



Finado Electrónicamente por
Gabriel Molina Sosa
en fecha 2012-02-13 10:36:02.449
Prima Superintendente

MODELO TECNICO PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO

NORMA SUSCERTE
N° 065-01/12

PÁGINA: 1 DE: 19
EDICIÓN N°: 1
FECHA: 01/2012

MODELO TECNICO PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO



Firma Superintendente

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Enero 2012

ÍNDICE

**MODELO TECNICO PARA LA PRESTACIÓN DEL
 SERVICIO DE ESTAMPADO DE TIEMPO**

Firma Superintendente

1. OBJETO Y CAMPO DE APLICACIÓN.....	5
2. REFERENCIAS NORMATIVAS.....	5
3. DEFINICIONES Y TERMINOLOGÍAS.....	5
4. SÍMBOLOS Y ABREVIATURAS.....	7
5. PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO.....	8
5.1. Principio Básico.....	8
5.2. Consideraciones Generales.....	8
5.3. Obligaciones para los PSET.....	9
6. MODELO JERARQUICO PARA EL SERVICIO DE ESTAMPADO DE TIEMPO.....	10
6.1. Principio Básico.....	10
6.2. Consideraciones Generales.....	10
6.3. Consideraciones Específicas.....	12
Tabla N° 1. Nomenclatura de campos del certificado del PSET.....	12
7. MODELO FUNCIONAL DEL SERVICIO DE ESTAMPADO DE TIEMPO.....	15
7.1. Principio Básico	15
7.2. Consideraciones.....	15
8. ANEXOS.....	19
8.1. Anexo 1.....	19

TRÁMITE



**MODELO TECNICO PARA LA PRESTACIÓN DEL
SERVICIO DE ESTAMPADO DE TIEMPO**

Firma Superintendente

NOMBRE	CARGO SUSCERTE
	Superintendente Superintendente Adjunto
	Director de Registro y Acreditación Directora de Inspección y Fiscalización Director de Investigación y Desarrollo Tecnológico Directora de la Oficina de Gestión Administrativa Asesora Legal

GRUPO DE TRABAJO:			COMISIÓN ESPECIAL:		
COORDINADOR:					
MIEMBROS PERMANENTES:			CARGO:		
NOMBRE	UNIDAD	CARGO	NOMBRE	ENTIDAD	CARGO

OBSERVACIONES	RESPONSABLE DE LA EDICIÓN
	COORDINADOR:
	FECHA: FIRMA:
	SUPERINTENDENTE:
	FECHA: FIRMA:
	APROBACIÓN APLICACIÓN EN:
	FECHA: FIRMA:

Firma Superintendente

1. OBJETO Y CAMPO DE APLICACIÓN

La presente norma consiste en regular y establecer los mecanismos y procedimientos técnicos para prestar el Servicio de Estampado de Tiempo en el Sistema Nacional de Certificación Electrónica de la República Bolivariana de Venezuela de conformidad con lo establecido en el Decreto con Fuerza de Ley N° 1204 Sobre Mensaje de Datos y Firmas Electrónicas en su artículo 34.

2. REFERENCIAS NORMATIVAS

2.1 Decreto 1.204 con Fuerza de Ley Sobre Mensaje de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero del 2001. (LSMDFE).

2.2 Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.086 del 14 de diciembre del 2004.

2.3 Norma 032-07/08. Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Lista de Certificados Revocados emitidas por SUSCERTE.

2.4 Norma 040-04/08. Guía de estándares tecnológicos y lineamientos de seguridad para la acreditación como PSC.

2.5 Norma 027-04/08. Guía para la acreditación de Proveedores de Servicios de Certificación.

2.6 Norma ISO 8601. Elementos de datos y formatos intercambiables — Intercambio de información Representación de fechas y horas . 3era Edición. Diciembre 2004.

2.7 RFC 1305. Protocolo de Tiempo en Redes (NTP).

2.8 RFC 3280. Internet X.509 Public Key Infrastructure Certificate. Abril 2002.

2.9 RFC 3161. Protocolo para el Estampado de tiempo (TSP).

2.10 RFC 3628. Requerimiento para las Autoridades de Estampado de Tiempo. Noviembre 2003.

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta norma, se establecen las siguientes definiciones y terminologías:

ACREDITACIÓN

Licencia que otorga la Superintendencia de servicios de Certificación Electrónica a las personas que expresan su voluntad de ser Proveedores de Servicios de Estampado de Tiempo, todo conforme a lo establecido en la LSMDFE y previo cumplimiento de los requisitos establecidos en la norma N° 064-01/12 referente a la Acreditación de Proveedores de Servicios de Estampado de Tiempo.

AUTORIDAD DE ESTAMPADO DE TIEMPO

Actúa como tercera parte de confianza quien certifica la existencia de unos datos electrónicos en una fecha y hora concreta.



Firma Superintendente

**CERTIFICADO
ELECTRÓNICO**

Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

**SUPERINTENDENCIA
DE SERVICIOS DE
CERTIFICACIÓN
ELECTRÓNICA
(SUSCERTE)**

Servicio Autónomo que pertenece al Ministerio del Poder Popular para la Ciencia y Tecnología, cuyo objeto es acreditar, supervisar y controlar, en los términos previstos en el Decreto-Ley 1.204 (LSMDFE) y su Reglamento Parcial, a los Proveedores de Servicios de Certificación de carácter público o privado.

HASH

Resultado de aplicar un algoritmo de hashing o resumen sobre un documento. Son funciones en un sólo sentido, es decir, conociendo el resultado es prácticamente imposible conocer el dato original.

**IDENTIFICADOR DE
OBJETO**

Valor universal único asociado a un objeto para identificarlo inequívocamente.

**OFICINA
INTERNACIONAL DE
PESOS Y MEDIDAS**

Coordinador mundial de Metrología situado en Francia, responsable de la generación del Tiempo Universal Coordinado (UTC). Su cometido es asegurar en todo el mundo la uniformidad de las mediciones y su trazabilidad al Sistema Internacional de Unidades.

**POLÍTICA DE
CERTIFICADOS**

Documento en el cual el Proveedor de Servicios de Estampado de Tiempo (PSET) acreditado, define las reglas a seguir para el uso de un Certificado Electrónico de Estampado de Tiempo, en una comunidad de signatarios o aplicación determinada y sus requerimientos de seguridad.

**PROVEEDOR DE
SERVICIOS DE
ESTAMPADO DE
TIEMPO**

Persona Jurídica, dedicada a proporcionar el Servicio de Estampado de Tiempo dentro de la República Bolivariana de Venezuela y demás actividades previstas en esta normativa.

**RELOJ MAESTRO DE
TIEMPO (TMC)**

Dispositivo de tiempo que de forma segura distribuye en red la hora exacta al Servicio de Estampado de Tiempo.

**ESTAMPADO DE
TIEMPO**

Documento electrónico emitido por un Proveedor de Estampado de Tiempo, que sirve como evidencia de que una información digital existió en una determinada fecha y hora en el pasado.

**SERVIDOR DE
ESTAMPADO DE
TIEMPO**

Servidor de red que criptográficamente emite tokens de tiempo asociado a un conjunto de datos electrónicos, los cuales son firmados electrónicamente.

SIGNATARIO

Persona titular de un Certificado Electrónico.

SOLICITANTE

Cualquier Persona Jurídica ó PSC Acreditado ante SUSCERTE.

**TIEMPO UNIVERSAL
COORDINADO (UTC)**

Escala del tiempo adoptada como el estándar de tiempo oficial internacional, utilizada para el sistema de Metrología internacional, convención del metro, determinada y distribuida por la BIPM.

Firma Superintendente

**FUENTE CONFIABLE
DE TIEMPO**

Organismo encargado de proveer la Hora Legal de Venezuela a los PSET.

INTEROPERABILIDAD

Habilidad de que diversos componentes de un sistema puedan compartir e intercambiar información.

**SERVICIO
REDUNDANTE**

Servicio implementado de manera que permitan brindar disponibilidad del mismo, aún en caso de fallo o desperfecto de algún componente del sistema.

TOKEN

Dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación y firma.

TOKEN DE TIEMPO

Objeto o cadena de caracteres que vincula una serie de datos a un momento determinado de tiempo, estableciendo así la evidencia de que esos datos existen desde cierto instante de tiempo.

**AUDITOR DE
ESTAMPADO DE
TIEMPO (AET)**

Equipo computarizado que permite asegurar que todos los elementos que intervienen en el proceso de Estampado de Tiempo están sincronizados con una fuente confiable, así como también, registrar todos los acontecimientos acaecidos en dicho proceso.

4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma, se establecen los siguientes símbolos y abreviaturas:

AC	Autoridad de Certificación
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas
AC Raíz	Autoridad de Certificación Raíz del Estado Venezolano
BIPM	Oficina internacional de pesos y medidas - Bureau International des Poids et Mesures
DPC	Declaración de Prácticas de Certificación
HLV	Hora Legal de Venezuela
OID	Identificador de Objeto
PC	Política de Certificados
PSC	Proveedor de Servicios de Certificación
PSET	Proveedor de Servicio de Estampado de Tiempo
RPLSMDFE	Reglamento Parcial de la Ley sobre Mensajes de Datos y Firmas Electrónicas
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica
TMC	Reloj Maestro de Tiempo - Time-Source Master Clock
TSA	Autoridad de Estampado de Tiempo – Time Stamping Authority
TSS	Servidor de Estampado de Tiempo - Time Stamping Server

Firma Superintendente

AET	Auditor de Estampado de Tiempo
SNTP	Servidor de Protocolo de Tiempo de Red
DIF	Dirección de Inspección y Fiscalización
DRA	Dirección de Registro y Acreditación
Stratum	Representa el nivel en que se encuentra un servidor local NTP, y viene representado por un entero de 8 bit.

5. PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO

5.1. Principio Básico

A través de la presente normativa, se establecen las regulaciones, mecanismos y procedimientos para la prestación del servicio de Estampado de Tiempo en el Sistema Nacional de Certificación Electrónica de la República Bolivariana de Venezuela.

5.2. Consideraciones Generales

- 5.2.1** El Servicio de Estampado de Tiempo es un servicio del Sistema Nacional de Certificación Electrónica de la República Bolivariana de Venezuela.
- 5.2.2** El Servicio de Estampado de Tiempo podrá ser prestado por cualquier Persona Jurídica (de carácter público o privado), debidamente acreditado ante SUSCERTE, una vez cumplido con los requisitos legales, técnicos y financieros.
- 5.2.3** Para todo trámite y gestión de carácter público y/o privado, que se contemple en el ordenamiento jurídico venezolano, el signatario podrá hacer uso del servicio de Estampado de Tiempo para fijar la hora legal.
- 5.2.4** SUSCERTE establecerá los procedimientos de monitoreo y auditoría de conformidad con el Servicio de Estampado de Tiempo de los PSET, a objeto de verificar la prestación del mismo, así como el cumplimiento de la presente normativa.
- 5.2.5** SUSCERTE obtendrá la Hora Legal de Venezuela (HLV) a partir de los servicios del organismo responsable de la administración de la HLV.
- 5.2.6** SUSCERTE, a los efectos del cumplimiento de la presente Normativa, será la Fuente Confiable de Tiempo para todo PSET acreditado.

Firma Superintendente

- 5.2.7** SUSCERTE como ente rector en la materia de estampado de tiempo, funcionará como Autoridad de Estampado de Tiempo y en este sentido definirá en su DPC las características de todo certificado electrónico utilizado para la prestación del Servicio de Estampado de Tiempo por parte de los PSET.
- 5.2.8** SUSCERTE como órgano rector de la materia y fuente confiable de tiempo, en pro de actualizar tecnológicamente la infraestructura para la prestación del Servicio de Estampado de Tiempo; podrá aceptar contribuciones, donaciones o aportes dirigidos a su mejora continua.
- 5.2.9** SUSCERTE, incorporará sistemas de monitoreo y auditoría para garantizar la sincronización confiable entre la HLV y los PSET, en los tiempos establecidos durante el proceso de Estampado de Tiempo, así como también registrar cualquier evento relacionado al mismo.
- 5.2.10** El uso del servicio de estampado de tiempo en el ámbito de la Infraestructura Nacional de Certificación Electrónica Venezolana es opcional. Por tanto, los documentos digitales firmados electrónicamente con la clave privada correspondiente a los Certificados Electrónicos emitidos dentro de dicha Infraestructura serán válidos con o sin el servicio de estampado de tiempo.

5.3. Obligaciones para los PSET

- 5.3.1** El PSET deberá solicitar la autorización debida y formalmente ante SUSCERTE, para realizar cualquier modificación en las condiciones del servicio, donde se vea afectado el signatario.
- 5.3.2** El PSET está en la obligación de garantizar el cumplimiento de los estándares y mejores prácticas internacionales en materia de estampado de tiempo, mencionadas en el Numeral dos (2) de la presente normativa.
- 5.3.3** El PSET debe garantizar una comunicación activa con los TMC o SNTP de SUSCERTE, a objeto de garantizar y mantener en todo momento la sincronización de la HLV tal como se describe en el apartado N° 7.
- 5.3.4** Todo PSET debe contar con una infraestructura de servicio redundante que permita asegurar como mínimo un 99% de operatividad anual.
- 5.3.5** Todo PSET debe disponer de un proceso de monitoreo constante de sus equipos,

Firma Superintendente

TSSs, con el fin de asegurar el sincronismo entre los TMC ó SNTP de SUSCERTE.

- 5.3.6** Todo PSET a fin de garantizar el proceso constante de auditoría y monitoreo, deberá de suministrar trimestralmente a SUSCERTE los registros logs o cualquier otra información necesaria, sobre los equipos que intervienen en el Servicio de Estampado de Tiempo de los PSET para garantizar el correcto funcionamiento de los Relojes y el Tiempo de Sincronización de los TSS.
- 5.3.7** En caso de que el PSET incurra en el incumplimiento de lo establecido en el marco legal y sug legal definido por SUSCERTE, será motivo para la apertura de un procedimiento administrativo para la revocación de la acreditación del PSET.
- 5.3.8** Todo PSET debe contar con una infraestructura de servicio que permita la interoperabilidad con los protocolos y tecnologías que para ese momento disponga SUSCERTE.
- 5.3.9** Los PSET son responsables de la emisión de los token de estampado de tiempo a sus signatarios, así como deben asegurar y dejar constancia del uso u objetivo de los token de tiempo que se generen y de la identidad de los usuarios responsables del mismo.

6. MODELO JERARQUICO PARA EL SERVICIO DE ESTAMPADO DE TIEMPO

6.1. Principio Básico

En esta norma se presenta la estructura jerárquica de la Infraestructura Nacional de Certificación Electrónica, empleada para la distribución de los campos en los Certificados Electrónicos de Estampado de Tiempo que serán emitidos para los PSET, así como para las DPC y Listas de Certificados Revocados, entre otros.

Firma Superintendente

6.2. Consideraciones Generales

- 6.2.1** Para la selección del modelo a implementar en el marco de la Infraestructura Nacional de Certificación Electrónica, se siguió el modelo jerárquico de una Autoridad de Certificación Raíz única nacional de la cual se desprenden dos ramas, la de los Proveedores de Servicios de Certificación Acreditados y la de los Casos Especiales, ubicándose el Servicio de Estampado de Tiempo dentro de esta última.
- 6.2.2** En la Figura N° 1 se establecen las relaciones de confianza basadas en la arquitectura jerárquica con una única raíz de la Infraestructura Nacional de Certificación Electrónica.
- 6.2.3** En la arquitectura jerárquica de la Infraestructura Nacional de Certificación Electrónica existe un nivel subordinado a la Autoridad Raíz, para los Casos Especiales, dentro del cual se constituirá la AC Estampado de Tiempo.

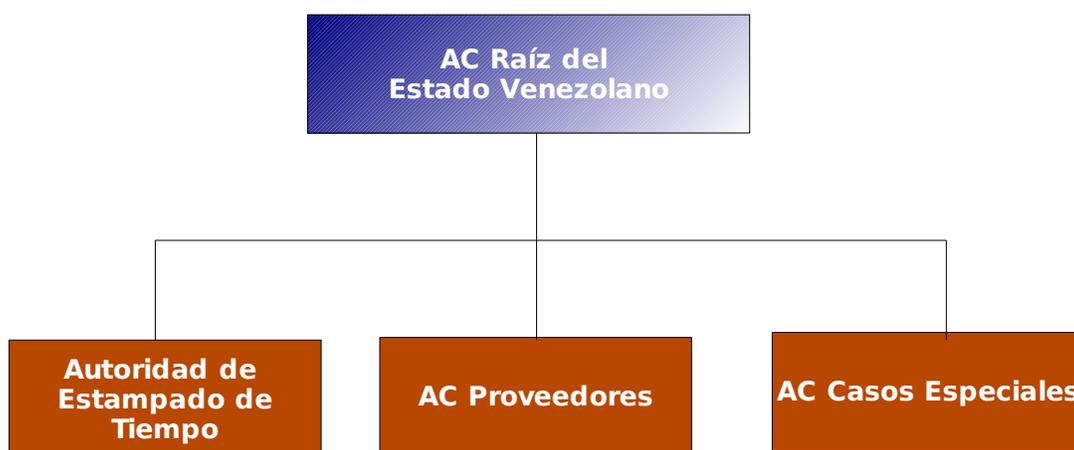


Fig. No 1. Arquitectura Jerárquica subordinada

- 6.2.4** La única que puede firmar el certificado de la AC Estampado de Tiempo es la AC Raíz, no existe otra AC que pueda realizar dicha operación.
- 6.2.5** La AC de Estampado de Tiempo luego de poseer el certificado firmado por la AC Raíz, firma con éste, los certificados electrónicos del Reloj de Tiempo Maestro, los TSSs que prestarán el servicio y la LCR que genere la mencionada AC.



Firma Superintendente

- 6.2.6** La AC Raíz no emite certificados a los signatarios, sólo emite el certificado de la AC Estampado de Tiempo. Por su parte, la AC de Estampado de Tiempo no emite certificados a los signatarios, sólo emite los certificados para los TSSs de los PSET.
- 6.2.7** El certificado electrónico utilizado por la AC Estampado de Tiempo se puede renovar tantas veces como se requiera y la tecnología lo permita. El tiempo de vida y tamaño mínimos requerido para los pares de claves de dicho certificado, de acuerdo a su tipo, son los establecidos en la DPC.
- 6.2.8** Los PSET sólo pueden gestionar certificados para TSSs ante SUSCERTE, donde dicho certificado será generado por la AC Estampado de Tiempo de la mencionada Superintendencia.

6.3. Consideraciones Específicas

- 6.3.1** La estructura de campos del certificado electrónico de la TSA se especifican en la tabla número 1 y número 2 de éste documento.

Tabla N° 1. Nomenclatura de campos del certificado del PSET

Abreviatura	Significado	Corresponde a
CN	Common Name (nombre común)	Nombre de la persona natural o jurídica, servidor o aplicación
O	Organization Name (nombre de la organización)	Nombre de la organización relacionada con el CN
OU	Organizational Unit (unidad organizacional)	Nombre de la unidad organizacional relacionada con el CN
C	Country (país)	País
E	E-mail (correo electrónico)	Dirección de correo electrónico
L	Locality (localidad)	Localidad
ST	State (estado)	Estado o Provincia

Tabla N° 2. Estructura de campos del certificado del PSET

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC principal del PSC
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.



MODELO TECNICO PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO

Firma Superintendente

Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. El algoritmo de firma permitido es SHA256 withRSAEncryption.
--------------------------------	---

DATOS DEL EMISOR

CN	Identificación de la AC de Estampado de Tiempo
O	Sistema Nacional de Certificación Electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)

PERÍODO DE VALIDEZ (VALIDITY)

No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina

DATOS DEL TITULAR

CN	(Identificación del Servidor o Aplicación)
O	Nombre de la Organización
OU	Nombre de la Unidad Organizacional
C	País
E	(correo electrónico)
L	(Dirección)
ST	(Estado)

INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)

Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	2048 ó 4096 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de PSET
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: FALSE
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
Other Name	Other Name



MODELO TECNICO PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO

Firma Superintendente

N° de Identificación OID 2.16.862.2.2	RIF-G-20004036-0
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Digital Signature, Non Repudiation y Time Stamping
Nombre alternativo del titular (Subject Alternative Name)	
DNS Name	(nombre de dominio del PSET registrado en nic.ve)
Other Name	Other Name
OID 2.16.862.2.1	(Código de identificación del PSET acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-(RIF del PSET)
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR con SHA256 del PSET URL: http://acraiz.suscerte.gob.ve/lrc
Acceso a la Autoridad de Información (Authority Information Access)	Campo opconal URI:http://ocsp.suscerte.gob.ve
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC). URL:http://www.suscerte.gob.ve/dpc

Firma Superintendente

7. MODELO FUNCIONAL DEL SERVICIO DE ESTAMPADO DE TIEMPO

7.1. Principio Básico

En este apartado de la norma se presenta la estructura de funcionamiento del Servicio de Estampado de Tiempo en el marco de la Estructura Jerárquica para la Infraestructura Nacional de Certificación Electrónica. En la misma, se describen todos los procedimientos necesarios para la implantación del Servicio de Estampado de Tiempo así como las funciones de los elementos activos y pasivos que intervienen.

7.2. Consideraciones

- 7.2.1** El Servicio de Estampado de Tiempo se establece sobre el modelo funcional expresado en el Anexo N° 1 apartado N° 8.1, donde se señalan los equipos que intervienen en dicho modelo así como el nivel de ubicación, sus responsables y las conexiones que se deben establecer y mantener.
- 7.2.2** El lo que respecta a los *Stratum*, El servicio de Fuente Confiable de Tiempo para Estampado de Tiempo está constituido sobre una infraestructura compuesta por tres (3) niveles de *Stratum* reflejado en el Anexo 1, el *Stratum 0* se encuentra en el Observatorio Naval Cagigal que provee la HLV a través del Reloj Atómico; en el *Stratum 1*, figuran los equipos MCs de SUSCERTE que obtendrán la HLV del Observatorio Naval Cagigal, el *Stratum 2*, viene representada por los equipos NTP de SUSCERTE siendo para los PSET la fuente confiable de tiempo; además puede observarse en el Anexo 1 que se encuentra la TSA administrada por SUSCERTE, la cual se encargará de emitir todos los certificados electrónicos de los TSSs de los PSET en el proceso de Estampado de Tiempo; por último en el *Stratum 3* se encuentran los equipos NTP de los PSETs, donde estos una vez sincronizados con el servicio de fuente confiable de tiempo de SUSCERTE, suministrarán a sus TSS la fecha y hora legal, necesarios para generar los Tokens de estampado de tiempo a sus signatarios.
- 7.2.3** El funcionamiento del Servicio de Estampado de Tiempo y los protocolos de comunicación signatario-TSS seguirán lo establecido en el RFC 3161 con la actualización ESSCertIDv2 referente al Protocolo de Estampado de Tiempo (TSP).

Firma Superintendente

- 7.2.4** El Servicio de Estampado de Tiempo se establece sobre una red de sincronismo, donde SUSCERTE como órgano rector en la materia, obtiene la HLV del Observatorio Naval Cagigal asumiendo la figura de *Fuente Confiable de Tiempo* para el Servicio de Estampado de Tiempo.
- 7.2.5** SUSCERTE como Fuente de Tiempo provee la HLV a los PSET mediante la red de sincronismo mostrada en el Anexo N°1 apartado 8.1, donde se establece que los TSSs de los PSET deben sincronizar la hora con los NTPs dispuestos por SUSCERTE para tal fin.
- 7.2.6** La Red de sincronismo se establecerá mediante el uso de pulsos por segundo para la obtención de la HLV del Observatorio Naval Cagigal y del protocolo NTP para lograr la sincronización de los equipos TMCs y NTPs de SUSCERTE y TSSs de los PSET.
- 7.2.7** Para asegurar el correcto funcionamiento del servicio de estampado de tiempo, y velar por el cumplimiento por parte de los PSET de las consideraciones establecidas en esta norma, se realizará un proceso de auditoría de conformidad con el esquema funcional del Servicio de Estampado de Tiempo, debiendo someterse a los procesos que intervienen en la auditoría, reflejado en el Capítulo N° 6 de la GUIA PARA LA ACREDITACIÓN, ESTÁNDARES TECNÓLOGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN DE PROVEEDORES DEL SERVICIO DE ESTAMPADO DE TIEMPO (PSET)

Firma Superintendente

- 7.2.8** Los PSETs, deberán actualizar la hora con los equipos que intervienen en el proceso de Estampado de Tiempo (NTPs y TSSs) con la *Fuente Confiable de Tiempo* cada 3180 seg = 53 min

El Servicio Digital de Tiempo y los equipos de los PSET se conectarán a un Servidor NTP Stratum 2, sincronizando periódicamente (cada minuto) el reloj del sistema. El Servidor NTP Stratum 2 consiste en un emisor de paquetes IP con información horaria sobre el valor del tiempo universal actual UTC a través del protocolo NTP (Network Time Protocol). El nivel de operación es Stratum 2 porque el servidor obtiene sus señales de tiempo a partir de un equipo hardware dedicado que está sincronizado con la escala UTC (Universal Time Coordinates) con una precisión del microsegundo.

Los TMC de SUSCERTE cuenta con relojes hardware redundantes y está destinado exclusivamente a recibir la fecha y hora UTC para su posterior transmisión a la TSA mediante protocolo NTP. El sistema UTC utiliza la hora del meridiano de Greenwich, ignorando los desplazamientos provocados por el horario de verano. La escala de tiempo UTC, es definida y recomendada por International Telecommunications Radio Committee (ITU-R).

Con respecto a el Tiempo Atómico Internacional (TAI) es calculado por Bureau International des Poids et Mesures (BIPM), de la lectura de una red de 200 relojes atómicos localizados en laboratorios de institutos y observatorios de metrología repartidos en más de 30 países del mundo.

- 7.2.9** Los PSETs, establecerán conexión con los NTPs del servicio de Fuente Confiable de Tiempo, a través de conexiones seguras, relaciones de confianza u otro mecanismo seguro de conexión que SUSCERTE disponga.

Firma Superintendente

- 7.3.0** Si bien las normas de referencia no establecen ningún requisito técnico al respecto, con el objeto de garantizar la fiabilidad y confianza del sistema en caso de que se produzca una falla de disponibilidad del servicio suministrado y para que la captación de tiempos sea precisa y disponible y no esté sujeta a las fallas en la sincronización con el Sistema de Fuente Confiable de SUSCERTE, la misma se ha dotado de servidores NTP redundantes. Los servidores se encuentran dispuestos en diferentes centros alternos de datos en distintos puntos geográficos del país, donde los PSET se conectarán según muestra la siguiente tabla a continuación.

Localidad a conectar (Servidores NTP)	Tiempo Fuera de Sincronismo (min)
1	10 min – 20 min
2	30 min
3	50 min

- 7.3.1** Los proveedores deben cumplir con todo lo establecido en las auditorías para seguir operando durante el tiempo establecido en su acreditación, los mismos deberán conectarse con los servidores NTP de SUSCERTE tal como se describe en el apartado 7.2.8 de ésta sección. La conexión de los PSET con los servidores NTP de SUSCERTE (Fuente Confiable de Tiempo), distribuidos a nivel nacional (si así lo amerita) se realizarán a través de niveles de relaciones de confianza vía SSH con cada uno de los PSET que soliciten Fuente Confiable de Tiempo para sus TSSs



Firma Superintendente

8. ANEXOS
8.1. Anexo 1

DIAGRAMA DEL MODELO FUNCIONAL Y SINCRONISMO DEL SERVICIO DE ESTAMPADO DE TIEMPO

