejercer la administración y representación legal de la Autoridad de Fiscalización y Control Social de Teleconunicaciones y Transportes y asumir la responsabilidad de sus actos legales y administrativos en el marco de la Ley N° 1178, de 20 de julio de 1990 Ley de Administración y Control Gubernamentales, y demás disposiciones legales vigentes*" y "*f) Ordenar o realizar los actos necesarios para garantizar el cumplimiento de los fines relativos a la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes*".

La Disposición Transitoria Novena de la Ley N° 164, de 08 de agosto de 2016, General de Telecomunicaciones, Tecnologías de Información y Comunicación, establece que la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes cambia de denominación a AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT, asumiendo las atribuciones, competencias, derechos y obligaciones en materia de telecomunicaciones; tecnologías de la información y comunicación; transportes; servicio postal; bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda.

Los Numerales 2 y 5 del Artículo 2 de la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, disponen como objetivos asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; y promover el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.

El Artículo 71 de la Ley N° 164, declara de prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos.

La Disposición Transitoria Sexta de la referida Ley, señala que todos los aspectos que se requieran para la aplicación de la citada Ley serán reglamentados por el Órgano Ejecutivo y regulados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

El Decreto Supremo N° 1793 de 13 de noviembre de 2013, tiene como objetivo aprobar el Reglamento a la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación, para el Desarrollo de Tecnologías de Información y Comunicación.

La Disposición Transitoria Primera del Decreto Supremo N° 1793, establece que la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, tiene los siguientes plazos:

a. *Ocho (8) meses a partir de la publicación del presente Decreto Supremo, elaborará y aprobará los estándares técnicos y otros lineamientos establecidos para el funcionamiento de las entidades certificadoras;*
b. *Seis (6) meses a partir de la aprobación de los estándares técnicos, deberá implementar la infraestructura y procedimientos internos necesarios para la aplicación de la firma y certificación digital como Certificadora Raíz.*

DIRECCIÓN JURÍDICA V°B° R.C.Z. A.T.T.

DIRECTOR EJECUTIVO V°B° R.A.M.S.O. A.T.T.

DIRECCIÓN JURÍDICA V°B° A.T.T.

El Artículo 24 del señalado Reglamento, establece que: *"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"*.

El Numeral 1 del Artículo 37 del Reglamento a la Ley N° 164, establece los niveles de organización de la Infraestructura Nacional de Certificado Digital, señalando lo siguiente: *"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 públicas y privadas subordinadas*".

El inciso j) del Artículo 38 del Reglamento a la Ley N° 164, establece una de las funciones para el cumplimiento de las atribuciones establecidas para la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT en la Ley N° 164 General de Telecomunicaciones, Tecnologías de la Información y Comunicación, la misma que es la siguiente: *"Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones"*.

CONSIDERANDO 3: (Análisis).-

Que conforme al Artículo 14 de la Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de 08 de agosto de 2011, la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, tiene la atribución de cumplir y hacer cumplir la Ley N° 164 y sus reglamentos, asegurando la correcta aplicación de sus principios, políticas y objetivos.

Que el Informe Técnico ATT ATT-DTL TIC-INF TEC LP 1149/2016 de 09 de diciembre de 2016 y el Informe Jurídico ATT-DJ-INF-JUR LP XXX/2016 de 22 de diciembre de 2016, recomiendan la emisión de la Resolución Administrativa por la que se disponga la Aprobación del Documento "ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO DE TIEMPO", de conformidad con lo establecido en el inciso j) del Artículo 38 del Reglamento a la Ley N° 164, de 08 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

CONSIDERANDO 4: (Del ámbito de la competencia).-

Que las competencias y atribuciones para la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes están definidas por el Decreto Supremo N° 0071 de 09 de abril de 2009, quedando sometidas a ésta las personas naturales y jurídicas, privadas, comunitarias, públicas, mixtas y cooperativas, garantizando los intereses y derechos de los usuarios o consumidores, promoviendo la economía plural prevista en la Constitución Política del Estado y las leyes en forma efectiva.

Que la Disposición Transitoria Séptima de la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación, dispone: *"La presente Ley entrará en vigencia en la fecha de su publicación, con aplicación progresiva, conforme a la aprobación de sus reglamentos específicos; en tanto se aprueben éstos, se aplicarán los reglamentos vigentes de telecomunicaciones y postal en todo lo que no contravenga a esta Ley"*.

Que de conformidad a lo dispuesto por la Disposición Transitoria Novena de la mencionada Ley, la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes cambia de denominación a AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT, asumiendo las atribuciones, competencias, derechos y obligaciones en materia de telecomunicaciones; tecnologías de la información y comunicación; transportes; servicio postal; bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda.

Que mediante Resolución Suprema N° 19249 de 03 de agosto de 2016 del Señor Presidente del Estado Plurinacional de Bolivia, se designó a ROQUE ROY MENDES SOLETO, como Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

POR TANTO:

El Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes - ATT, Ingeniero ROQUE ROY MÉNDEZ SOLETO, designado mediante Resolución Suprema N° 19249 de 03 de agosto de 2016, en uso de sus atribuciones conferidas por ley y demás normas vigentes, a nombre del Estado Plurinacional de Bolivia;

RESUELVE:

PRIMERO.- APROBAR el documento "ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO SELLADO DE TIEMPO" anexo indivisible de la presente Resolución.

SEGUNDO.- INSTRUIR a la Dirección Técnico Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación de esta Autoridad, publicar la presente Resolución en un Matutino de Circulación nacional, así como en el portal WEB de la Institución.

Regístrese, comuníquese y archívese.

Ing. Roque Roy Méndez Soleto
DIRECTOR EJECUTIVO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

Es conforme;

DIRECCIÓN JURÍDICA V°B° A.T.T.

Dr. Javier Martín Castro Zacobeta
DIRECTOR JURÍDICO SUPLENTE
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

ESTANDAR TÉCNICO PARA EL FUNCIONAMIENTO DEL SERVICIO DE SELLADO DE TIEMPO

Capítulo I
Disposiciones Preliminares

Artículo 1 (Objeto).-

Establecer los requisitos, condiciones legales, económicas y técnicas adicionales que deben cumplir las Entidades Certificadoras Autorizadas del Estado Plurinacional de Bolivia, para la prestación de servicios de Sellado de Tiempo.

Artículo 2 (Estándares).-

El presente estándar establece los formatos y procedimientos necesarios para que una Entidad Certificadora Autorizada brinde los servicios de Sellado de Tiempo, basado en los siguientes estándares internacionales:

a) ETSI TS 102 023 v1.2.2 "Policy requirements for timestamping authorities - Requisitos de política para las autoridades de sellado de tiempo".
b) ISO 8601 que establece los "Elementos de datos y formatos intercambiables — Intercambio de información, representación de fechas y horas".
c) RFC 1305, RFC 5905 respecto a "Network Time Protocol – Protocolo de tiempo de la red".
d) RFC 3161 Internet X.509 Infraestructura de clave pública para el Protocolo de sellado de tiempo (TSP).
e) RFC 3628 que establece los "Requisitos de políticas para las Autoridades de Sellado de Tiempo (TSA)".
f) ETSI TS 101 861 "Time stamping profile – Perfil de sellado de tiempo".
g) XML: XML "Perfil de Timestamping de la OASIS (Digital Signature Services (DSS)- Servicio de Firmas Digitales)".

Artículo 3 (Normativa aplicable).-

I. Los artículos del 78 al 84 de la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación.
II. Los artículos del 24 al 56 del Reglamento a la Ley N° 164, para el Desarrollo de Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793 de 13 de noviembre de 2013.
III. La Disposición Transitoria Primera del Decreto Supremo N° 1793 del 13 de noviembre de 2013.

Artículo 4 (Abreviaturas).-

Para efectos del presente estándar entiéndase por:

a) **BIPM:** (Bureau International des Poids et Measures) Oficina Internacional de Pesos y Medidas.
b) **CIPM:** (International Committee for Weights and Measures) Comité Internacional de Pesos y Medidas.
c) **CRL:** (Certificate Revocation List) Lista de Certificados Revocados.
d) **ECA:** Entidad Certificadora Autorizada
e) **ECR:** Entidad Certificadora Raíz.
f) **ETSI:** (European Telecommunications Standards Institute) Instituto Europeo de Estándares de Telecomunicaciones.
g) **GMT:** (Greenwich Mean Time) Meridiano de Greenwich.

DIRECTOR EJECUTIVO V°B° F.A.M.S. A.T.T.

DIRECCIÓN JURÍDICA V°B° J.C.Z. A.T.T.

DIRECCIÓN JURÍDICA V°B° R.P.P.B.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

h) **GPS:** (Global Positioning System) Sistema de Posicionamiento Global.
i) **HSM**[1]**:** (Hardware Security Module) Modulo de Hardware de Seguridad.
j) **HTTPS:** (Hypertext Transfer Protocol Secure) Protocolo de red seguro.
k) **IBMETRO:** Instituto Boliviano de Metrología
l) **IERS:** (International Earth Rotation Service) Servicio Internacional de Rotación de la Tierra.
m) **IETF:** (Internet Engineering Task Force) Grupo de Trabajo de Ingeniería de Internet.
n) **ISO:** (International Organization for Standardization) Organización Internacional de Normalización.
o) **MRA:** (Mutual Recognition Arrangement) Acuerdo de Reconocimiento Mutuo.
p) **NTP**: (Network Time Protocol) Protocolo de Tiempo de Red según RFC 1305.
q) **OCSP:** Protocolo de Estado de Certificados en Línea, según RFC 2560.
r) **OID**[2]**:** (Object Identifier) Identificador de Objeto.
s) **PKI:** (Public Key Infrastructure) Infraestructura de Clave Pública
t) **RFC**[3]**:** (Request For Comments) Requerimiento de Comentarios.
u) **RSA:** (Rivest Shamir Adleman) Sistema criptográfico de clave pública.
v) **SHA**: (Secure Hash Algorithm) Algoritmo de Hash Seguro.
w) **SI:** Sistema Internacional de Unidades
x) **SIM:** Sistema Interamericano de Metrología
y) **TIC:** Tecnologías de Información y Comunicación.
z) **TSA:** (Time StampAuthority) Autoridad de Sellado de Tiempo.
aa) **TSP:** (Time-StampProtocol) Protocolo de Sellado de Tiempo
bb) **TSS:** (Time StampingServices) Servicios de Sellado de Tiempo
cc) **TST** (Time Stamp Token) Sello de Tiempo
dd) **TSU:** (Time Stamp Unit) Unidad de Sellado de Tiempo.
ee) **TTP:** (Trusted Third Party) Terceros Aceptantes.
ff) **URI:** (Uniform Resource Identifier) Identificador Uniforme de Recursos.
gg) **URL:** (Uniform Resource Locator) Localizador Uniforme de Recursos.
hh) **UTC (k):** (Universal Time Coordinated(k)[4]): Hora Universal Coordinada que se mantienen en institutos u observatorios que contribuyen con sus datos de reloj a la BIPM nacionales de metrología.
ii) **UTC:** (Universal Time Coordinated) Hora Universal Coordinada.

Articulo 5 (Definiciones).-

En lo referido a la Autoridad de Sellado de Tiempo – TSA:

a) **ATT**: Es la Autoridad de Regulación y Fiscalización de Transportes y Telecomunicaciones que fiscaliza, controla, supervisa y regula las actividades de Telecomunicaciones y Transportes y se constituye en la Entidad Certificadora Raíz.
b) **ECA**: Entidad Certificadora Autorizada por la ATT, pública o privada que brindan los servicios de certificación digital, registro y otros servicios relacionados a la certificación digital, dentro de los cuales está el de Sellado de Tiempo.
c) **Auditorías Técnicas:** Evaluación de 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

DIRECTOR EJECUTIVO V°B° R.N.M.S. A.T.T.

DIRECCIÓN JURÍDICA V°B° J.C.C. A.T.T.

DIRECCIÓN JURÍDICA V°B° R.J.P.B.

[1] El HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege claves criptográficas.
[2] OID es una nomenclatura que permite identificar objetos dentro de la estructura de la PKI Bolivia, existen valores predefinidos de los algoritmos.
[3] Es un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.
[4] (k) Es una abreviación para referirse a un tiempo obtenido en un laboratorio

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772265 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

políticas de sellado de tiempo definidas por la autoridad, su declaración de prácticas de sellado de tiempo y los planes de seguridad y de contingencia aprobados.

d) **Autoridad de Sellado de Tiempo - TSA:** Entidad Certificadora Autorizada de confianza que emite sellos de tiempo.

e) **Declaración de Prácticas de Sellado de Tiempo:** Establece las prácticas y procedimientos específicos del servicio de Sellado de Tiempo.

f) **Código de verificación (hash o resumen):** Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que:
   i. El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo.
   ii. Sea improbable, a través de medios técnicos, que el mensaje de datos puedaser derivado o reconstruido a partir del código de verificación producido por elalgoritmo.
   iii. Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

g) **IBMETRO:** El Instituto Boliviano de Metrología (IBMETRO) es la entidad del Estado Plurinacional de Bolivia que custodia los patrones nacionales de medición y es la referencia para las mediciones, brindando trazabilidad al Sistema Internacional de Unidades (SI). Esta entidad es signataria del Acuerdo de Reconocimiento Mutuo (CIPM MRA) de la Oficina Internacional de Pesos y Medidas (BIPM). El Tiempo Universal Coordinado (UTC) es generado por el BIPM, es una escala de tiempo que constituye la base para la difusión coordinada de frecuencias patrón y señales horarias, la realización física de la UTC, llamada UTC (k), es generada en los distintos Institutos Nacionales de Metrología u observatorios astronómicos nacionales que contribuyen con los datos de sus relojes atómicos al BIPM. IBMETRO forma parte de la red de tiempo del Sistema Interamericano de Metrología (SIM), reportando los datos de su reloj atómico con una periodicidad de 10 minutos, de esta manera se garantiza la trazabilidad permanente de la escala de tiempo UTC (IBMETRO).

h) **Listas de Certificados Revocados:** lista donde figuran las relaciones de certificados revocados o suspendidos.

i) **Módulo Criptográfico Hardware:** módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

j) **Política de Sellado de Tiempo:** Establece las normas y condiciones generales de los servicios de Sellado de Tiempo.

k) **Servicio de Sellado de Tiempo:** Servicio de una TSA que permite probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces generando un sello de tiempo con el resumen, la fecha y la hora. Dicho instante será obtenido por una fuente de tiempo segura determinada por la ATT.

l) **Terceros aceptantes.-** Son las personas naturales o jurídicas que confían y hacen uso de los sellos de tiempo emitidos por una TSA autorizado por la ATT.

m) **Tiempo:** Magnitud física que permite ordenar la secuencia de los sucesos, estableciendo un pasado, un presente y un futuro, y cuya unidad en el sistema internacional es el segundo.

n) **Unidad de Sellado de Tiempo – TSU:** Es el conjunto de hardware y software que es gestionado como una unidad y que emite el sello de tiempo firmado con una clave privada de la TSA.

o) **Usuario: Persona natural o jurídica:** que utiliza el servicio de sellado de tiempo de una Entidad Certificadora Autorizada compatible con el estándar RFC-3161.

DIRECTOR EJECUTIVO N° P. P.M.S. A.T.T.

DIRECCIÓN JURÍDICA V°B° A.T.T.

DIRECCIÓN JURÍDICA V°B° N.T.P.B.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

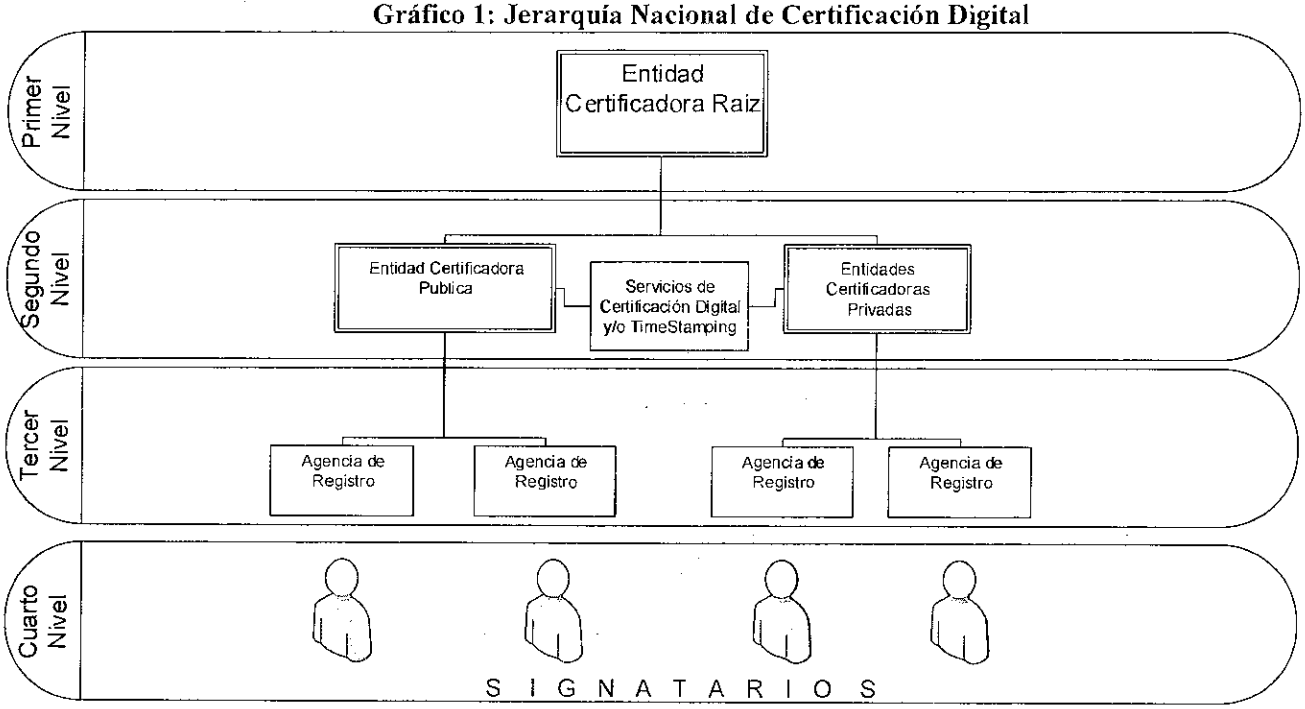
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

Capítulo II
Servicio de Sellado de Tiempo

Artículo 6 (Jerarquía).-

I. Conforme a la organización de la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia, la ATT es la Entidad Certificadora Raíz, que autoriza a las Entidades Certificadoras Autorizadas, tanto pública como privadas a brindar los servicios de certificación digital. Dentro de éstos servicios está el de Sellado de Tie

Gráfico 1: Jerarquía Nacional de Certificación Digital



Fuente: Elaboración propia a partir del Decreto Supremo N° 1793 del 13 de noviembre de 2013.

II. El sellado de tiempo es un tipo de firma digital que consiste en un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo, es verificable y sólo puede generarse por prestadores de servicio reconocidos, con políticas definidas y asegurando una precisión determinada y fiabilidad en los datos generados. El hecho de que la hora sea proporcionada por un sistema certificado, independiente y ajeno al procedimiento ofrece garantías de imparcialidad ante un posible litigio.

III. A una Entidad Certificadora Autorizada que brinde los servicios de Sellado de Tiempo también se le denominará Autoridad de Sellado de Tiempo (TSA).

Artículo 7 (Claves privadas de una TSA).- Para que la TSA brinde el Servicio de Sellado de Tiempo deberá tomar en cuenta las siguientes consideraciones:

a) La TSA deberá firmar digitalmente cada Sello de Tiempo con una clave privada reservada específicamente para ese propósito.
b) La TSA puede tener varias TSU cada una con sus propias claves privadas para diferentes propósitos

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

de sellado de tiempo, cada una de estas debe tener claramente identificada su Política de Sellado de Tiempo.

Articulo 8 (Consideraciones de uso).- El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la Autoridad de Sellado de Tiempo (TSA). Para efectos del servicio de sellado de tiempo se prestará tomando como referencia el uso horario GMT -4 Hora Boliviana.

Articulo 9 (Obtención de la referencia de tiempo fiable).-

I. La TSA deberá realizar la sincronización de su escala de tiempo con IBMETRO mediante el protocolo NTP a través de Internet.
II. En caso de contingencias la TSA podrá recurrir a una fuente secundaria reconocida por IBMETRO.

Capítulo III
Requisitos y Condiciones de Autorización para que una ECA brinde servicios de Sellado de Tiempo

Articulo 10 (Autorización del servicio).- Las entidades de certificación autorizadas podrán prestar servicios de sellado de tiempo como parte de sus servicios previa solicitud a la ATT y cumplimiento de los requisitos establecidos en esta sección.

Artículo 11 (Requisitos económicos para laTSA Pública).-

Los requisitos económicos para la prestación de servicios de Sellado de Tiempo son los siguientes:

I. Plan de negocio proyectado para un período de cinco (5) años, vinculados a la autorización solicitada que contenga además el programa de inversiones generales a efectuar.
II. Boleta de Garantía de Cumplimiento de Contrato, por el siete por ciento (7%) de sus ingresos brutos sobre sus proyecciones para el primer año, que respalde su actividad durante la vigencia de la autorización para la prestación de servicios de sellado de tiempo de acuerdo al artículo 45 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
III. La TSA deberá pagar por adelantado a la ATT el uno por ciento (1%) de sus ingresos brutos de operación del servicio de sellado de tiempo, como Tasa de Fiscalización y Regulación, en base a la proyección de sus ingresos brutos de acuerdo al artículo 38 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
IV. Presentación de su estructura tarifaria a la ATT para su aprobación y registro de acuerdo al artículo 42 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto Supremo N° 1793.

Artículo 12 (Requisitos económicos para una TSA Privada.).-

Los requisitos económicos para la prestación de servicios de Sellado de Tiempo son los siguientes:

I. Plan de negocio proyectado para un período de cinco (5) años, vinculados a la autorización solicitada que contenga además el programa de inversiones generales a efectuar.
II. Boleta de Garantía de Cumplimiento de Contrato, por el siete por ciento (7%) de sus ingresos brutos sobre sus proyecciones para el primer año, que respalde su actividad durante la vigencia de la autorización para la prestación de servicios de sellado de tiempo de acuerdo al artículo 45 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.
III. La TSA deberá rendir una caución por medio de una póliza de seguros expedida por una Entidad de Seguros debidamente establecida en el Estado Plurinacional de Bolivia. El monto será fijado por la ATT

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

anualmente.

IV. La TSA deberá pagar por adelantado a la ATT el uno por ciento (1%) de sus ingresos brutos de operación del servicio de sellado de tiempo, como Tasa de Fiscalización y Regulación, en base a la proyección de sus ingresos brutos de acuerdo al artículo 38 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto supremo N° 1793.

V. Presentación de su estructura tarifaria a la ATT para su aprobación y registro de acuerdo al artículo 42 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto Supremo N° 1793.

Artículo 13 (Requisitos técnicos para las TSA).-

Los requisitos técnicos que deben presentar para la prestación de servicios de Sellado de Tiempo son los siguientes:

I. Descripción de servicios prestados incluyendo duración y alcance de los mismos.
II. Políticas de Sellado de Tiempo que deberán ser presentadas a la ATT para su aprobación.
III. Declaración de Prácticas de Sellado de Tiempoque deberá ser presentada a la ATT para su aprobación.
IV. Infraestructura tecnológica: describir detalladamente la plataforma tecnológica incluyendo un detalle pormenorizado de hardware, software, dispositivos de comunicación y seguridad con los que cuenta, sus características y funcionalidad.
V. La clave privada del certificado de firma de cada sello de tiempo deberá ser resguardada durante su uso dentro de un módulo de hardware criptográfico con certificación FIPS 140-2 nivel 3 al igual que las copias de seguridad, toda esta información deberá estar especificada en su Política de Sellado de Tiempo
VI. La TSA deberá contar un sistema de información permanente y actualizada de acceso libre vía web con la siguiente información:
    a) Condiciones y términos de uso del sellado de tiempo para sus usuarios.
    b) Información de las diferentes TSU de sellos de tiempo que dispongan.
    c) Acceso a la información de estado o revocación.
    d) Acceso a los documentos públicos de la TSA.
    e) Procedimientos de reclamos.
    f) Tarifas y servicios aprobados por la ATT.
    g) Domicilio legal, teléfonos y correo electrónico de contacto.
VII. Modelo de Contrato tipo con suscriptores (Anexo 3).
VIII. Términos y condiciones de servicio con los suscriptores (Anexo 4).
IX. Contrato de servicios de tercerización (Si corresponde).
X. Política de Operación y Gestión de la TSA de acuerdo al punto 7.4 del RFC-3628 y que deberá estar conforme a la norma ETSI TS 102 023 v1.2.2.

Artículo 14 (Obligaciones de la TSA con la ATT).- Dentro de las obligaciones de la TSA en la Infraestructura de Clave Pública del Estado Plurinacional de Bolivia están:

I. Emitir sellos de tiempo de acuerdo a la información proporcionada en sus Políticas de Sellado de Tiempo y Declaración de Prácticas de Sellado de tiempo específicas para cada TSU.
II. Monitorear a la fuente confiable de tiempo para mantener un margen de desviación de 500 milisegundosen la precisión de hora en el momento de brindar los servicios de Sellado de Tiempo.
III. Cumplir con el contrato y términos y condiciones realizados con sus usuarios.
IV. Permitir y facilitar la realización de auditorías técnicas por parte de la ATT.
V. Mantener una comunicación segura y constante con el servidor NTP de IBMETRO.
VI. Hacer públicas sus Políticas de Sellado de Tiempo y Declaraciones de Prácticasde Sellado de Tiempo por cada TSU.
VII. Brindar el servicio de sellado de tiempo de acuerdo a los estándares establecidos en el presente

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

reglamento.

VIII. Conservar física y/o digitalmente la documentación que respalda la prestación del servicio de sellado de tiempo y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.

IX. Advertir, sobre las medidas de seguridad que deben observar los usuarios del servicio de sellado de tiempo.

Artículo 15 (Obligaciones de la TSA con sus usuarios).- Dentro de las obligaciones de la TSA en la Infraestructura de Clave Pública del Estado Plurinacional de Bolivia están:

I. Emitir cada sello de tiempo a partir de que se reciba una solicitud válida de un usuario de la TSA.
II. Cada sello de tiempo deberá tener un número único de serie.
III. Cada sello de tiempo generado deberá tener un identificador que indique la política de sellado de tiempo bajo la cual fue creado.
IV. Notificar oportunamente a sus usuarios en caso de interrupciones del servicio debido a mantenimiento planificado con antelación utilizando los medios de difusión disponibles de acuerdo al contrato de autorización de servicios como ECA suscrito con la ATT.
V. Firmar digitalmente cada sello de tiempo.
VI. Guardar la confidencialidad debida de los datos personales relacionados a los sellos de tiempo generados.
VII. Definir la disponibilidad para el acceso a los servicios de sellado de tiempo que proporciona a sus usuarios, establecidos en el parágrafo IV del artículo 15 del presente reglamento.
VIII. Publicar y comunicar por su página web a sus usuarios, en caso de que un certificado digital que se utilice para alguna TSU sea revocado.

Articulo 16 (Terceros aceptantes).- Para verificar la confiabilidad de un sello de tiempo, los terceros aceptantes deberán verificar si el certificado digital utilizado estuvo vigente y no revocado en la fecha en la que se realizó la firma, así como si el certificado utilizado ha sido emitido por la Entidad Certificadora Raíz. Además, deberá verificar las limitaciones de uso establecidas en la Política de Sellado de Tiempo.

Capítulo IV
Otros Aspectos

Articulo 17 (Incumplimiento).-El incumplimiento a cualquier disposición del mismo implica una infracción de acuerdo a los alcances del Reglamento de Sanciones vigente.

Articulo 18 (Modificaciones al estándar técnico).- El presente estándar está sujeto a modificaciones de acuerdo al artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo Nº 1793.

Articulo 19 (Proceso de Autorización del Servicio).- El Proceso de Autorización para que una Entidad Certificadora Autorizada brinde el servicio de Sellado de Tiempo se realizara de acuerdo al Procedimiento de Autorización aprobado con la RAR ATT-DJ-RA TL LP 32/2015.

DIRECTOR EJECUTIVO V°B° R.R.M.S. A.T.T.

DIRECCIÓN JURÍDICA V°B° N.R.B.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

ANEXO 1: FORMATO DEL CERTIFICADO DIGITAL DE LA AUTORIDAD DE SELLADO DE TIEMPO

1. Formato para el Certificado Digital de la Autoridad de Sellado de Tiempo

El formato de los Tipos de Certificados Digitales debe seguir los lineamientos del Estándar ITU X.509 en todos los aspectos relativos al formato, codificación, contenidos e interpretación. Se adhiere en consiguiente al RFC 5280 y el RFC 3161.

El certificado correspondiente deberá contener sólo una instancia para el campo extendido extendedKeyUsage como se define en el [RFC 2459] Sección 4.2.1.13 con los valores que debe tener KeyPurposeId:
id-kp-timeStamping. Esta extensión debe ser crítica
El siguiente identificador de objeto identifica los valores KeyPurposeID que puede tener id-kp-timeStamping
id-kp-timeStamping OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp (3) timestamping (8)}

i. El formato para el Certificado Digital para cada TSU tendrá los siguientes atributos y contenidos:

a) Versión (version): v3.
b) Número de Serie (serialNumber): Número asignado por la ECR.
c) Algoritmo de firmas (signatureAlgorithm): OID: 1.2.840.113549.1.15 (SHA256withRSA).
d) Nombre del Emisor (issuer): CN = Entidad Certificadora Raíz de Bolivia; O =ATT; C = BO de acuerdo a ISO3166.
e) Periodo de validez (validity): Fecha de emisión del Certificado, Fecha de caducidad del Certificado (YYMMDDHHMMSSZ, formato UTC Time).
f) Nombre suscriptor (subject): CN ="Autoridad de Sellado de Tiempo" y el nombre de la ECA; O = Razón social de la ECA; C = BO de acuerdo a ISO3166.
g) Clave pública del suscriptor (subjectPublicKey): Algoritmo: RSA, Longitud: 2048 bits.

ii. Las extensiones del Certificado Digital de una ECA serán las siguientes:

a) Identificador de la clave de la Autoridad Certificadora (authorityKeyIdentifier): Valor en la extensión subjectKeyIdentifier del Certificado de la EC raíz.
b) Identificador de la clave del suscriptor (subjectKeyIdentifier): Función HASH (SHA 256) del atributo subjectPublicKey.
c) Uso de Claves (keyUsage): digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 0, dataEncipherment = 0, keyAgreement = 0, keyCertSign = 0, cRLSign = 0, encipherOnly = 0, decipherOnly = 0.
d) Política de Certificación (certificatePolicies): URI: (archivo en formato de texto).
e) Restricciones Básicas (basicConstraints): CA = FALSE
f) Uso de Claves Extendida (extKeyUsage) critical: id-kp-timeStamping
g) Punto de distribución de las CRL (cRLDistributionPoints): URI: (.crl).
h) Información de Acceso de la ECA (authorityInformationAccess): URI: (.crt).

El servicio de Sellado de Tiempo mínimamente debe ser accesible vía http, https y la TSA publicara una dirección (URL) y/o un puerto en internet.

DIRECTOR EJECUTIVO P.M.S. A.T.T.

DIRECCIÓN JURÍDICA V°B° A.T.T.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

2. Formato del Sellado de Tiempo

2.1. Formato ASN.1

En el estándar RFC 3161 se define el formato para la solicitud y el sello de tiempo codificado en la norma ASN.1, norma para codificar datos de forma que su representación sea independiente de la máquina y el lenguaje de programación con la que se esté ejecutando.

2.1.1 Proceso de petición (TimeStampRequest)

Las solicitudes de sellos son realizadas por los usuarios siguiendo el formato especificado en la RFC 3161 en el punto 2.4.1.

TimeStampReq ::= SEQUENCE {

Campo	Valor	Descripción
version	INTEGER { v1(1) },	Número de la versión de la sintaxis utilizada. La actual es 1 (v1)
messageImprint	MessageImprint,	OID del algoritmo hash y el valor del hash de los datos. Se detalla en el cuadro siguiente.
reqPolicy	TSAPolicyId OPTIONAL,	OID de la política de la TSU Indica a la TSU la política bajo la cuál quiere que se proporcione el sello
Nonce	INTEGER OPTIONAL,	Si se incluye el nonce permite al cliente comprobar el retardo en la respuesta cuando no se dispone de reloj local. La respuesta debe contener este mismo número o se rechazará.
CertReq	BOOLEAN DEFAULT FALSE,	Si el campo certReq está presente y con valor true, la clave pública de la TSA debe estar referenciada por el identificador ESSCertID dentro de un atributo SigningCertificate en la respuesta debe ser provista por la TSA en el campo SignedData. Ese campo además puede contener otros certificados. Si falta el campo certReq o tiene valor false entonces, el campo SigningCertificate de la estructura SignedData no debe aparecer en la respuesta.
extensions	[0] IMPLICIT Extensions OPTIONAL	Es una forma de permitir añadir nuevos campos en el futuro. Si se incluye algún campo de extensión que la TSA no reconozca, ésta devolverá un mensaje de error de extensión no aceptada (unacceptedExtension). Más información en: RFC 2459

MessageImprint ::= SEQUENCE

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

Campo	Valor	Descripción
hashAlgorithm	AlgorithmIdentifier,	OID del algoritmo hash: El algoritmo de hash indicado en hashAlgorithm debería ser uno conocido por la TSA. También comprobará que sea suficientemente fuerte. Si la TSA no reconoce el algoritmo usado o piensa que es débil, entonces la TSA denegará el servicio al cliente devolviendo un pkiStatusInfo de 'bad_alg'.
hashedMessage	OCTET STRING	Este campo contiene el hash de los datos que se quiere sellar. La longitud del hash tiene que coincidir con la longitud de hash del algoritmo utilizado

El mensaje TimestampRequest no identifica al cliente, y esta información no es validada por la TSA en el momento del Sello de Tiempo. La TSA utilizara un mecanismo alternativo de identificación o autenticación.

2.1.2. Proceso de sellado (Timestamp Response)

La respuesta con el sello de tiempo tiene el formato especificado en la RFC 3161 en el punto 2.4.2.

TimeStampResp ::= SEQUENCE {

Campo	Valor	Descripción
status	PKIStatusInfo,	Estado de la respuesta. Ver sección 3.2.3 del RFC 2510. Se describe en el siguiente cuadro.
timeStampToken	TimeStampToken OPTIONAL	Este campo que contiene el sello de tiempo generado. Es una estructura ContentInfo que encapsula información firmada en una estructura TSTInfo. Está definida en la RFC 2630.

PKIStatusInfo ::= SEQUENCE {

Campo		Descripción
status	PKIStatus,	Estado de la respuesta. • **granted(0):** Marca de tiempo presente. • **grantedWithMods(1):** Sello de tiempo presente con modificaciones. • **rejection(2):** Petición rechazada • **waiting(3):** Esperando • **revocationWarning(4) :** Advertencia de revocación inminente • **revocationNotification (5):** Notificación de revocación

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

statusString	PKIFreeText OPTIONAL,	Se usa para indicar eventos de error
failInfo	PKIFailureInfo OPTIONAL	Causas del fallo: • **badAlg(0)**: Identificador de algoritmo no soportado • **badRequest(2)**: Transacción no permitida o soportada • **badDataFormat(5)**: Datos enviados con formato incorrecto • **timeNotAvailable(14)**: Origen de tiempo no disponible • **unacceptedPolicy(15)**: Política solicitada no soportada • **unacceptedExtension(16)**: Extensión no soportada • **addInfoNotAvailable(17)**: Información adicional no disponible • **systemFailure(25)**: Error del sistema

TSTInfo ::= SEQUENCE{

Campo	Valor	Descripción
version	INTEGER { v1(1) },	Versión de la respuesta TimeStamp (v1)
policy	TSAPolicyId,	OID de la política de la TSU Indica la política de la TSU bajo la cual se proporciona el sello, si se ha generado el sello, debe ser igual al del mensaje de petición
messageImprint	MessageImprint,	OID del algoritmo hash y el valor del hash de los datos. Debe tener el mismo valor que el campo correspondiente de la petición.
serialNumber	INTEGER,	Es un valor entero asignado por la TSA y debe ser único para cada sello que Genere cada TSU. Por tanto, un sello será identificado por el nombre de la TSU que lo generò y el número este valor asignado. Permite hasta 160 bits
genTime	GeneralizedTime	Es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala GMT -4, hora boliviana para evitar confusiones con las horas

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

		locales.

accuracy	Accuracy OPTIONAL,	Representa la desviación del tiempo UTC contenido en genTime, en los casos que sea necesario, proporciona una precisión incluso de microsegundos:
		Accuracy ::= SEQUENCE {
		seconds [1] Integer OPTIONAL,
		millis [2] Integer (1..999) OPTIONAL,
		micros [3] Integer (1..999) OPTIONAL,
		}
		Cuando este campo no está presente la precisión puede obtener a través de otros métodos, por ejemplo TSAPolicyId.

ordering	BOOLEAN DEFAULT FALSE,	Si falta el campo ordering o está presente y tiene valor false, entonces el campogenTime solo indica el momento en el que la marca de tiempo ha sido creada por la TSA. En este caso, el orden de la marcas de tiempo emitidas por una misma TSA o distintas TSAs solo es posible cuando la diferencia entre el genTime de la primera marca de tiempo es mayor que la suma de las precisiones del genTime de cada marca de tiempo.
nonce	INTEGER OPTIONAL,	El nonce es un número aleatorio con una elevada probabilidad de que el cliente lo genere una única vez (entero de 64 bits). Debe tener el mismo valor que el campo correspondiente de la petición.
tsa	[0] GeneralName OPTIONAL,	Identificador de la TSA definido en el Certificado ESSCertIDAttribute)
extensions	[1] IMPLICIT Extensions OPTIONAL	Es una forma de permitir añadir nuevos campos en el futuro. Las extensiones están definidas en la RFC 2459

2.1.3. Solicitud de verificación

La entidad que recibe la petición TimeStamp Response, debe validarla y extraer los datos necesarios para su almacenamiento.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

ValidateRequest:: SEQUENCE {

Campo	Valor	Descripción
version	INTEGER { v1(0) },	Número de la versión de la sintaxis utilizada. La actual es 1 (v1)
tst	TimeStampToken	Sello de tiempo a verificar
requestID	0 OCTET STRING OPTIONAL	Identificador que se utiliza para vincular una petición con su respuesta.

2.1.4. Respuesta de verificación

La TSA envía el mensaje como respuesta a una petición de verificación.

ValidateReply:: = SEQUENCE {

Campo	Valor	Descripción
version	INTEGER { v1(0) },	Número de la versión de la sintaxis utilizada. La actual es 1 (v1)
Status	PKIStatusInfo,	Toma los valores descritos en la tabla de respuesta.
tst	TimeStampToken	Sello de tiempo a verificar.
requestID	0 OCTET STRING OPTIONAL	Identificador que se utiliza para vincular una petición con su respuesta.

2.2. Formato XML

XML TimestampingProfile de la OASIS Digital SignatureServices (DSS) ver 1.0. especifica el intercambio de mensajes en la generación, validación y resellado de sellos de tiempo, este formato permite que se puedan definir los servicios de sellado de tiempo como web services.

Un sello de tiempo en XML tiene el siguiente formato:

```
<dss:timestampxmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
        <ds:signaturexmlns:ds=http://www.w3.org/2000/09/xmldsig# Id="Id-b898">
        <ds:SignedInfo Id="Id-45d6cc1d-960a-4185-b80b-38f205cb 1bae">
        <ds:canonicalizationMethodAlgorithm=http://www.w3.org/2001/10/xml-exc-
                c14n#WithComments/>
      <ds:SignatureMethod Algorithm="http://www.w3org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference Id="Id-bed8bc1e-47be-4813-ba42-972712edc9fb">
      <ds:DigestMethod Algorithm=http://www.w3.org/2000/09/xmldsig#sha 1>
      <ds:DigestValue> NAXrr45K011fbNBATVDQH4OBc6U=</ds:DigestValue>
      </ds:Reference>
      <ds:ReferenceId="Id-771"Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken"
      URI="#TSTInfo-Id-c57f7f58-9712-4a55-821c-4334d75ab100">
```


LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

```
<ds:Transforms>
<ds:Transform Algorithm=http://www.w3.org/2001/10/xml-exc-c14n#/>
</ds:Transforms>
<ds:DigestMethod Algorithm=http://www.w3.org/2000/09/xmldsig#sha1/>
<ds:Digestvalue>IU8FzVDfK7AhkDb0TphMypNyeDY=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>gYxon9Qr..=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MII..c=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
<ds:Object Id="TSTInfo-Id-c57f7f58-9712-4ª55-821c-4334d75ab100"MimeType="application/xml">
<dss:TstInfo>
<dss:SerialNumber>600806</dss:SerialNumber>
<dss:CreationTime>2010-09-28T08:49:02.312+02:00</dss:CreationTime>
  <dss:Policy>urn:oid:1.2.3.4.5.6.7</dssPolicy>
  <dss:ErrorBound>PT1.001001S</dss:ErrorBound>
  <dss:Ordered>true<7dss:Ordered>
  <dss:TSAFormat="urn:oasis:names:tc:SAML:1:nameidnameidformat:X509SubjectName">CN=TSA
Pruebas SEvillaOU=SteriaO=SteriaO=Sevilla</dss:TSA>
</dss:TstInfo>
  </ds:Object>
</ds:Signature>
</dss:Timestamp>
```


DIRECTOR EJECUTIVO V° B° R.J.M.S. A.T.T.

DIRECCIÓN JURÍDICA V° B° J.C.C. A.T.T.

DIRECCIÓN JURÍDICA V° B° N.F.P.B.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772268 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

ANEXO 2: FUENTE DE TIEMPO FIABLE Y ESTANDAR APLICABLE EN LA REPRESENTACION DE LAS FECHAS Y HORAS.

1.- Fuente de tiempo Fiable

En las recomendaciones de la RFC 3628 que se especifica los requerimientos que deben tener todas las autoridades de sellado de tiempo, se indica que el sistema deberá contar con una fuente de tiempo fiable, sin especificar el mecanismo por el cual se obtiene dicho valor del tiempo, la exactitud mínima que se debe garantizar o qué mecanismos han de utilizarse para garantizar la integridad del servicio.

Para el caso del Estado Plurinacional de Bolivia la TSA deberá proporcionar los valores asignados al tiempo del día y la fecha con base a la sincronización de su escala de tiempo con la del Instituto Boliviano de Metrología (IBMETRO) mediante el Protocolo NTP a través de Internet cumpliendo las recomendaciones de la RFC 1305 Network Time Protocol.

IBMETRO es signatario del Acuerdo de Reconocimiento Mutuo (CIPM MRA) de la Oficina Internacional de Pesos y Medida (BIPM). El tiempo Universal Coordinado (UTC) es generado por el BIPM, es una escala de tiempo que constituye la base para la difusión coordinada de frecuencias patrón y señales horarias, la realización física de la UTC, llamada UTC (k), es generada en los distintos Institutos Nacionales de Metrología u observatorios astronómicos nacionales que contribuyen con los datos de sus relojes atómicos al BIPM.

Los valores asignados al tiempo del día y la fecha no tienen en cuenta ni aplican en ningún caso los valores que el sistema informático del solicitante del servicio de sellado de tiempo señale. Ni el solicitante de los servicios de sellado de tiempo, ni ningún tercero pueden cambiar o solicitar la aplicación de valores distintos de tiempo del día y fecha.

La TSA deberá adoptar las siguientes medidas en la sincronización de su reloj con IBMETRO:

a) La sincronización de los relojes será monitoreada y mantenida de modo que no se desvíen de la exactitud declarada, con el fin de detectar y corregir cualquier desviación.
b) Cuando un cambio en el tiempo sea notificado por una autoridad competente, los respectivos cambios serán realizados el último minuto del día cuando el cambio en el tiempo haya sido planificado para ocurrir. En este escenario se mantendrá un registro del tiempo exacto (dentro de la exactitud declarada) y será notificado a los terceros que confían mediante una publicación en la página web de la TSA o mediante correo electrónico a todos los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.
c) Cada tiempo incluido en el sello de tiempo será sincronizado con la GMT-4, hora boliviana, dentro de la exactitud de +/- 500milisegundo.
d) Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la exactitud indicada los sellos de tiempo no deben emitirse.
e) Los sistemas o aplicaciones implicadas en la provisión de un servicio público por vía electrónica se sincronizarán con el servidor NTP de IBMETRO, el cual está disciplinado a su reloj atómico.
f) A nivel interno la TSA deberá disponer de mecanismos de seguridad que evitan la manipulación física de sus sistemas.

2.- Estándar aplicable en la representación de las fechas y horas

La representación de la fecha y hora conjunta en el servicio de sellado de tiempo deberá estar acorde al estándar ISO 8601 *Data elements and interchangeformats — Informationinterchange — Representation of dates and times*, donde se establece que para representar una fecha y hora del día de manera conjunta se debe expresar con un formato concreto (básico o extendido), debe estar presente el señalador de hora 'T' y estar representado ya sea

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65
COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Pradn) Telf./Fax: 4-4581182 - 4-44581184 4-4581185
SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Turre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978
TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611
Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

en formato local o UTC.

No puede hacerse uso de las representaciones de precisión reducida en las fechas, ni mezclarse el formato básico con el extendido.

Algunos ejemplos de fecha y hora conjuntas (en negrilla las representaciones completas):

Hora local: **20071103T131805, 2007-11-03T13:18:05**, +0020071103T1318, +002007-11-03T13:18, 20071103T13,30 2007-11-03T13,30.

Hora UTC: **20071103T161805Z, 2007-11-03T16:18:05Z**, 20071103T16Z, 2007-11-03T16Z, +0020071103T161805,32Z, +002007-11-03T16:18:05,32Z.

V° B° DIRECTOR EJECUTIVO M.S. A.T.T.

DIRECCIÓN J.U. V° B° N.F.P.B.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-4581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

ANEXO 3: MODELO DE CONTRATO DE ADHESIÓN PARA LA PROVISIÓN DE SERVICIOS DE SELLADO DE TIEMPO

Conste por el tenor del presente Documento Privado, que los suscribientes acuerdan celebrar un Contrato para la PROVISIÓN DE SERVICIOS DE SELLADO DE TIEMPO, que con el reconocimiento de firmas y rubricas surtirá los mismos efectos de documento público, sujeto a las siguientes cláusulas:

PRIMERA (PARTES CONTRATANTES).- Intervienen en la suscripción del presente Contrato:

1.1.- EMPRESA/ECA....., representada (o) legalmente por..... por el Sr. (a) ..... en virtud al Poder Especial N° ...../..... de fecha de.....del ..... otorgado mediante Notaría de Fe Pública N° .....que para efectos de éste Contrato se denominará .....

(LLENAR EN CASO DE PERSONA NATURAL)

1.2.- El/la Señor/ra/ita . , C.I. N° , que en lo sucesivo se denominará USUARIO (A), cuyos datos personales se detallan en el Anexo de Solicitud de Provisión de Servicios, mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

(LLENAR EN CASO DE PERSONA JURIDICA)

1.3.- La Empresa ....., legalmente representada (o) por el Sr. (a)....., en virtud al Poder Especial ...../ de fecha .....de.....del....., otorgado ante la Notaría de Fe Pública N° ..... a cargo del Dr.(a) .....con C.I. con Matricula N°.....con NIT N° .....con Domicilio legal .....que en lo sucesivo se denominará ....., cuyos datos se detallan en el Anexo de Solicitud de Provisión de Servicios mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

SEGUNDA (ANTECEDENTES).- Descripción del (los) servicio (s) a prestar, usos del certificado y limitaciones.

TERCERA (OBJETO DEL CONTRATO)- Describir el objeto del Contrato del servicio y la no transferibilidad de las claves y el certificado digital.

CUARTA (TÉRMINOS Y CONDICIONES).- Establecer que el servicio a contratar se someterá a sus términos y condiciones, señalando que deben formar parte integrante, indivisible, e inseparable del presente Contrato para todos los efectos legales (debiendo realizar un breve resumen).

QUINTA (PLAZO DEL CONTRATO. VIGENCIA Y PRORROGA).- Establecer plazo, vigencia y prórroga y/o renovación del Contrato de acuerdo a la normativa establecida por el ente regulador.

SEXTA (PLAZOS PARA LA ENTREGA. HABILITACIÓN, SUSPENSION, REVOCACION Y VIGENCIA DEL SERVICIO).- Establecer y describir los plazos, costos y requisitos señalado en los términos y condiciones del servicio a contratar.

SÉPTIMA (TITULARIDAD).- Describir la titularidad del uso del servicio a contratar.

OCTAVA (ESTRUCTURA TARIFARIA).- Establecer estructura tarifaria según lo señalado en los términos y condiciones del servicio a contratar.

NOVENA (FACTURACIÓN Y COBRANZA).- Establece los plazos señalados en los términos y condiciones.

DÉCIMA (DERECHOS Y OBLIGACIONES).- Describir derechos y obligaciones según señala en los términos y condiciones.

- (DE LA USUARIA Y/O USUARIO)
- (DE LA ECA)

DÉCIMA SEGUNDA (EXENCIONES DE RESPONSABILIDAD).- Descripción para ECA, en consideración a los marcos legales aplicables, sobre el servicio, la responsabilidad civil y penal u otro que se considere pertinente. Causales y condiciones bajo las cuales deba efectuarse la Revocatoria.

DÉCIMA TERCERA (ATENCIÓN DE RECLAMOS).- Describir los procedimiento y sus plazos de acuerdo a la normativa regulatoria aplicable.

DIRECTOR EJECUTIVO V° B° A.T.T.

DIRECCIÓN JURÍDICA V° B° J.C.Z. A.T.T.

DIRECCIÓN JURÍDICA V° B° A.T.T.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

DÉCIMA CUARTA (SERVICIOS DE INFORMACIÓN Y ASISTENCIA).- Establecer, y detallar los horarios días de atención, teléfono(s) y dirección del mismo.
DÉCIMA QUINTA (DECLARACIÓN EXPRESA).- Relativo a la voluntad de las partes y considerando que no media presión para la firma del presente Contrato.
DÉCIMA SEXTA (INVIOLABILIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE LA USUARIA O USUARIO).- Establecer la manera de proteger la información proporcionada por la usuaria o usuario a la ECA.
DÉCIMA SÉPTIMA (RESOLUCIÓN Y RESCISIÓN DEL CONTRATO).- Describe, establece las formas y atribuciones de la disolución del Contrato.
DÉCIMA OCTAVA (INTEGRIDAD DEL CONTRATO).- Establece una breve descripción de los documentos que forman parte del presente Contrato, como formularios, documentos requeridos por la Entidad Certificadora los términos y condiciones del servicio ofrecido, entre otros, los mimos que deberán ser entregados al momento de la suscripción del contrato.
DÉCIMA NOVENA (CLÁUSULA DE INTERPRETACIÓN).-En caso de duda sobre la interpretación del presente Contrato, se aplicará lo más favorable al usuario o usuaria.
VIGÉSIMA (ACEPTACIÓN).- Describir la conformidad de la usuaria o usuario y la aceptación por parte de la Entidad Certificadora, debiendo entregarse copia del presente Contrato al usuario o usuaria en el momento de la suscripción del contrato.

DIRECTOR EJECUTIVO V° B° R.A.M.S. A.T.T.

DIRECCIÓN JURÍDICA V° B° J.C.Z. A.T.T.

DIRECCIÓN JURÍDICA V° B° A.T.T.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera
Telf.: 2772268 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso
Esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-44581184
4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio
Club Torre Sur Planta Baja Of. 2,
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito Nº 720 Primer Piso,
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-6000
www.att.gob.bo

ANEXO 4: CONTENIDO MÍNIMO DE LOS TÉRMINOS Y CONDICIONES DE LAS AUTORIDADES DE SELLADO DE TIEMPO

La redacción de los Términos y Condiciones por parte de la TSA deberá incluir aspectos propios del servicio de Sellado de Tiempo que el usuario deberá conocer para que no se vea perjudicado.

TÉRMINOS Y CONDICIONES PARA LA PROVISIÓN DE SERVICIOS DE SELLADO DE TIEMPO

Con carácter previo a la celebración de los términos y condiciones entre la Entidad Certificadora y el usuario, para la provisión de servicios de sellado de tiempo deberá tenerse en cuenta la normativa que regula esta materia, prevista tanto en la Ley N° 164/ 2011 como en el Decreto Supremo N° 1793 y normas complementarias.

1. DESCRIPCIÓN DEL SERVICIO Y ASPECTOS ASOCIADOS: La ECA deberá detallar de manera exhaustiva la descripción de los objetivos y servicios a brindar.

2. MODALIDADES DE PRESTACIÓN DEL SERVICIO: Describir por nombre de modalidad los servicios involucrados en el contrato.

3. REQUISITOS TÉCNICOS NECESARIOS PARA ACCEDER AL SERVICIO: La ECA proveedora de servicios debe establecer cuáles son los requisitos mínimos necesarios para acceder al servicio. Asimismo, debe informar a los usuarios de las variables técnicas que pueden afectar la prestación del servicio y las limitaciones de éste.

4. HABILITACIÓN Y PLAZO PARA LA PROVISIÓN DEL SERVICIO: La Entidad debe establecer plazos para la habilitación del servicio.

5. TARIFAS: En este caso la Entidad Certificadora deberán establecer las tarifas considerando criterios sustentados y orientados en costos del servicio de certificación digital, previa presentación y aprobación por parte de la ATT según lo establecido por el artículo 42 del Reglamento para el Desarrollo de las TIC aprobado mediante D.S. 1793 y publicadas en medios de comunicación escrita y en su página web.

6. DERECHOS Y OBLIGACIONES DEL USUARIO DEL SERVICIO DE SELLADO DE TIEMPO: Para la elaboración de este punto la ECA de servicios deberá listar y regirse a lo establecido por el artículo 54 y artículo 55 de la ley N° 164, y los artículos 52, 53, 54 y 55 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793 y en los "ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA QUE UNA ENTIDAD CERTIFICADORA AUTORIZADA BRINDE EL SERVICIO DE SELLADO DE TIEMPO".

8. DERECHOS Y OBLIGACIONES DE LA ECA: Para la elaboración de este punto la Entidad Certificante deberá listar y regirse a lo establecido por el artículo 58 y artículo 59 de la ley N° 164, y los artículos 43 al 46 y 56 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793 y en los "ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA QUE UNA ENTIDAD CERTIFICADORA AUTORIZADA BRINDE EL SERVICIO DE SELLADO DE TIEMPO".

9. DERECHOS Y OBLIGACIONES DE LA ECA, Y ANTE TERCEROS ACEPTANTES: Para la elaboración de este punto el operador o proveedor de servicios deberá listar y regirse a lo establecido en el artículo 44 del Reglamento para el Desarrollo de las TIC a la Ley N° 164 aprobado por D.S. 1793 y en los "ESTANDARES TECNICOS Y OTROS LINEAMIENTO ESTABLECIDOS PARA QUE UNA ENTIDAD CERTIFICADORA AUTORIZADA BRINDE EL SERVICIO DE SELLADO DE TIEMPO".

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercita N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

10. ATENCIÓN DE CONSULTAS, RECLAMACIONES Y EMERGENCIAS Y/O SERVICIOS DE INFORMACIÓN Y ASISTENCIA: Para la elaboración de este punto la ECA de servicios debe regirse a lo establecido en el Reglamento de la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial aprobado por D.S. 27172. El contratante tiene derecho a recibir por parte de la Entidad Certificadora, a través de la Oficina de Atención del Consumidor ODECO, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación del servicio.

13. MEDIDAS PARA SALVAGUARDAR LA INVIOLABILIDAD DE LAS TELECOMUNICACIONES Y PROTECCIÓN DE LA INFORMACIÓN: Para la elaboración de este punto la Entidad Certificante de servicios debe regirse a lo establecido por el artículo 56 de la ley N° 164 que establece la inviolabilidad y secreto de las comunicaciones.

14. CAMBIO O MODIFICACIONES EN LA LEY O REGLAMENTOS DE TELECOMUNICACIONES: Los términos y condiciones deben estar enmarcados en la Ley de Telecomunicaciones y sus Reglamentos vigentes. Cualquier modificación futura a estas disposiciones legales será de aplicación inmediata en lo concerniente a los términos y condiciones.

DIRECCIÓN JURÍDICA V° B° J.O.Z. A.T.T.

DIRECTOR EJECUTIVO V° B° R.J.M.S. A.T.T.

DIRECCIÓN JURÍDICA V° B°

DIRECCIÓN JURÍDICA V° B° R.P.B.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso
Esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-44581184
4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° anillo. calle 3, Gardenia Condominio
Club Torre Sur Planta Baja Of. 2,
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso,
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-6000
www.att.gob.bo

ANEXO 5: CONTENIDO MÍNIMO DE LAS POLÍTICAS DE SELLADO DE TIEMPO PARA UNA TSA

La política de sellado de tiempo deberá estar conforme a la norma del ETSI TS 102 023 v1.2.2 y a su especificación equivalente RFC-3628.

POLÍTICAS DE SELLADO DE TIEMPO

1. INTRODUCCIÓN
    1.1. OBJETO
2. DEFINICIONES Y ABREVIATURAS
    2.1. DEFINICIONES
    2.2. ABREVIATURAS
3. CONCEPTOS GENERALES
    3.1. SERVICIO DE SELLADO DE TIEMPO (TSS)
    3.2. AUTORIDAD DE SELLADO DE TIEMPO (TSA)
    3.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN
4. POLÍTICA DE SELLADO DE TIEMPO
    4.1. VISTA GENERAL
    4.2. IDENTIFICACIÓN DE LA POLÍTICA DE SELLADO DE TIEMPO
    4.3. APLICACIÓN DEL SELLADO DE TIEMPO
5. OBLIGACIONES Y RESPONSABILIDADES
    5.1. OBLIGACIONES DE LA TSA
    5.2. OBLIGACIONES DE LOS SUBSCRIPTORES
    5.3. OBLIGACIONES DE LOS TERCEROS QUE CONFIAN
    5.4. RESPONSABILIDAD FINANCIERA
6. REQUERIMIENTOS DE LA AUTORIDAD DE SELLADO DE TIEMPO
    6.1. PRÁCTICAS DE SELLADO DE TIEMPO
    6.2. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES
    6.3 GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO USADO PARA FIRMAR LOS SELLOS DE TIEMPO
    6.4. SELLADO DE TIEMPO
    6.5. OPERACIÓN Y GESTIÓNDE LATSA
    6.6. ESQUEMA ORGANIZATIVO
    6.7. REQUISITOS COMERCIALES Y LEGALES
        6.7.1. Tarifas
        6.7.2. Capacidad financiera
        6.7.3. Notificaciones
        6.7.4. Modificaciones Certificación
        6.7.5. Resolución de conflictos
7. AUDITORIA DE CONFORMIDAD
8. PERFILES DE CERTIFICADO, CRL Y OSCP.
9. ADMINISTRACIÓN DOCUMENTAL

DIRECCIÓN JURÍDICA V° B° J.O.Z. A.T.T.

DIRECTOR EJECUTIVO V° B° R.L.M.S. A.T.T.

DIRECCIÓN T. V° B° N.F.L.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera
Telf.: 2772266 - Fax: 2772299
Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso
Esq. España y La Paz (El Prado)
Telf./Fax: 4-4581182 - 4-44581184
4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio
Club Torre Sur Planta Baja Of. 2,
Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso,
Telf.: 4-6644136 - 4-6666484
Fax: 4-6112611

Línea Gratuita de Protección al Usuario
800-10-6000
www.att.gob.bo

ANEXO 6: CONTENIDO MÍNIMO DEL DOCUMENTO DE DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN PARA UNA AUTORIDAD DE SELLADO DE TIEMPO

La Declaración de Prácticas de Certificación deberá estar conforme a la norma del ETSI TS 102 023 v1.2.2 y a su especificación equivalente RFC-3628.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. INTRODUCCIÓN
    1.1. OBJETO
2. DEFINICIONES Y ABREVIATURAS
    2.1. DEFINICIONES
    2.2. ABREVIATURAS
3. CONCEPTOS GENERALES
    3.1. SERVICIO DE SELLADO DE TIEMPO (TSS)
    3.2. AUTORIDAD DE SELLADO DE TIEMPO (TSA)
    3.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN
        3.3.1. Subscriptores
        3.3.2. Terceros que confían
        3.3.3. Ámbito de aplicación
4. POLÍTICA DE SELLADO DE TIEMPO
    4.1. VISTA GENERAL
    4.2. IDENTIFICACIÓN DE LA POLÍTICA DE SELLADO DE TIEMPO
    4.3. APLICACIÓN DEL SELLADO DE TIEMPO
        4.3.1 Límites de uso
        4.3.2 Prohibiciones de uso
5. OBLIGACIONES Y RESPONSABILIDADES
    5.1. OBLIGACIONES DE LA TSA
        5.1.1. Obligaciones de la Autoridad de Sellado de Tiempo con la ECR
        5.1.2. Obligaciones de la Autoridad de Sellado de Tiempo hacia sus subscriptores
    5.2. OBLIGACIONES DE LOS SUBSCRIPTORES
    5.3. OBLIGACIONES DE LOS TERCEROS QUE CONFIAN
    5.4. RESPONSABILIDAD FINANCIERA
6. REQUERIMIENTOS DE LA AUTORIDAD DE SELLADO DE TIEMPO
    6.1. PRÁCTICAS DE SELLADO DE TIEMPO
        6.1.1. Prácticas de Sellado de Tiempo
    6.2. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES
        6.2.1. Generación de claves de la TSA
        6.2.2. Protección de la clave privada de la TSA
        6.2.3. Distribución de la clave pública de la TSA
        6.2.4. Regeneración de la clave de la TSA
        6.2.5. Destrucción de la clave privada de la TSA
        6.2.6. Gestión de los HSM
    6.3 GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO USADO PARA FIRMAR LOS SELLOS DE TIEMPO
    6.4. SELLADO DE TIEMPO
        6.4.1. Sellado de tiempo de acuerdo al punto 7.3 del RFC 3628.
        6.4.2. Sincronización del reloj con UTC de acuerdo al punto 7.3.2 del RFC 3628.
    6.5. OPERACIÓN Y GESTIÓNDE LATSA

DIRECTOR EJECUTIVO V°B° P.M.S.C. A.T.T.

DIRECCIÓN JURÍDICA V°B° A.T.T.

DIRECCIÓN JURÍDICA V°B° M.F.B.

LA PAZ: Calle 13 de Calacoto N° 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián N° 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4° y 5° aoillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O´Connor y Avenida Ejercito N° 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gnb.bo

DIRECTOR EJECUTIVO V° B° R.A.J.M. A.T.T.

DIRECCIÓN JURÍDICA V° B° R.E.P.B.

LA PAZ: Calle 13 de Calacoto Nº 8260 - 8280 Entre Av. Los Sauces y Av. Costanera Telf.: 2772266 - Fax: 2772299 Casilla: 6692 - Casilla: 65

COCHABAMBA: Avenida Ballivián Nº 683, Primer Piso Esq. España y La Paz (El Prado) Telf./Fax: 4-4581182 - 4-44581184 4-4581185

SANTA CRUZ: Avenida Beni, entre 4º y 5º anillo. calle 3, Gardenia Condominio Club Torre Sur Planta Baja Of. 2, Telf./Fax: 3-3120587 - 3-3120978

TARIJA: Calle Alejandro del Carpio entre calle O'Connor y Avenida Ejercito Nº 720 Primer Piso, Telf.: 4-6644136 - 4-6666484 Fax: 4-6112611

Línea Gratuita de Protección al Usuario 800-10-6000 www.att.gob.bo

CONTENIDO

DIRECCIÓN JURÍDICA V° B° A.T.T.

DIRECTOR EJECUTIVO V° B° R.R.M.S. A.T.T.

DIRECCIÓN JURÍDICA V° B° A.T.T.