RICARDO JAVIER ENRIQUE SAAVEDRA MAVILA
Gerente de Certificación y Registro Digital
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

SAAVEDRA MAVILA Ricardo Javier Enrique (FAU20295613620)
Soy el Autor del Documento
2016.12.15 16:08:13 -05'00'

Declaración de Prácticas y Política de Valor Añadido

PRESTADOR DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

Servicio de Sellado de Tiempo

TSA-RENIEC

Versión: 1.2	**Año:** 2016

Elaborado por:	Revisado por:	Aprobado por:
• Coordinador de procesos PKI • Analista de Servicios PKI	Sub Gerencia de Certificación Digital	Gerente Certificación y Registro Digital

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	01/08/2014	Elaboración y Aprobación	SGRD	Aprobado
1.1	15/05/2015	Revisión	SGCD	Aprobado
1.2	16/11/2016	Revisión	SGCD	Aprobado

INDICE

1. INTRODUCCIÓN 4
2. DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS 4
2.1. Definiciones 4
2.2. Acrónimos y abreviaturas 7
3. ALCANCE 8
4. CONCEPTOS GENERALES 9
4.1. Servicio de sellado de tiempo (TSS) 9
4.2. Autoridad de sellado de tiempo (TSA) 9
4.3. Usuarios 9
4.4. Política de sellado de tiempo y declaración de prácticas de la TSA 9
4.4.1. Propósito 10
4.4.2. Nivel de especificidad 10
4.4.3. Enfoque 10
5. POLÍTICAS DE SELLADO DE TIEMPO 11
5.1. Visión general 11
5.2. Identificación 13
5.3. Comunidad de usuarios y aplicabilidad 13
5.3.1. Terceros que confían 13
5.3.2. Otros participantes 13
5.4. Conformidad 13
6. OBLIGACIONES Y RESPONSABILIDADES 15
6.1. Obligaciones de la TSA 15
6.1.1. Generalidades 15
6.1.2. Obligaciones de la TSA con los suscriptores 15
6.2. Obligaciones de los suscriptores 15
6.3. Obligaciones de los terceros que confían 16
6.4. Responsabilidades 16
7. REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA 18
7.1. Declaración de Prácticas y Declaración de Libre Divulgación de la TSA 18
7.1.1. Declaración de Prácticas de la TSA 18
7.1.2. Declaración de Libre Divulgación de la TSA 19
7.2. Ciclo de vida de la gestión de las llaves 20
7.2.1. Generación de las llaves de la TSA 20
7.2.2. Protección de las llaves privadas de la TSU 20
7.2.3. Distribución de las llaves públicas de la TSU 20

7.2.4. Regeneración de llaves de la TSU 21
7.2.5. Fin del ciclo de vida de las llaves de la TSU 21
7.2.6. Gestión del ciclo de vida del módulo criptográfico usado para la firma de sellos de tiempo 21
7.3. Sellado de tiempo **22**
7.3.1. Sello de tiempo 22
7.3.2. Sincronización del reloj 22
7.4. Gestión y operación dela TSA **22**
7.4.1. Gestión de la seguridad 22
7.4.2. Gestión y clasificación de activos 23
7.4.3. Seguridad del personal 23
7.4.4. Seguridad física y del entorno 24
7.4.5. Gestión de operaciones 24
7.4.6. Gestión de acceso a los sistemas 25
7.4.7. Mantenimiento y despliegue de sistemas confiables 26
7.4.8. Compromiso de los servicios de la TSA 26
7.4.9. Terminación de la TSA 27
7.4.10. Cumplimiento de requisitos legales 27
7.4.11. Registro de información concerniente a la operación de los servicios de sellado de tiempo 27
7.5. Aspectos organizacionales **28**
8. CONSIDERACIONES DE SEGURIDAD 30
9. BIBLIOGRAFÍA. 31

1. INTRODUCCIÓN

El Registro Nacional de Identificación y Estado Civil (en adelante el RENIEC) es un organismo constitucional y autónomo con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante la Ley Orgánica N° 26497, goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de registrar la identidad, los hechos vitales y los cambios de estado civil de las personas; participar del Sistema Electoral; y promover el uso de la identificación y certificación digital.

Mediante la Ley Nº 27269 - Ley Firmas y Certificados Digitales[1] se regula en el Perú la utilización de la firma electrónica y los certificados digitales, así como el establecimiento de los Prestadores de Servicios de Certificación Digital. Su Reglamento vigente, aprobado mediante el Decreto Supremo Nº 052-2008-PCM[2] (en adelante el Reglamento), reglamentó el empleo de la firma digital para los sectores público y privado, otorgando a la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) la misma validez y eficacia jurídica que el uso de una firma manuscrita, asimismo, estableció el régimen de la IOFE, definida[3] como un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (en adelante AAC), provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: la integridad de los documentos electrónicos y la identidad de su autor.

Este sistema incluye la generación de firmas digitales, en las que participan Entidades de Certificación y Entidades de Registro o Verificación acreditadas ante la AAC, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

El artículo 47º del Reglamento designó al RENIEC como Entidad de Certificación Nacional para el Estado Peruano (en adelante ECERNEP), Entidad de Certificación para el Estado Peruano (en adelante ECEP) y Entidad de Registro o Verificación para el Estado Peruano (en adelante EREP), disponiendo se realicen los trámites correspondientes ante la AAC, con el fin de acreditarse como Prestador de Servicios de Certificación Digital y formar parte de la IOFE. Adicionalmente, el artículo 46º dispone que la ECERNEP o la ECEP *"…podrán brindar servicios de valor añadido en condición de Prestador de Servicios de Valor Añadido para el Estado Peruano conforme a lo dispuesto en la Ley y el presente Reglamento, siempre y cuando cuenten con la correspondiente acreditación.*"

El RENIEC en el año 2012 logró la acreditación de la ECERNEP Y ECEP, y en el 2013 la acreditación de la EREP, incluyéndose además la acreditación de una aplicación de software para la generación y verificación de firmas digitales. En dicho orden de ideas y en concordancia con lo dispuesto por el Reglamento, el RENIEC en su rol de Prestador de Servicios de Valor Añadido para el Estado Peruano ofrece el servicio de Sellado de Tiempo (TSA-RENIEC), para la creación de evidencia de la existencia de datos electrónicos vinculados con determinado momento en el tiempo.

2. DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS

2.1. Definiciones

[1] Publicada en el Diario Oficial el peruano el 28 de mayo de 2000.

[2] Publicada en el Diario Oficial el peruano 19 de julio de 2008.

[3] Décimo Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales.

- **Acreditación**: es el acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento de la Ley de Firmas y Certificados Digitales a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

- **Autoridad Administrativa Competente:** es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el Reglamento de la Ley de Firmas y Certificados Digitales o aquellas que requiera en el transcurso de sus operaciones.

- **Tercero que confía:** persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez del mismo.

- **Suscriptor:** El suscriptor es la entidad o el usuario final que requiere los servicios provistos por la TSA-RENIEC y que ha dado su conformidad, explícita o implícitamente, a sus términos y condiciones de uso. Esta entidad a su vez puede comprender a uno o varios usuarios finales.
  Haciendo uso de un software cliente, los usuarios efectúan peticiones de sellado y reciben sellos de tiempo conforme el protocolo RFC3161 Time-Stamp Protocol (TSP). Los suscriptores deben adaptar sus sistemas para poder realizar peticiones de sellado de tiempo y recibir las respuestas correspondientes.
  Las obligaciones del suscriptor se describen en el ítem 6.2. “Obligaciones del Suscriptor”.

- **Sello de tiempo:** Estructura de datos conformada básicamente por tres elementos: el resumen del dato que está siendo sellado, el momento en el que el sello fue emitido y una firma digital generada por la TSA-RENIEC.

- **Software cliente:** software usado para efectuar peticiones y recibir sellos de tiempo de la TSA-RENIEC.

- **Autoridad de sellado de tiempo**: Prestador de servicios de valor añadido para el Estado Peruano que emite sellos de tiempo confiables.

- **Declaración de Prácticas y Política de Sellado de Tiempo**: declaración de las prácticas que un prestador de servicios de valor añadido emplea en la emisión de sellos de tiempo. El documento es presentado oficialmente por la misma ante la Autoridad Administrativa Competente.

- **Declaración de la Autoridad de Sellado de Tiempo para divulgación**: en inglés *TSA Disclosure statement,* conjunto de afirmaciones acerca de las políticas y prácticas de un Prestador de servicios de Sellado de Tiempo que requieren particularmente de énfasis o necesidad de divulgación a los suscriptores y terceros que confían, por ejemplo para cumplir con requisitos normativos.

- **Política de sellado de tiempo**: conjunto de reglas que señalan la aplicabilidad de un sello de tiempo a una comunidad particular y/o clase de aplicación bajo requisitos comunes de seguridad.

- **Tiempo Universal Coordinado**: en inglés *Coordinated Universal Time,* es el principal estándar de fecha y hora con el cual se regulan los relojes y el tiempo en el mundo. Se encuentra definido en la Recomendación ITU-R TF.460-5.

  NOTA: Para la mayoría de los propósitos prácticos el Tiempo Universal Coordinado es equivalente al tiempo solar medio en el primer meridiano. Más específicamente, el Tiempo Universal Coordinado es un compromiso entre el altamente estable tiempo atómico *(Temps Atomique International - TAI)* y el tiempo solar que se deriva de la rotación irregular de la Tierra (relacionado con el tiempo medio sideral de Greenwich (GMST) bajo una relación dada por convención).

- **Unidad de sellado de tiempo**: conjunto de hardware y software que es gestionado como una unidad y que tiene una única llave de firma correspondiente a un sello de tiempo que se encuentra activa en un momento dado.

- **UTC(k)**: Escala de tiempo proporcionada por el laboratorio “k”, que mantiene estrecha concordancia con el Tiempo Universal Coordinado (UTC), con la meta de lograr una desviación permitida de ±100ns. (Ver Recomendación ITU-R TF.536-1)

  NOTA: Una lista de los laboratorios UTC(k) se puede encontrar en la sección 1 de la Circular T difundida por BIPM (Oficina Internacional de Pesas y Medidas) y disponible en su sitio WEB (http://www.bipm.org/).

- Unidad de Sellado de Tiempo (TSU): conjunto de hardware y software que operan creando firmas y sellos de tiempo en nombre de una TSA. La TSA-RENIEC opera uno o más TSU, cada uno con su par de llaves y certificado digital propio.

2.2. Acrónimos y abreviaturas

- **AAC** Autoridad Administrativa Competente.
- **DPR o RPS** Declaración de Prácticas y Políticas de Registro *(Registration Authority Practice Statement).*
- **CPS o DPC** Declaración de Prácticas y Políticas de Certificación *(Certificate Practice Statement).*
- **CP** Políticas de Certificación *(Certification Policy)*
- **CRL** Lista de Certificados Revocados (*Certificate Revocation List)*
- **EC** Entidad de Certificación.
- **ECEP–RENIEC** Entidad de Certificación para el Estado Peruano.
- **EREP–RENIEC** Entidad de Registro o Verificación para el Estado Peruano.
- **GCRD** Gerencia de Certificación y Registro Digital
- **INDECOPI** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- **IETF** *Internet Enginerring Task Force*
- **IOFE** Infraestructura Oficial de Firma Electrónica.
- **RENIEC** Registro Nacional de Identificación y Estado Civil.
- **RUC** Registro Único de Contribuyentes.
- **PSVA o VASP** Prestador de Servicios de Valor Añadido. (Value Added Service Provider)
- **TSA** Autoridad de Sellado de Tiempo *(Time-Stamping Authority).*
- **TST** Sello de Tiempo *(Time-Stamp Token).*
- **TSS** Servicio de sellado de tiempo **(**"Time Stamp Service"**)**
- **TSU** Unidad de Sellado de Tiempo *(Time-Stamping Unit).*
- **TUPA** Texto Único de Procedimiento Administrativo.
- **UTC** Tiempo Universal Coordinado *(Coordinated Universal Time).*
- **VAPS** Declaración de Prácticas y Política de Sellado de Tiempo ***("Value-Added Products and Services")***

3. ALCANCE

La presente Declaración de Prácticas y Política de Sellado de Tiempo (en adelante VAPS por las siglas en Ingles de “Value-Added Products and Services”) define las prácticas operativas y de gestión del RENIEC en su rol de Prestador de Servicios de Valor Añadido para el Estado Peruano y ha sido redactada conforme lo establece la *“Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA”*, Versión 3.3, la que en su numeral 10.1 señala que deberán observarse para su elaboración los lineamientos establecidos en el RFC 3628, *“Policy Requirements for Time-Stamping Authorities (TSAs)”.*

A fin de dotar de uniformidad al documento, facilidad de lectura y análisis, se incluyen todas las secciones establecidas en el referido RFC, indicándose en aquella sección que no resulta de aplicación para la TSA-RENIEC, la frase “No aplica”. También, se colocará entre comillas y en negrita las referencias a documentos, siendo estos públicos o confidenciales según la evaluación de seguridad efectuada y las normas adoptadas por el RENIEC.

El presente documento, en conjunto con la Declaración de Prácticas y Políticas de Certificación de la ECEP-RENIEC y ECERNEP, puede ser utilizado por organismos independientes como base para evaluar la confiabilidad del RENIEC como prestador de servicios de certificación digital. Se presenta a dicho efecto el detalle suficiente sobre la implementación de las políticas en los procesos y prácticas correspondientes.

4. CONCEPTOS GENERALES

4.1. Servicio de sellado de tiempo (TSS)

El servicio de sellado de tiempo consta de dos procedimientos

- Provisión: La provisión del servicio se efectúa en los siguientes pasos
  - El software cliente calcula el resumen hash del documento a sellar
  - El software cliente envía una petición a una URL determinada por TSA-RENIEC, conforme a lo que indica el RFC 3161, incluyendo el hash del dato o documento a sellar
  - La TSA-RENIEC recibe el pedido y la firma, generando un Sello de Tiempo (que incluye el hash del documento, la fecha y hora obtenidas de una fuente confiable y la firma digital de la TSA)
  - El sello de tiempo es retornado al cliente
  - La TSA-RENIEC registra el sello emitido en un repositorio, para futuras verificaciones.
- Administración: Gestiona el control y monitoreo de la operación de los servicios para asegurar que sea provisto de acuerdo a los especificado en este documento.

Actualmente, la TSA-RENIEC soporta peticiones de sello de tiempo con algoritmo hash SHA-1 y SHA-256. Al respecto, cabe resaltar que las peticiones de sellos de tiempo con algoritmo SHA-1 serán aceptadas únicamente hasta el 31 de Diciembre de 2016. A partir del 01 de Enero de 2017 solamente se aceptarán peticiones de sellos de tiempo con algoritmo SHA-256

4.2. Autoridad de sellado de tiempo (TSA)

La ECEP-RENIEC administra el servicio que opera una o más TSU, las cuales crean y firman sellos en nombre de la TSA-RENIEC, en la cual confían los usuarios del servicio de sellado de tiempo (suscriptores y terceros que confían) para la emisión de los sellos de tiempo. La TSA-RENIEC tiene responsabilidad global en la provisión del servicio de sellado de tiempo que se identifica en la cláusula 4.1.

4.3. Usuarios

Los usuarios son los suscriptores del servicio, los cuales pueden ser: una entidad o un usuario final. El suscriptor puede ser una entidad que comprende varios usuarios finales o un usuario final individual.
Cuando el suscriptor es una entidad, puede comprender uno o varios usuarios finales, y las obligaciones que se aplican a esa entidad tendrán que aplicarse también a los usuarios finales. En cualquier caso la organización se hace responsable si no se cumplen correctamente las obligaciones de sus usuarios finales y por lo tanto, se espera que la organización informe adecuadamente a sus usuarios.

Cuando el Suscriptor es un usuario final, éste es directamente responsable del cumplimiento de las obligaciones.

4.4. Política de sellado de tiempo y declaración de prácticas de la TSA

La declaración de prácticas política de sellado de tiempo de la TSA-RENIEC especifica los lineamientos del servicio de sellado de tiempo para cumplir con la

Guía de acreditación de la Prestador de Servicios de Valor Añadido y ha sido elaborado en concordancia con el RFC 3628

4.4.1. Propósito

El presente documento de declaración de prácticas y política de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC indica qué actividades son necesarias para la provisión del servicio y detalla el cómo se deben realizar estas actividades.

4.4.2. Nivel de especificidad

El presente documento no pretende representar la totalidad de las políticas, estándares, procedimientos y estándares que ofrece el RENIEC. Específicamente, describe los procedimientos utilizados para brindar el servicio de Sellado de Tiempo (TSA) como Prestador de Servicios de Valor Añadido dentro del marco de la IOFE.

Sin embargo, debido a que la TSA-RENIEC se apoya en procedimientos desarrollados por la ECEP-RENIEC. Debido a ello el presente documento hace referencia a los correspondientes puntos de la CPS de la ECEP-RENIEC y la CP de la ECERNEP

4.4.3. Enfoque

El presente documento se ha desarrollado en conformidad con el RFC 3628, “Policy Requirements for Time-Stamping Authorities (TSAs)” de la IETF. Como parte de la declaración de prácticas de la TSA se detallan las actividades de provisión del servicio de la TSA-RENIEC, y dado que la TSA-RENIEC utiliza para brindar el servicio de sello de tiempo la infraestructura de la ECEP y la ECERNEP, los procedimientos referidos a la estructura de la organización, instalaciones físicas e infraestructura tecnológica de la información, son desarrollados en la CPS de la ECEP-RENIEC y la CP de la ECERNEP.

Algunos procedimientos técnicos son de carácter confidencial y no están disponibles al público.

5. POLÍTICAS DE SELLADO DE TIEMPO

5.1. Visión general

La política de sellado de tiempo de la TSA-RENIEC comprende un conjunto de reglas y procesos que deben ser usados para la emisión de sellos de tiempo confiables, en concordancia con la Ley de Firmas y Certificados Digitales, su Reglamento, la "Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", Versión 3.3, y las recomendaciones definidas en el RFC 3628.

El perfil de los certificados de la TSA-RENIEC, utilizados en la emisión de los sellos de tiempo, se ajusta a las recomendaciones del RFC 3161 En la Tabla 1 se detalla el perfil de los certificados digitales de la TSA-RENIEC

TSA-RENIEC SHA1

Campo	Valor
Emitido para	RENIEC Time-Stamping Authority
Emitido por	RENIEC Certification Authority
Versión del Certificado	V3
Número de Serie del Certificado	
Algoritmo de Firma	Sha1WithRSAEncryption
Algoritmo de hashing	SHA1
Emisor	CN = RENIEC Certification Authority O = Registro Nacional de Identificación y Estado Civil C = PE
Validez (no antes)	*<<Fecha y hora de emisión>>*
Validez (no después)	*<<Fecha y hora de caducidad>>*
Validez (en años)	10 años
Sujeto [Atributos de Nombre Distinguido]	CN = RENIEC Time-Stamping Authority OU = RENIEC Certification Authority O = Registro Nacional de Identificación y Estado Civil C = PE
Llave Pública	RSA (4096 Bits)
Algoritmo de identificación	SHA1
Identificador de llave del Titular	*<Resumen hash SHA1 (160 bits) de la llave pública contenida en el certificado>*
Identificador de llave de la entidad emisora	*<Resumen hash SHA1 (160 bits) de la llave pública del certificado RENIEC High Grade Certification Authority*
Restricciones Básicas	**CRITICO**, Tipo de asunto=Entidad Final Restricción de longitud de ruta=Ninguno
Uso de la llave	Firma Digital, Sin repudio (c0)
Directiva del Certificado	[1]Directiva de certificados: Identificador de directiva=Todas las directivas de emisión [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.reniec.gob.pe/repository
Nombre Alternativo del Sujeto	Ausente Dirección URL=<URL del servicio>
Uso mejorado de la llaves	Impresión de fecha (1.3.6.1.5.5.7.3.8) **CRÍTICO**
Puntos de Distribución CRL	1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL= *<URL de la CRL>*

TSA-RENIEC SHA256

Campo	Valor
Emitido para	RENIEC High Grade Time-Stamping Authority
Emitido por	RENIEC High Grade Certification Authority
Versión del Certificado	V3
Número de Serie del Certificado	
Algoritmo de Firma	Sha256WithRSAEncryption
Algoritmo de hashing	SHA256
Emisor	CN = RENIEC High Grade Certification Authority O = Registro Nacional de Identificación y Estado Civil C = PE
Validez (no antes)	*<<Fecha y hora de emisión>>*
Validez (no después)	*<<Fecha y hora de caducidad>>*
Validez (en años)	10 años
Sujeto [Atributos de Nombre Distinguido]	CN = RENIEC High Grade Time-Stamping Authority OU = RENIEC Certification Authority O = Registro Nacional de Identificación y Estado Civil C = PE
Llave Pública	RSA (4096 Bits)
Algoritmo de identificación	SHA1
Identificador de llave del Titular	*<Resumen hash SHA1 (160 bits) de la llave pública contenida en el certificado>*
Identificador de llave de la entidad emisora	*<Resumen hash SHA1 (160 bits) de la llave pública del certificado RENIEC High Grade Certification Authority*
Restricciones Básicas	**CRITICO**, Tipo de asunto=Entidad Final Restricción de longitud de ruta=Ninguno
Uso de la llave	Firma Digital, Sin repudio (c0)
Directiva del Certificado	[1]Directiva de certificados: Identificador de directiva=Todas las directivas de emisión [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.reniec.gob.pe/repository
Nombre Alternativo del Sujeto	Ausente Dirección URL=<URL del servicio>
Uso mejorado de la llaves	Impresión de fecha (1.3.6.1.5.5.7.3.8) **CRÍTICO**
Puntos de Distribución CRL	1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL= *<URL de la CRL>*

5.2. Identificación

Esta política es de aplicación a las distintas unidades de sellado de tiempo (TSU) que la TSA-RENIEC pudiera establecer para la prestación del servicio.

- **Nombre:** Declaración de Prácticas y Políticas de Valor Añadido. Prestador de Servicios de Valor Añadido para el Estado Peruano. Servicio de Sellado de Tiempo. TSA- RENIEC
- **Versión:** 1.1
- **OID:** 1.3.6.1.4.1.35300.1.1.1.3
- **Website:** http://www.reniec.gob.pe/repository
- **Fecha de elaboración:** 10/12/2015
- **Fecha de última modificación:** 16/11/2016
- **Lugar:** Lima, Peru

5.3. Comunidad de usuarios y aplicabilidad

Un sello de tiempo es utilizado para probar la existencia de ciertos datos en un determinado momento de tiempo (como algunos ejemplos: contratos, registros médicos, firmas digitales, entro otros) sin que ninguna de las partes pueda colocar una fecha y hora diferente a la que provee el servicio de sellado de tiempo desde una fuente confiable.

La comunidad de usuarios que solicitan sellos de tiempo se compone de los suscriptores (personas naturales o jurídicas) que cuentan con la autorización respectiva para hacer uso del servicio de sellado de tiempo de la TSA-RENIEC. El procedimiento que debe seguirse acceder a dichos servicios es publicado en el TUPA del RENIEC, dentro de la página web institucional http://www.reniec.gob.pe,

Terceros que confían

Los terceros que confían pueden ser personas naturales, jurídicas, equipos, servicios o cualquier otro ente diferente al usuario que decide aceptar y confiar en un sello de tiempo emitido por la TSA-RENIEC y que confía en las jerarquías RENIEC Certification Authority y RENIEC High Grade Certification Authority, tal como se indica en el numeral 1.3.6 de la CP de la ECERNEP.

.

5.3.2. Otros participantes

Todas las funciones, operaciones y actividades organizadas para brindar el servicio de sellado de tiempo de la TSA-RENIEC serán desarrollados y estarán a cargo del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital. Sin embargo, el RENIEC tiene la potestad para contratar los servicios de un tercero para realizar algún servicio relacionado a la TSA-RENIEC, realizando la firma de un contrato de servicios con cláusulas específicas de confidencialidad y protección de datos personales, de ser el caso.

5.4. Conformidad

La política de sellado de tiempo de la TSA-RENIEC incorporada en el presente documento guarda conformidad con en el RFC 3628, en respaldo de lo cual cumple con el procedimiento de acreditación establecido bajo el marco de la IOFE a cargo de la AAC. Además, los sellos de tiempo emitidos cumplen con el RFC 3161 incluyendo el Identificador de Objeto (OID) indicado en el numeral 5.2.2 del presente documento.

En dicho sentido, la TSA-RENIEC demuestra bajo dicha acreditación que cumple con las obligaciones definidas en el numeral 6.1 del presente documento y que ha implementado controles que cumplen con los requisitos especificados en el numeral 7.

6. OBLIGACIONES Y RESPONSABILIDADES

6.1. Obligaciones de la TSA

6.1.1. Generalidades

El RENIEC, en su calidad de Prestador de Servicios de Valor Añadido, asegura que todos los requerimiento de Sellado de Tiempo, detallados en el numeral 7, han sido implementados como aplicación a la presente política.

Además, asegura que se cumplen a cabalidad los procedimientos descritos en esta política, incluso si se realiza la contratación de terceros para algún servicio relacionado con la TSA-RENIEC.

Se provee la declaración de prácticas de sellado de tiempo para cumplimiento de todos los servicios en completa conformidad con la política de sellado de tiempo.

6.1.2. Obligaciones de la TSA con los suscriptores

- Realizar el servicio de sellado de tiempo en conformidad con esta política de sellado de tiempo.
- Proteger las llaves privadas emitidas para cada una de sus TSU
- Emitir sellos de tiempo que sean conformes con la información conocida en el momento de su emisión y libres de errores de entrada de datos
- Utilizar componentes de hardware y software fiables, que estén protegidos contra toda alteración y que garanticen la seguridad técnica.
- La correcta ejecución de los procesos criptográficos durante la emisión y verificación del sello de tiempo.
- Garantizar que se puede determinar con precisión y confiabilidad la fecha y hora en la que un sello de tiempo fue emitido
- Publicar este documento y los relacionados al servicio, garantizando el acceso a la versión actual y las anteriores.
- Garantizar que todos los requerimientos de la TSA, incluidos procedimientos, prácticas relativas a la emisión de sellos de tiempo y revisión de sistemas están conforme a los descrito en los documentos operaciones y técnicos de la TSA-RENIEC

La TSA-RENIEC garantiza que los sellos de tiempo son emitidos en concordancia a los siguientes documentos normativos:

- Ley de Firmas y Certificados Digitales
- Reglamento de la Ley de Firmas y Certificados Digitales
- Guía de Acreditación de Prestador de Servicios de Valor Añadido, versión 3.3

6.2. Obligaciones de los suscriptores

Es responsabilidad del suscritor en el proceso de obtención de un sello de tiempo:

- Verificar que el sello de tiempo ha sido firmado correctamente y que la llave privada de la TSU usada para firmar el sello de tiempo no se encontraba comprometida hasta el momento de la verificación, debiendo disponerse para tal efecto del software de verificación de sello de tiempo adecuado, y así dar conformidad a lo establecido en el marco de la IOFE.
- Comprobar el estado del certificado digital de la TSA-RENIEC en la CRL. Durante el periodo de vigencia del certificado digital de la TSU se puede verificar la validez del certificado digital en la CRL publicada por la ECERNEP o a través de otro mecanismo de consulta que ésta ponga a disposición.
- Tendrá en cuenta cualquier limitación en el uso del sello de tiempo conforme se encuentra indicado en el documento Declaración y políticas de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC.

6.3. Obligaciones de los terceros que confían

Es responsabilidad de los terceros que confían:

- Verificar que el sello de tiempo ha sido firmado correctamente y que la llave privada de la TSU usada para firmar el sello de tiempo no se encontraba comprometida hasta el momento de la verificación, debiendo disponerse para tal efecto del software de verificación de sello de tiempo adecuado, y así dar conformidad a lo establecido en el marco de la IOFE. Durante el periodo de vigencia del certificado digital de la TSU se puede verificar la validez del certificado digital en el repositorio de la CRL publicada por la ECERNEP o a través de otro mecanismo de consulta que ésta ponga a disposición.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo conforme se encuentra indicado en el documento de declaración de prácticas y política de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo prescrita en otros documentos estipulados y comunicados por la TSA-RENIEC.

6.4. Responsabilidades

El RENIEC opera la TSA-RENIEC en concordancia con los siguientes documentos:

- La Ley de Firmas y Certificados Digitales (Ley 27269) y su modificatoria (Ley 27310).
- El Reglamento de la Ley de Firmas y Certificados Digitales, D.S. Nº 052-2008-PCM y sus modificatorias, D.S N° 070-2011-PCM y D.S N° 105-2012-PCM.
- La Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, Versión 3.3, INDECOPI.
- Declaración de prácticas y políticas de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC.
- Declaración de Prácticas y Políticas de Certificación de la ECEP-RENIEC.
- Política General de Certificación de la ECERNEP.
- Otros acuerdos vinculantes que pudieran establecerse entre RENIEC y los usuarios de los servicios de su TSA

El RENIEC no se hace responsable de la veracidad ni del contenido de los datos sellados por la TSA-RENIEC.

Bajo ninguna circunstancia, el RENIEC será responsable por cualquier pérdida, daños indirectos o consecuentes, o por pérdida de datos por la utilización de un software no confiable. Además, no será responsable por daños que resulten del incumplimiento de las obligaciones que confía respecto de los términos y condiciones de uso aplicables, incluyéndose el exceso en el límite establecido para las transacciones.

El RENIEC, bajo ninguna circunstancia, será responsable por daños que resulten de eventos de fuerza mayor o desastres naturales, conforme se detalla en la sección 7.1.2 del presente documento. El RENIEC tomará medidas razonables para mitigar los efectos de eventos de fuerza mayor en un plazo razonable.

7. REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA

La TSA-RENIEC ha establecido controles para la provisión del servicio de sellado de tiempo, los cuales se indican a continuación, adicionalmente cumple los controles establecidos en la CPS de la ECEP-RENIEC.

7.1. Declaración de Prácticas y Declaración de Libre Divulgación de la TSA

7.1.1. Declaración de Prácticas de la TSA

Los procedimientos de la TSA-RENIEC son evaluados bajo el proceso de acreditación seguido ante la AAC (INDECOPI) en el marco de la IOFE conforme a su rol definido en el Reglamento de la Ley de Firmas y Certificados Digitales.

Esta Declaración de Prácticas de TSA y cualquier otra información relevante es publicada en http://www.reniec.gob.pe/repository.

Los documentos de carácter confidencial no son publicados. La Declaración de Libre Divulgación de la TSA-RENIEC, se incluye en el numeral 7.1.2 del presente documento.

La TSA-RENIEC brinda el servicio de sellado de tiempo, conforme a lo siguiente:

a) Para los procesos de la TSA-RENIEC, y los procesos de soporte del mismo tales como copias de seguridad, seguridad de redes, etc. se ha desarrollado un análisis de riesgos como parte de la certificación ISO 27001, en el cual se identifican sus activos y las amenazas a dichos activos determinando los controles de seguridad necesarios para mitigar dichos riesgos y los procedimientos operativos correspondientes.
b) Dado que las actividades de la TSA-RENIEC, se soportan en los procedimientos de la ECEP-RENIEC, los procedimientos de la TSA-RENIEC son los mismos de la ECEP-RENIEC, esto de acuerdo a la CPS de la ECEP-RENIEC.
c) Los servicios de la TSA-RENIEC serán soportados internamente por el propio RENIEC. En caso de que se recurra a terceros para la prestación de los mismos en el futuro, ello se divulgará a suscriptores y terceros que confían.
d) La TSA-RENIEC pone a disponibilidad de los suscriptores y terceros que confían su Declaración de prácticas y políticas de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC, y otra documentación relevante en su repositorio, disponible en http://www.reniec.gob.pe/repository.
e) La TSA-RENIEC divulgará a todos los suscriptores y terceros que confían los términos y condiciones de uso de sus servicios de sellado de tiempo según se encuentran especificados en la sección 7.1.2.
f) La aprobación de la VAPS es responsabilidad del Gerente de la GCRD. El “Comité para gestiones sobre acreditación ante la AAC”, es responsable de la gestión ante INDECOPI para la aprobación de la VAPS.
g) El Gerente de la GCRD, es el encargado de designar al Responsable de la TSA-RENIEC, este último debe asegurar el cumplimiento de las prácticas indicadas en el presente documento.
h) Como parte del cumplimiento de lo declarado en:

- Declaración de prácticas y políticas de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC,
- Declaración de Prácticas y Políticas de Certificación de la ECEP-RENIEC y
- Política General de Certificación de la ECERNEP.

La TSA-RENIEC ha establecido un Plan anual de auditorías, cuya ejecución tiene por objetivo la verificación del cumplimiento de lo declarado en dichos documentos.

i) En caso de cambios a la VAPS de la TSA-RENIEC, se tiene que tener las siguientes consideraciones:
   - Debe estar aprobado antes de su publicación por la autoridad máxima de la TSA-RENIEC.
   - Se debe seguir lo indicado en la CPS de la ECEP-RENIEC, ítem 9.12 “Enmendaduras”.
   - Se publicará la nueva versión de la VAPS en la URL http://www.reniec.gob.pe/repository, y
   - Se mantendrá disponible a los suscriptores y terceros que confían el historial de versiones de la VAPS.

7.1.2. Declaración de Libre Divulgación de la TSA

a) Las consultas relacionadas al presente documento pueden ser dirigidas a la cuenta de correo electrónico identidad digital: identidaddigital@reniec.gob.pe
b) La política de sellado de tiempo aplicable a los servicios de la TSA-RENIEC es la especificada en el presente documento.
c) Los algoritmos de hash soportados en la aplicación del sello de tiempo son SHA-1 y SHA-256. Este algoritmo se determina en la petición del sello de tiempo.
d) La petición de sellos de tiempo con algoritmo SHA-1 será soportado únicamente hasta el 31 de Diciembre de 2016. A partir del 01 de Enero de 2017 solamente se aceptarán peticiones de sellos de tiempo con algoritmo SHA-256
e) El periodo de validez de los certificados digitales de la TSA-RENIEC es de 10 años.
f) La precisión del sellado de tiempo emitidos por la TSA-RENIEC guarda conformidad con el estándar NTP que establece una precisión mínima respecto al UTC de ± 1 segundo.
g) El servicio sólo puede ser utilizado dentro de lo establecido en esta declaración de prácticas y política de valor añadido de sello de tiempo.
h) Las obligaciones del suscriptor están definidas en el numeral 6.2 del presente documento.
i) Las obligaciones de los terceros que confían se encuentran definidas en el numeral 6.3 del presente documento.
j) La información sobre cómo verificar la veracidad y validez del sello se detalla en el numeral 6.3.
k) La TSA-RENIEC, como Prestador de Servicios de Valor Añadido, puede obligar a los suscriptores y demás participantes a cumplir con acuerdos y términos de uso adicionales, siempre y cuando no se contravenga lo requerido en la Ley de Firmas y Certificados Digitales, su reglamento, CP de la ECERNEP y normas complementarias.
l) El periodo de tiempo durante el cual se guardan los registros de los eventos de la TSA-RENIEC es de 10 años, en conformidad con lo

indicado en el numeral 5.4.3 “Periodo de conservación del registro de auditorías” de la CPS de la ECEP-RENIEC.

m) .

n) El RENIEC cobra las tasas pertinentes por los servicios prestados por la TSA-RENIEC, conforme se encuentra detallado en el TUPA del RENIEC.

o) El RENIEC tiene políticas y procedimientos para resolución de quejas y reclamos recibidos por clientes o terceros sobre los servicios de sellado de tiempo u otros servicios relacionados. El RENIEC como parte del proceso de acreditación como TSA-RENIEC ha sido evaluada en el cumplimiento de lo declarado en Declaración de prácticas y políticas de valor añadido del servicio de sellado de tiempo de la TSA-RENIEC, por un auditor independiente, tanto en la parte documentaria como en la parte funcional del servicio de sellado de tiempo.

7.2. Ciclo de vida de la gestión de las llaves

7.2.1. Generación de las llaves de la TSA

La TSA-RENIEC almacena y protege sus llaves privadas en módulos criptográficos que fueron generadas y que cumplen lo indicado en el numeral 6.2.1 de la CPS de la ECERNEP.

La TSA-RENIEC puede realizar copia de respaldo (backup) de sus llaves privadas, aplicando la misma protección establecida para la llave privada original

7.2.2. Protección de las llaves privadas de la TSU

La TSA-RENIEC almacena y protege sus llaves privadas en módulos criptográficos que fueron generadas y que cumplen lo indicado en el numeral 7.2.1 del presente documento, en concordancia al numeral 6.2.1 de la CPS de la ECERNEP.

La TSA-RENIEC puede realizar copia de respaldo (*backup*) de sus llaves privadas, aplicando la misma protección establecida para la llave privada original.

7.2.3. Distribución de las llaves públicas de la TSU

Los certificados digitales de la TSA-RENIEC, que incluyen la llave pública son distribuidos en el repositorio correspondiente. El certificado TSA-RENIEC SHA1 es emitido por RENIEC Certification Authority y el certificado TSA-RENIEC SHA256 es emitido por RENIEC High Grade Certification Authority, según se indica en la CP de la ECERNEP.

7.2.4. Regeneración de llaves de la TSU

La llave privada de la TSU será reemplazada antes que finalice el periodo de validez de su correspondiente certificado digital, cuando se verifique el compromiso de la misma, debilidad de los algoritmos de firma y resumen o cuando la TSA-RENIEC lo requiera para poder seguir brindando un servicio de sellado de tiempo con un periodo de validez razonable.

La generación de la nueva llave privada se lleva a cabo conforme a lo indicado en el numeral 7.2.1

7.2.5. Fin del ciclo de vida de las llaves de la TSU

La TSA-RENIEC garantiza que la llave privada asociada a una TSU no pueda ser usada en un tiempo posterior al fin del ciclo de vida del certificado asociado (validez).

El ciclo de vida de la llave privada de una TSU, está asociada al ciclo de vida del certificado digital que le corresponde. La TSA-RENIEC garantiza que sus sistemas de emisión y gestión de sellos de tiempo no aceptan peticiones que involucren a certificados digitales de TSU caducos o cancelados (revocados).

7.2.6. Gestión del ciclo de vida del módulo criptográfico usado para la firma de sellos de tiempo

- Los HSM se trasladan por personal interno de la ECEP-RENIEC con roles autorizados para su inicialización y puesta en marcha dentro de las dependencias internas seguras, con los controles de seguridad física adecuados, siendo desde este momento todas las manipulaciones registradas y auditadas, tal como se detalla en el punto 5.4. “Procedimiento de registro de auditorías” de la CPS correspondiente a la ECEP-RENIEC.
- Los dispositivos HSM son mantenidas en ambientes protegidos mediante controles de acceso físico y lógico, tal como se detalla en el punto 5.1.2 Acceso físico y 6.7. Controles de seguridad de la red.
- En caso de cambio o baja del dispositivo criptográfico HSM, se procederá con el borrado seguro y destrucción de toda la información interna del equipo.

7.3. Sellado de tiempo

7.3.1. Sello de tiempo

La TSA-RENIEC emite sellos de tiempo que cumplen con lo recomendado en el RFC 3161 y que cuentan con fecha y hora precisa. En particular, cada sello de tiempo contiene:

- Identificador OID de la Política de Sellado de Tiempo que aplica
- Un resumen del dato (hash) a ser sellado, tal cual fue provisto por el solicitante y un identificador (OID) del algoritmo de hashing utilizado.
- Un número de serie único
- La fecha y hora en la que fue generado el sello de tiempo
- La firma digital emitida utilizando la llave privada de la TSA-RENIEC.

7.3.2. Sincronización del reloj

La TSA-RENIEC cuenta con un servidor horario NTS 150 SYMMETRICOM NETWORK TIME SERVER incluyendo ATENA L1 GPS 12V UP/DN W500 FT que cumple con el protocolo NTP y brinda las seguridad necesaria para que su reloj se mantenga sincronizado con el UTC dentro del nivel de precisión de ± 1 segundo.

La fecha y hora son obtenidas del servidor NTP, siendo esta una fuente confiable. A través del protocolo NTP (Network Time Protocol) se sincronizan todos los sistemas y equipos con los que cuenta la TSA-RENIEC.

7.4. Gestión y operación dela TSA

7.4.1. Gestión de la seguridad

La TSA asegura que los procedimientos de administración y gestión aplicados son adecuados y correspondan a las mejores prácticas reconocidas, en particular:

a) La TSA-RENIEC mantiene bajo su control la gestión, administración u operación del servicio de sellado de tiempo para todos los aspectos de la provisión del servicio dentro del alcance de esta política.
b) La Política de Seguridad de la Información de la ECEP-RENIEC se aplica a la TSA-RENIEC, ya que esta última sustenta sus procesos de soporte en la ECEP-RENIEC. La TSA-RENIEC garantiza la publicación y comunicación de esta política a todos los empleados afectados.
c) La infraestructura de seguridad de la información de la TSA-RENIEC se basa en la ISO/IEC 27001:2005, cualquier cambio que pueda impactar en el nivel de seguridad es aprobado por el Responsable de la TSA-RENIEC.
d) Todos los elementos relativos al control de la seguridad se describen en la “Política de Seguridad” y en la CPS de la ECEP-RENIEC, ítems 5. “Controles de las instalaciones, de la gestión y controles operacionales” y 6. “Controles de seguridad técnica”, estando estos documentos alineados al ISO/IEC 27001:2005.

e) La TSA-RENIEC garantiza la seguridad de la provisión del servicio de sellado de tiempo. Cabe mencionar además que las funciones de la TSA-RENIEC no han sido tercerizadas.

7.4.2. Gestión y clasificación de activos

Todos los elementos relativos a la gestión y clasificación de activos se encuentran en documentación interna manejada por la ECEP-RENIEC.

El detalle de la clasificación, riesgos identificados y controles implementados sobre los activos se encuentran en el documento denominado "Matriz AMEF" (Matriz de Análisis de Modos y Efectos de Fallos), la cual ha sido elaborada por la ECEP-RENIEC en base lo establecido en el estándar ISO-27001.

7.4.3. Seguridad del personal

Los trabajadores, contratistas y consultores designados para gestionar la infraestructura de la TSA-RENIEC son considerados como "personas de confianza". Se designan, de manera oficial, los roles incluyendo sus funciones, responsabilidades y riesgos, mediante un contrato de trabajo u orden de servicio, según corresponda.

La TSA asegura que el personal y las prácticas contractuales mejoren y soporten la confiabilidad de las operaciones de la TSA.

a) El personal que opera la TSA-RENIEC cuenta con la experiencia, calificaciones y requisitos establecidos en la CPS de la ECEP-RENIEC, ítem 5.3. "Controles de personal". Sólo se proporciona a quien acredite necesidad de conocerla y son revisados de forma periódica. Se sigue lo establecido en el estándar ISO-27001.
b) Los roles de la TSA-RENIEC (incluyendo los de confianza) y las responsabilidades están descritas en el documento "Asignación de roles" de la ECEP-RENIEC.
c) El personal que opera la TSA-RENIEC tiene conocimiento de sus funciones establecidas según el documento "Asignación de roles" de la ECEP-RENIEC. Cabe mencionar que la verificación de antecedentes y entrenamiento lo realiza el área de recursos humanos del RENIEC.
d) El personal ejecuta procedimientos y procesos de acuerdo a los procedimientos de seguridad de la información ISO 27001
e) El personal que opera la TSA-RENIEC tiene conocimiento de:
   - sellado de tiempo
   - firma digital,
   - mecanismos de sincronización del servidor NTP.
   - seguridad física
   - seguridad de la información y gestión de riesgos
f) Todo el personal con roles de confianza deberá ser libre de conflictos de interés que puedan perjudicar la imparcialidad de la operación de la TSA
g) Los roles de confianza incluyen los siguientes:
   - Oficial de seguridad-GCRD: Responsabilidad general para administrar la implementación de prácticas de seguridad de la información.

- Especialista en HW y SW: Autorizados para instalar, configurar y mantener la confiabilidad de los sistemas de la TSA-RENIEC para la gestión del sellado de tiempo
- Administrador de Base de datos: Autorizado para realizar mantenimiento, soporte, ver archivos y registros auditables de la base de datos de la TSA.
- Supervisor Especialista en PKI: Autorizado para ver archivos y registros auditables de los sistemas que soportan a la TSA-RENIEC

h) El personal que opera la TSA ha sido formalmente designado, de acuerdo a sus roles de confianza.
i) La TSA-RENIEC no deberá designar en roles de confianza a ninguna persona que es conocida por tener una condena por un delito grave u otra ofensa la cual pueda afectar su idoneidad para el puesto.

7.4.4. Seguridad física y del entorno

La TSA-RENIEC debe asegurar de que el acceso físico a los servicios críticos es controlado de la siguiente manera:

a) Para la entrega y gestión de sellado de tiempo:
   - El acceso físico a los ambientes de soporte del servicio de sellado de tiempo solo es permitido a personal autorizado, de acuerdo al documento "control de acceso físico"
   - Se han establecido controles para evitar la pérdida, daño o compromiso de los activos o interrupción del servicio de la TSA-RENIEC, esto acuerdo al documento "Plan de Contingencias"
   - Se han establecido controles para evitar el compromiso o robo de información y sus medios de procesamiento, esto según el documento "control de acceso lógico".
b) Se han establecido controles de acceso físico a los módulos criptográficos, estos incluyen:
   - Control de acceso dual
   - Identificación de personal

   Estos controles están descritos en el documento: "Control de acceso físico".
c) Adicionalmente se han contemplado los siguientes controles:
   - Los medios de procesamiento de información son operados en un ambiente con protección física que impida el acceso no autorizado.
   - Se han implementado perímetros de seguridad, tal como barreras físicas.
   - Se ha implementado una política de seguridad física y del ambiente para proteger las instalaciones que contienen los recursos informáticos, y las instalaciones usadas para su operación. La política de seguridad considera el control de acceso físico, la protección contra desastres naturales, factores de protección contra incendio, fallas en los servicios de soporte (energía, comunicaciones), colapso de la estructura, aniego, protección contra robo, allanamiento, y recuperación de desastres.
   - Se deben adoptar controles para impedir que el equipamiento, información, medios de comunicación y software relacionados con los servicios de sellado de tiempo hayan sido retirados de las instalaciones sin autorización.

7.4.5. Gestión de operaciones

La TSA-RENIEC brinda las seguridades necesarias para que los componentes de sus sistemas se encuentren seguros y sean correctamente operados, todo ello bajo un mínimo riesgo de falla.

a) La integridad de los componentes informáticos y de la información están protegidos contra virus, software malicioso y no autorizado, esto de acuerdo al control de acceso lógico.
b) La TSA-RENIEC u realiza el reporte de incidentes y los procedimientos de respuesta según el documento "Gestión de incidentes" de la ECEP-RENIEC.
c) Los medios de comunicación dentro de los sistemas confiables de la TSA deberán ser protegidos durante su uso contra daño, robo, acceso no autorizado u obsolescencia, tal como se indica en el documento: "control de acceso físico" y "control de acceso lógico".
d) Se han establecido los roles (incluyendo los de confianza) para la operación de la TSA-RENIEC así como para la operación de los sistema de soporte de la misma, esto según el documento de "Asignación de roles"
e) La información de la TSA-RENIEC, antes de su desecho, es eliminada, esto según el documento "Borrado seguro y destrucción de medios de almacenamiento"
f) Las demandas de capacidad son monitoreadas para realizar proyección de requerimientos de capacidad
g) La TSA-RENIEC actúa de forma coordinada e inmediata frente a incidentes con la finalidad de reducir el impacto de seguridad de los mismos de acuerdo al documento "Gestión de incidentes" de la ECEP-RENIEC.
h) Las operaciones de seguridad de la TSA-RENIEC son realizadas por roles de confianza según lo descrito en el documento “Asignación de roles” y la “Política de Seguridad” de la ECEP-RENIEC.

7.4.6. Gestión de acceso a los sistemas

El acceso al sistema de la TSA o a los sistemas de soporte de la misma solo está disponible para personal autorizado.

a) Se han implementado controles de seguridad de red (incluye firewalls), y se han establecido políticas para el acceso de suscriptores y terceros que confían, conforme se encuentra definido en el documento “Control de Acceso Lógico”.
b) La TSA asegura la efectiva administración de accesos de usuarios (incluyendo a operadores, administradores y auditores) para mantener la seguridad de los sistemas, incluyendo gestión de cuentas de usuario, auditoría y modificación periódica o remoción de acceso
c) La TSA asegura que el acceso a las aplicaciones es restringida en concordancia con la política de control de acceso y que los sistemas de la TSA proveen suficientes controles informáticos para permitir la separación de roles, particularmente entre las funciones de administrador y la de operador. En particular, el uso de programas utilitarios es restringido y controlado estrictamente

d) Solo el personal autorizado puede acceder a las aplicaciones críticas relacionadas a las actividades de sellado de tiempo. Para mayor detalle se puede consultar el documento “Control de Acceso Lógico” y la CPS de ECEP-RENIEC, ítem 5.1.2. “Acceso físico”.
e) Todas las actividades de la operación de la TSA-RENIEC se almacenan en registros de auditoría.
f) Los dispositivos y equipos de red son protegidos en un ambiente aislado de otras áreas y que su configuración es auditada periódicamente respecto del cumplimiento de los requerimientos especificados por la TSA
g) Se ha implementado un sistema de monitoreo continuo del servicio de la TSA-RENIEC, además se cuenta con sistemas de para detectar, registrar y reaccionar oportunamente sobre intentos no autorizados de acceso a los recursos de la TSA

7.4.7. Mantenimiento y despliegue de sistemas confiables

La TSA-RENIEC utiliza sistemas y productos confiables que están protegidos contra modificaciones no autorizadas.

- La TSA-RENIEC utiliza productos confiables los cuales garantizan que los requerimientos de seguridad han sido contemplados en su diseño y construcción.
- Cuando se requiere realizar cambios a los sistemas de soporte de la TSA-RENIEC se sigue lo indicado en el documento "Control de cambios a sistemas" de la ECEP-RENIEC.

Dentro de la operación de la TSA-RENIEC, la generación de llaves se lleva a cabo mediante una ceremonia de llaves.

7.4.8. Compromiso de los servicios de la TSA

En caso que los servicios de la TSA-RENIEC se vean comprometidos o se pierda la exactitud de los sellos de tiempo, la información relevante será comunicada a los usuarios del servicio y se interrumpirá el servicio.

Se procederá a la realización de una nueva ceremonia de llaves para la generación de un nuevo certificado TSA o se procederá a utilizar otro certificado vigente de la TSA-RENIEC que no haya sido comprometido.

7.4.9. Terminación de la TSA

La TSA-RENIEC garantiza la minimización del impacto en caso de cese del servicio de sellado de tiempo. En particular, asegura la continuidad de la información requerida para verificar el estado de los sellos de tiempo.

a) En caso de cese de actividad voluntaria, la TSA-RENIEC, realizará con una antelación mínima de treinta (30) días, las siguientes acciones:
   - Informar a todos los subscriptores y terceros que confían del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.
   - Comunicar a la AAC, conforme a lo indicado en el documento “Cese de actividades de entidad raíz y de nivel intermedio”, del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.

b) No aplica a la TSA-RENIEC el tener acuerdos para cubrir los costos de cumplir los requisitos mínimos, en caso de que la TSA se declarara en quiebra o por otras razones sea incapaz de cubrir los costos por sí misma.

c) La TSA ha declarado en su Declaración de prácticas y políticas de sellado de tiempo, las provisiones para la terminación del servicio, esto incluye:
   - Notificación a todos los suscriptores y terceros que confían la información concerniente a su terminación.
   - Transferir las obligaciones a los terceros que confían de mantener los registros de eventos y archivos auditables necesarios para demostrar la correcta operación de la TSA por un periodo razonable.

d) Tomar medidas para que los certificados de los TSU sean revocados, esto de acuerdo al documento: ""Cese de actividades de entidad raíz y de nivel intermedio”.

7.4.10. Cumplimiento de requisitos legales

La TSA-RENIEC cumple con los requisitos legales indicados en la “Guía de Acreditación de Prestador de Servicios de Valor Añadido”, los lineamientos del RFC 3628, lo lineamientos indicados en el RFC 3161, la Ley de Firmas y Certificados Digitales y su reglamento

7.4.11. Registro de información concerniente a la operación de los servicios de sellado de tiempo

La TSA asegura que toda la información relevante concerniente a la operación de los servicios de sellado de tiempo es registrada por el periodo de 10 años, ver punto 5.4.3. Periodo de conservación del registro de auditorías de la CPS de la ECEP-RENIEC, esto con el propósito de proveer evidencia para procesos legales.

a) Los eventos y datos específicos son almacenados en los registros de auditoría y están documentados, esto según el documento "Gestión de registros de auditoría" de la ECEP-RENIEC.

b) La TSA-RENIEC mantiene la confidencialidad e integridad de los registros concernientes a la operación de los servicios de sellado de

tiempo, durante todo su ciclo de vida, esto según el documento "Gestión de registros de auditoría"

c) La TSA-RENIEC conserva y mantienen confidencialmente todo registro concerniente a la operación de los servicios de sellado de tiempo.
d) Los registros concernientes a la operación de los servicios de sellado de tiempo deberán están disponibles si son requeridos para propósitos de proveer evidencia de la correcta operación del servicio para propósitos de procesos legales.
e) La TSA-RENIEC registra la fecha y hora exacta de ocurrencia de eventos significativos tales como gestión de llaves y sincronización del reloj.
f) Los registros concernientes a los servicios de sellado de tiempo son ser protegidos y almacenados por un periodo de tiempo de un año después de la expiración de la validez del certificado digital de la TSU para proveer la evidencia legal necesaria.
g) Los registros de eventos son almacenados en copias internas y externas, esto para evitar su manipulación.
h) La TSA-RENIEC no procesa datos personales asociados a las operaciones de la TSA-RENIEC, por lo tanto, la Ley N° 29733 Ley de Protección de Datos Personales y su Reglamento, así como la norma de Marco sobre Privacidad del APEC no son de alcance a la prestación del servicio de sellado de tiempo.
i) Se registran los eventos relacionados con el ciclo de vida de las llaves de los TSU.
j) Se registran los eventos relacionados con el ciclo de vida del certificado de la TSA-RENIEC.
k) Se registran los eventos relacionados con la sincronización del reloj de la TSA-RENIEC.
l) Se registran los eventos relacionados a la detección de perdida de la sincronización.

7.5. Aspectos organizacionales

Los aspectos organizacionales corresponden a:

a) La TSA-RENIEC asegura que las políticas y procedimiento bajo los que opera no son discriminatorios.
b) La TSA-RENIEC permite el acceso a sus servicios a todos los solicitantes cuyas actividades estén comprendidas dentro de su ámbito de operación y que se compromete a cumplir según lo especificado en la declaración de divulgación de la TSA.
c) La TSA-RENIEC es una autoridad de sellado de tiempo de acuerdo a la IOFE.
d) La TSA-RENIEC tiene un sistema ISO 9001 para la gestión de calidad de los servicios de sellado de tiempo que provee.
e) La TSA cuenta con disposiciones adecuadas para cubrir las obligaciones derivadas de su operación y/o actividades.
f) No aplica a la TSA-RENIEC el cumplimiento del criterio de estabilidad financiera, por ser una entidad del Estado Peruano
g) La TSA-RNIEC cuenta con personal altamente calificado, con la educación, entrenamiento, conocimiento técnico y experiencia para proveer el servicio de sellado de tiempo. El personal de la TSA-RENIEC está vinculado contractualmente con el RENIEC en el

desempeño de funciones de soporte de los servicios de sellado de tiempo de la TSA.

h) El RENIEC tiene políticas y procedimientos para resolución de quejas y reclamos recibidos por clientes o terceros sobre la provisión del servicio de sellado de tiempo u otros servicios relacionados.

i) El servicio de sellado de tiempo es brindado íntegramente por la TSA-RENIEC, y no por terceros en la prestación de este servicio.

8. CONSIDERACIONES DE SEGURIDAD

Cuando se realiza la verificación de los sellos de tiempo, es necesario asegurar que el certificado de la TSU se encuentre vigente y no revocado, además, que haya sido emitido por una entidad confiable dentro del marco de la IOFE. Es decir, se tiene que verificar el estado de revocación de la entidad raíz, en este caso de la ECERNEP, y luego el estado de revocación del certificado de la TSU.

Cuando se verifica un sello de tiempo como válido en un instante de tiempo dado, esto no quiere decir que se mantendrá necesariamente válido en el futuro. Cada vez que un sello de tiempo es verificado dentro del periodo de validez del certificado del TSU, es necesario también verificar el estado de revocación actual de la TSU, ya que, en caso de compromiso de la llave privada del TSU, todos los sellos de tiempo generados por ese TSU se vuelven inválidos.

En particular, al configurar la URL de la TSA-RENIEC en un software, es necesario verificar que el software se encuentre acreditado ante la AAC para asegurar que todo el procedimiento de generación del pedido y el sellado se realiza dentro de lo indicado en este documento y la normativa vigente.

9. BIBLIOGRAFÍA.

Para la redacción del presente documento se utilizó:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105-2012-PCM.
- RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. Internet Engineering Task Force (IETF) (sustituye al RFC 2527).
- Norma Técnica Peruana “NTP-ISO/IEC 17799:2001 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición (de uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática conforme lo dispone la Resolución Ministerial Nº 246-2007-PCM publicada el 25 de junio de 2007).
- RFC 3161: “Time-Stamp Protocol” Internet Engineering Task Force (IETF)