RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identidad digital
GERENCIA DE CERTIFICACION Y REGISTRO DIGITAL

CÓDIGO: DP-SVA-GRCD/SGCID-002-ROOT3

DECLARACIÓN DE PRÁCTICAS DE SERVICIO DE VALOR AÑADIDO

PRESTADORES DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

Autoridad de Sellado de Tiempo

TSA-RENIEC

Versión: 2.0	**Año: 2018**

Elaborado por: Sub Gerencia de Certificación e Identidad Digital	**Revisado por:** Sub Gerente de Certificación e Identidad Digital	**Aprobado por:** Gerencia de Registros de Certificación Digital

Historial de Cambios				
Ver.	**Fecha de cambio**	**Descripción**	**Responsable**	**Estado**
1.0	15/12/2017	Elaboración y aprobación	GRCD/SGCID	Aprobado
2.0	30/10/2018	Revisión y actualización	GRCD/SGCID	Aprobado

INDICE

INTRODUCCIÓN

El sellado de tiempo o *timestamping* es un mecanismo que permite verificar que una serie de datos han existido en un instante de tiempo. El protocolo de sellado de tiempo para el uso con certificados X.509 se describe en el RFC3161 y la norma ETSI EN 319 422. Además, en el ETSI EN 319 421[1] se define la Política y Requerimientos de Seguridad para un PSVA en la modalidad de TSA. .

El RENIEC, en su calidad de Prestador de Servicios de Valor Añadido, ofrece el servicio de sellado de tiempo (TSA) y define, en la presente Declaración de Prácticas, los lineamientos, condiciones necesarias y características técnicas para la prestación del servicio, cumpliendo con lo dispuesto por la ECERNEP en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo y en la Política General de Certificación (CP) de la jerarquía ECERNEP PERU CA ROOT 3.

1. VISIÓN GENERAL

Este documento describe de qué manera la PSVA-TSA-RENIEC implementa los procedimientos y controles para cumplir con los requerimientos dados en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo de la jerarquía PKI "ECERNEP PERU CA Root 3".

1.1. Repositorio

El PSVA-TSA-RENIEC gestiona repositorios accesibles desde Internet, con la siguiente información:

- Certificados digitales de TSU.
- Declaración de Prácticas de Servicio de Valor Añadido en la modalidad de Autoridad de Sellado de Tiempo (DPSVA-TSA)

Estos repositorios se encuentran accesibles en la Web, específicamente en:

- http://www.reniec.gob.pe/crt/
- http://www.reniec.gob.pe/repository/
- https://pki.reniec.gob.pe/repositorio/

1.2. Frecuencia de publicación

El PSVA-TSA-RENIEC gestiona y actualiza sus repositorios conforme a la siguiente frecuencia:

- Certificados digitales de TSU: Actualizado cada vez que se emite un nuevo certificado digital.
- Repositorio de la Declaración de Prácticas del PSVA-TSA-RENIEC: Actualizado anualmente o cada vez que la AAC aprueba una nueva versión.

[1] ETSI EN 319 421, publicado anteriormente como ETSI TS 102 023

1.3. Control de acceso a los repositorios

El PSVA-TSA-RENIEC no limita el acceso de lectura a la información en sus repositorios, pero establece controles físicos y lógicos para impedir que de forma no autorizada se puedan añadir, modificar o borrar registros del Repositorio, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad e integridad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

Los repositorios del PSVA-TSA-RENIEC son administrados, publicados y gestionados por la propia organización.

2. REFERENCIAS

2.1. Referencias Normativas

Los siguientes documentos son necesarios para la aplicación de la presente Declaración de Prácticas:

- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- Guía de Acreditación para PSVA-TSA 4.0 (2017)

2.2. Referencias Informativas

Los siguientes documentos no son necesarios para la aplicación de la presente Declaración de Prácticas, pero pueden ayudar a comprender mejor la aplicación de la PKI.

- RFC 3161[2], RFC 5816[3] y requisitos adicionales del ETSI EN 319 422
- Ley de Firmas y Certificados Digitales Nº 27269
- Reglamento de la Ley DS 052-2008/PCM

3. DEFINICIONES Y ABREVIATURAS

Ver Anexo 1

4. CONCEPTOS GENERALES

4.1. Requerimientos de la Política General

El presente documento es una declaración de "CÓMO uno se adhiere" a los requisitos establecidos en la Política Declaración de Prácticas de Valor añadido. Además, se incluye la Declaración de Libre Divulgación del PSVA-TSA-RENIEC.

[2] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[3] ESSCertIDv2 Update for RFC 3161

Esta declaración de prácticas de servicio sellado de tiempo está basada en el uso de criptografía de llave pública, certificados de llave pública y fuentes de tiempo confiables.

Los suscriptores del servicios y terceros que confían deberán consultar el presente documento para obtener los detalles de CÓMO se implementa el servicio de sellado de tiempo del PSVA-TSA-RENIEC.

4.2. Servicio de Sellado de Tiempo (TSS)

El servicio de sellado de tiempo de la PSVA-TSA-RENIEC consta de dos componentes:

- Provisión: Este componente del servicio genera los sellos de tiempo, propiamente dichos.
- Administración: Este componente del servicio controla y monitorea la operación de los servicios para asegurar que sean provistos de acuerdo a lo especificado en el presente documento. Además, es responsable de la activación o desactivación de la provisión del servicio.

4.3. Autoridad de Sellado de Tiempo (TSA)

Es la autoridad que emite sellos de tiempo en los que confían los usuarios de sellado de tiempo, es decir, los suscriptores del servicio y los terceros que confían.

La PSVA-TSA-RENIEC, debidamente acreditada ante la AAC, opera brindando el servicio de sellado de tiempo como subordinado a la EC-PSVA de la jerarquía ECERNEP PERU CA ROOT 3 y es responsable de brindar los servicios identificados en el numeral 4.1
Además, la PSVA-TSA-RENIEC emite los sellos de tiempo a través de uno o más TSU (Unidad de Sellado de Tiempo), cada uno con su par de llaves y certificado digital propios.

4.4. Suscriptor del servicio

El suscriptor del servicio puede ser cualquier Entidad Pública que solicite el servicio, obligándose a cumplir lo exigido mediante un contrato o convenio.

La Entidad será responsable de aquellas obligaciones que no se cumplan correctamente y de las consecuencias de las mismas.

4.5. Política de Sellado de Tiempo y Declaración de Prácticas de la TSA

La Declaración de Prácticas de Valor Añadido del PSA-TSA-RENIEC sigue la misma estructura que la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo, definida por la norma europea ETSI EN 319 421.

5. INTRODUCCIÓN A LAS POLÍTICAS DE SELLADO DE TIEMPO Y REQUERIMIENTOS GENERALES

5.1. Visión General

Una política de sellado de tiempo es un conjunto de reglas que definen la aplicabilidad de un sello de tiempo a una comunidad en particular y/o tipo de uso con requisitos de seguridad comunes.

Este documento implementa los requisitos definidos en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo de la jerarquía ECERNEP PERÚ CA ROOT 3, de acuerdo a lo señalado en el numeral 4.1 Requerimientos de la Política General.

El perfil de los certificados del PSVA-TSA-RENIEC, utilizados en la emisión de los sellos de tiempo, es el siguiente:

Perfil de Certificado PSVA-TSA-XX				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	EC-PSVA	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	12 años	Sí	-
Subject	CN	PSVA-TSA-RENIEC TSU-<código de TSU>	-	-
	O	Registro Nacional de Identificación y Estado Civil	Sí	
	C	PE	Sí	
Subject Public Key Info	algorithm	RSA	-	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	No
Certificate Policies	policyIdentifier (OID)	**1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0**	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	**0.4.2023.1**		
	cPSuri	-		
	explicitText	ETSI baseline time stamping policy		

Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	Time Stamping (1.3.6.1.5.5.7.3.8)	Sí	Sí
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecpsva.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecpsva.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecpsva.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	Sí	No
OCSP no check	-	-	-	-

5.2. Identificación

La presente Declaración de Prácticas tiene como OID asignado, dentro de la jerarquía ECERNEP PERÚ CA ROOT 3, el número 1.3.6.1.4.1.35300.2.1.3.2.0.105.1000.0

5.3. Comunidad de usuarios y aplicabilidad

La comunidad de usuarios está compuesta por los suscriptores del servicio, descritos en el numeral 4.4 Suscriptor del servicio, que cuentan con la autorización respectiva de la TSA para hacer uso del servicio y por los 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 el PSVA-TSA-RENIEC y que confía en la jerarquía ECERNEP PERÚ CA ROOT 3, tal como se indica en la Política de Servicio de Valor Añadido.

6. POLÍTICAS Y PRÁCTICAS

6.1. Evaluación de Riesgos

La PSVA-TSA-RENIEC, de acuerdo con lo indicado en la cláusula 5 de la norma europea ETSI 319 401, realiza una evaluación de riesgos anualmente, identificando los activos y las amenazas a dichos activos, determinando los controles de seguridad necesarios para mitigar los riesgos identificados.

6.2. Declaración de Prácticas de la TSA

El PSVA-TSA-RENIEC brinda el servicio de sellado de tiempo, según lo referido en la cláusula 6.1 de la norma europea ETSI EN 319 401[4], conforme a lo siguiente:

a) El algoritmo utilizado para representar los datos a los que se aplica el sello de tiempo es SHA-256, tal como se indica en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo.

[4] Se cumple con los requisitos del REQ-6.1-01 al REQ-6.1-11.

b) La precisión del tiempo utilizado en los sellos de tiempo emitidos por el PSVA-TSA-RENIEC, se encuentra en conformidad con el estándar NTP que establece la precisión mínima respecto al UTC de ± 1 segundo.
c) El RENIEC no se hace responsable por la veracidad o contenido de los datos sellados por el PSVA-TSA-RENIEC., ni por cualquier pérdida, daños indirectos o consecuentes o pérdida de datos por la utilización del servicio dentro de un software no confiable o propiedad de un tercero. Además, no será responsable por los daños que se resulten por el incumplimiento de las obligaciones del suscriptor del servicio o tercero que confía respecto a los términos y condiciones de uso, incluyendo el exceso en el límite establecido para las transacciones.
d) Las obligaciones de los suscriptores del servicio se detallan en el 6.5.3Obligaciones de los suscriptores del servicio.
e) Las obligaciones de los terceros que confían se detallan en el numeral 6.6 Información para los terceros que confían.
f) La información para que los terceros que confían puedan validar los sellos de tiempo emitidos por PSVA-TSA-RENIEC, se definen en el numeral 6.6.
g) En caso de consultas, reclamos o disputas relacionados con el Servicio de Valor Añadido-Sellado de Tiempo brindado por la TSA-RENIEC, remitirlo al correo electrónico identidaddigital@reniec.gob.pe

El PSVA-TSA-RENIEC brinda el servicio de sellado de tiempo, con un mínimo de tiempo de disponibilidad del 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

En el Anexo 02, se encuentra la Declaración de Libre Divulgación del PSA-TSA-RENIEC.

6.3. Términos y condiciones del servicio

El PSVA-TSA-RENIEC gestiona el servicio de sellado de tiempo con el suscriptor del servicio mediante contrato o convenio, en el cual se incluyen las obligaciones de ambas partes tal como se definen los numerales 6.5.2 Obligaciones de la TSA con los suscriptores y 6.5.3Obligaciones de los suscriptores del servicio.

6.4. Información de política de seguridad

a) El PSVA-TSA-RENIEC gestiona su seguridad de la información conforme al ISO 27001.
b) Cada vez que se requiere un cambio en las políticas de seguridad de la información, se coordina y comunica al Oficial de Seguridad de la Información.

6.5. Obligaciones de la TSA

6.5.1. Generalidades

El RENIEC, en su calidad de Prestador de Servicios de Valor Añadido cumple con implementar todos los requerimientos de sellado de tiempo detallados en el numeral 7, en base a la Política de Servicios de Valor Añadido Servicio de Sellado de Tiempo.

El RENIEC gestiona el servicio Sellado de Tiempo por sí mismo, sin la intervención de terceros.

6.5.2. Obligaciones de la TSA con los suscriptores

El PSVA-TSA-RENIEC está obligado a:

• Emitir sellos de tiempo de acuerdo al protocolo de sellado de tiempo indicado en el RFC 3161 y los requerimientos adicionales del ETSI EN 319 422.

• Proteger las llaves privadas emitidas para cada una de sus TSU.

• Garantizar que la precisión de la hora y fecha utilizada en los sellos de tiempo emitidos por el PSVA-TSA-RENIEC, se encuentra en conformidad con el estándar NTP que establece la precisión mínima respecto al UTC de ± 1 segundo.

• Publicar este documento y los relacionados al servicio, garantizando el acceso a la versión actual.

• Brindar el servicio de sellado de tiempo, con disponibilidad del 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

6.5.3. Obligaciones de los suscriptores del servicio

El suscriptor está obligado a:

- Cumplir los términos y condiciones descritos en el contrato o convenio celebrado con la PSVA-TSA-RENIEC.
- Utilizar un software de firma confiable y acreditado dentro de la IOFE que realice la verificación del certificado que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL provista por la EC-PSVA, o a través de otro mecanismo de consulta que ésta ponga a disposición.
- Tener en cuenta cualquier limitación de la responsabilidad del PSVA-TSA-RENIEC, conforme a lo indicado en el numeral 6.7 Limitaciones a la responsabilidad.

6.6. Información para los terceros que confían

Los terceros que confían están obligados a:

- Utilizar un software de firma confiable y acreditado dentro de la IOFE que realice la verificación del certificado que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL provista por el PSVA-TSA-RENIEC.
- Tener en cuenta cualquier limitación en el uso del sello de tiempo, conforme a lo indicado en el numeral 6.7 Limitaciones a la responsabilidad.
- Tener en cuenta cualquier otro requisito o precaución que publique la ECERNEP en su sitio web (https://pki.reniec.gob.pe/repositorio/) o la TSA en la dirección web que determine en su VAPS, los que no deberán contravenir lo establecido en la Ley de Firmas y Certificados Digitales, su Reglamento, normas complementarias y sustitutorias, y en la CP de la ECERNEP

6.7. Limitaciones a la responsabilidad

El PSVA-TSA-RENIEC no será en ningún caso responsable cuando se encuentra en alguna de las siguientes circunstancias:

- Estado de guerra, desastre natural o cualquier otra causa de fuerza mayor, incluida el funcionamiento defectuoso de los servicios de las redes telemáticas de los ISP (Proveedores de Internet), fluido eléctrico o equipos informáticos de terceros.

- Por el uso que se pueda realizar de los sellos de tiempo, en especial por el contenido de los mensajes o documentos sellados.

6.8. Procedimiento sobre resolución de disputas

En caso la disputa esté directamente relacionado con el Servicio de Valor Añadido-Sellado de Tiempo brindado por la TSA-RENIEC, se atenderá en un plazo de 48 horas y deberán dirigirse al siguiente contacto:

- **Contacto:** Sub Gerente de Certificación e Identidad Digital.
- **Dirección de correo electrónico:** identidaddigital@reniec.gob.pe
- **Dirección:** Jr. Bolivia 109, Centro Cívico, Cercado de Lima
- **Número de teléfono:** 3152700

7. Gestión y operación de la PSVA-TSA-RENIEC

7.1. Introducción

La provisión de un sello de tiempo, en respuesta a una solicitud, se gestiona a discreción de la PSVA-TSA-RENIEC, dependiendo del nivel de servicio acordado con el suscriptor del servicio, mediante contrato o convenio.

7.2. Organización interna

Según se indica en el numeral 7.2 de la norma europea ETSI EN 319 421, se aplican los requisitos indicados en la cláusula 7.1 de la norma europea ETSI EN 319 401[5]

a) El PSVA-TSA-RENIEC es operada por el Registro Nacional de Identificación y Estado Civil (RENIEC).
b) El PSVA-TSA-RENIEC forma parte del Sistema de Gestión de la Calidad y Sistema de Seguridad de la Información del RENIEC, apropiado para el servicio de sellado de tiempo que brinda.
c) El PSVA-TSA-RENIEC emplea personal suficiente para proveer el servicio que tengan experiencia y capacidades necesarias, previamente verificadas por el área de recursos humanos del RENIEC, antes de ser contratados.
d) El PSVA-TSA-RENIEC es confiable pues es operada por el RENIEC, como se indica en el literal a).
e) El PSVA-TSA-RENIEC cuenta con políticas y procedimientos no discriminatorios. El servicio se brinda a todas las entidades públicas que lo soliciten, de acuerdo al numeral 5.3 Comunidad de usuarios y aplicabilidad.
f) El PSVA-TSA-RENIEC poner a disponibilidad de los suscriptores del servicio al sellado de tiempo, de acuerdo a las obligaciones descritas en el numeral 6.5.2 Obligaciones de la TSA con los suscriptores.
g) El PSVA-TSA-RENIEC, al ser operado por el RENIEC, cuenta con recursos del Estado peruano para cumplir con el servicio, según la normativa peruana y operar de acuerdo a lo declarado.

[5] Requisitos del REQ-7.1.1-02 al REQ-7.1.1-07 y REQ-7.1.2-01

h) En caso de consultas, reclamos o disputas el PSVA-TSA-RENIEC responderá mediante correo electrónico a la cuenta identidaddigital@reniec.gob.pe
i) El PSVA-TSA-RENIEC opera con personal propio y no cuenta con servicios tercerizados.
j) El PSVA-TSA-RENIEC define los roles que requieren separación de funciones, sin que esto se excluyente para las siguientes actividades:
    - Generación, emisión o destrucción del par de llaves y certificados digitales de los TSU.
    - Acceso y gestión de los repositorios y base de datos.
    - Auditoría interna.

En general, las personas que se encargan de la implementación de una función, no tienen el rol de realización de la auditoría, evaluación o revisión de dicha implementación.

7.3. Seguridad del personal

a) El PSVA-TSA-RENIEC asegura la confianza en la provisión del servicio mediante la gestión apropiada de sus activos y sensibilizaciones o capacitaciones a su personal sobre Seguridad de la información, al menos una vez al año.
b) El PSVA-TSA-RENIEC, selecciona a sus trabajadores y contratistas según los literales c) e i) del numeral 7.2 Organización interna.
c) Se toman acciones administrativas y disciplinarias apropiadas contra el personal que, independientemente de la modalidad de contratación, ejecute acciones no autorizadas dentro de sus funciones o que viole las normas de seguridad, según lo indique el reglamento interno del RENIEC. Se consideran acciones no autorizadas las que contravengan, de manera negligente o malintencionada a la Política de Servicios de Valor Añadido, la Declaración de Prácticas de Servicios de Valor Añadido, así como a los documentos normativos de alcance al personal de la entidad.
d) Se cuenta con un documento oficial en el cual, el área encargada de la operación del PSVA-TSA-RENIEC, asigna los roles de seguridad y de confianza identificando las funciones más relevantes, incluyendo sus responsabilidades. La persona asignada acepta las funciones que se le encargan.
e) El personal del PSVA-TSA-RENIEC, tanto temporal como permanente, cuenta con la descripción de su puesto de trabajo en su contrato, orden de servicio u otro documento pertinente.
f) Todos los procedimientos administrativos o técnicos se realizan bajo el lineamiento de del ISO/IEC 27001 de Seguridad de la Información.
g) El personal de gestión del PSVA-TSA-RENIEC cuenta con las siguientes características:
    - Conocimientos de la tecnología de sellado de tiempo.
    - Familiaridad con procedimientos de seguridad de la información para gestionar al personal que cumple roles de seguridad.
    - Experiencia con seguridad de la información y evaluación de riesgos.

h) El PSVA-TSA-RENIEC no designa, para roles de confianza o de gestión, a cualquier persona que haya recibido sentencia por un crimen de gravedad u otro delito que afecte su idoneidad para el puesto. El personal no tiene acceso a las funciones de confianza hasta que se hayan efectuado las verificaciones necesarias. Esta verificación la realiza el área encargada de Recursos Humanos de la Entidad.
i) El personal del PSVA-TSA-RENIEC es designado oficialmente por la Entidad (RENIEC) para el puesto que ocupa dentro del área encargada del servicio de sellado de tiempo.
j) El personal no tiene acceso a las funciones de confianza hasta que se hayan efectuado las verificaciones necesarias. Esta verificación la realiza el área encargada de Recursos Humanos de la Entidad.
k) Todo el personal en roles de confianza debe encontrarse libre de conflicto de interese que pudiera perjudicar la imparcialidad de las operaciones del PSVA-TSA-RENIEC.

7.4. Gestión de activos

El PSVA-TSA-RENIEC realiza un inventario, clasificación y gestión de sus activos físicos y lógicos, evaluando los riesgos identificados y controles implementados, en base a lo establecido en el estándar ISO/IEC 27001.

7.5. Control de acceso

a) El acceso físico y lógico a los sistemas e instalaciones del PSVA-TSA-RENIEC se otorga solamente a personas autorizadas mediante controles biométricos o credenciales de acceso a los sistemas, respectivamente.
b) La red está protegida por controles, tales como, firewalls, sistemas de detección de intrusos, antivirus y DMZ.
c) Los firewalls cuentan con los protocolos necesarios para prevenir los accesos no autorizados.
d) Los sistemas del PSVA-TSA-RENIEC cuentan con usuarios de nivel administrador, operador y revisor de logs. Cada cuenta de usuario tiene diferente acceso, de acuerdo a las políticas de control de acceso.
e) Se realiza actualizaciones de las credenciales de acceso a los sistemas del PSVA-TSA-RENIEC, según el procedimiento aprobado.
f) Las personas que se encargan de las funciones de operación dentro del PSVA-TSA-RENIEC, no tienen el rol de la gestión de la seguridad de dicha función.
g) En caso de trabajadores nuevos, el área de recursos humanos del RENIEC realiza la confirmación de identidad del personal que inicia labores en las instalaciones del PSVA-TSA-RENIEC. Por otro lado, en caso de proveedores o visitas, antes de ingresar o realizar labores en los equipos del PSVA-TSA-RENIEC, se identifican mediante su documento de identidad.
h) El personal del PSVA-TSA-RENIEC es responsable de las actividades asignadas a su cargo.
i) La información que se requiere eliminar, es destruida física o lógicamente a fin de evitar la posibilidad de su recuperación.

7.6. Controles criptográficos

7.6.1. General

El PSVA-TSA-RENIEC cuenta con equipos criptográficos que cumplen con altos estándares de seguridad, tales como Common Criteria EAL4+ y FIPS 140-2 nivel 3, los cuales han sido evaluados ante vulnerabilidades por los fabricantes.

7.6.2. Generación de llaves de TSU

El par de llaves o los pares de llaves del PSVA-TSA-RENIEC se generan bajo las siguientes consideraciones:

a) En un ambiente que cuenta con seguridad de acceso físico mediante control biométrico, y registrando en acta y logs el procedimiento realizado. Este procedimiento es realizado por personal de confianza.
b) Las llaves se generan en un módulo criptográfico HSM certificado y operando bajo los estándares FIPS 140-2 nivel 3, que requiere control multipersonal (k de m) para su uso.
c) El algoritmo de generación de llaves es RSA con un tamaño de 2048 bits.
d) En caso se requiera contar con las llaves firmadoras en otro módulo criptográfico, se generan nuevas llaves en el nuevo módulo criptográfico.
e) Los TSU del PSVA-TSA-RENIEC utilizan una llave de firma a la vez.

7.6.3. Protección de la llave privada de TSU

a) La TSA-RENIEC almacena y usa sus llaves privadas en los módulos criptográficos que fueron generadas, según lo especificado en el numeral 7.6.2 Generación de llaves de TSU.

   En caso se requiera contar con las llaves firmadoras en otro módulo criptográfico, se generan nuevas llaves en el nuevo módulo criptográfico.
b) Los procedimientos de copia, almacenamiento y recuperación de llaves del PSVA-TSA-RENIEC, son realizados por personal en roles de confianza.
c) Se realiza al menos una copia de respaldo de las llaves privadas del PSVA-TSA-RENIEC utilizando algoritmos de cifrado, aprobados en conformidad con la certificación FIPS 140-2 nivel 3 del módulo criptográfico HSM donde éstas se generaron. De esta manera, se asegura su confidencialidad e integridad.

7.6.4. Certificado de llave pública de TSU

a) La llave pública de los TSU del PSVA-TSA-RENIEC se encuentran disponibles en los certificados digitales x.509 v3 correspondientes, que son distribuidos en el repositorio http://crl.reniec.gob.pe/root3/tsu/
b) Los certificados del PSVA-TSA-RENIEC, son emitidos por la EC-PSVA, que a su vez es emitido por la raíz de la jerarquía ECERNEP PERÚ CA ROOT 3, según se indica en la Política General de Certificación de la ECERNEP.
c) El TSU no emite sellos de tiempo hasta que el certificado digital (llave pública), emitido por la EC-PSVA, no haya sido cargado dentro del módulo criptográfico HSM correspondiente.

7.6.5. Reemisión de la llave TSU

El PSVA-TSA-RENIEC emite certificados digitales con un tiempo de validez de 12 años. Para asegurar un sello de tiempo que sea verificable al menos durante 10 años[6], se generan nuevos certificados cada año, permitiendo que lo anteriores sigan disponibles solamente para verificación, pero no para generar nuevos sellos de tiempo, de acuerdo al procedimiento establecido.

7.6.6. Gestión del ciclo de vida del hardware criptográfico de firma

a) El hardware criptográfico del PSVA-TSA-RENIEC es trasladado por personal con roles de confianza para asegurar que no se manipula durante su traslado.
b) Si el hardware criptográfico del PSVA-TSA-RENIEC necesitara ser almacenado, se colocaría en un lugar seguro y por personal con roles de confianza para asegurar que no se manipula ni al momento de ser guardado ni durante el tiempo que permanezca guardado.
c) La instalación, activación y duplicado de llaves TSU se realizan solamente por personal de con roles de confianza, según las especificaciones y el entorno seguro del hardware utilizado.
d) Se realiza un borrado seguro del hardware criptográfico, cuando se le da de baja, de tal manera que las llaves que se encontraban almacenadas no puedan ser recuperadas.
e) El PSVA-TSA-RENIEC garantiza que los módulos criptográficos donde se encuentran las llaves de los TSU funcionan correctamente.

7.6.7. Término del ciclo de vida de la llave del TSU

a) Se cuenta con un documento aprobado que indica el procedimiento para generar y poner en producción nuevas llaves de TSU.
b) Al final del periodo de validez, todas las copias y las llaves expiradas son destruidas de tal manera que no se puedan recuperar.
c) La fecha de expiración de las llaves de los TSU se encuentran declarados en un procedimiento.

7.7. Sellado de tiempo

7.7.1. Emisión del sello de tiempo

La TSA-RENIEC emite sellos de tiempo que cumplen con el formato establecido por la recomendación RFC 3161 (OID de Política, identificador único y hash) con los requerimientos adicionales ETSI EN 319 422. En particular, cada sello de tiempo contiene:

[6] La Ley de Firmas y Certificados indica que los registros se deben guardar al menos 10 años. El sello de tiempo del PSVA-TSA-RENIEC permite, entonces, que los documentos digitales sellados puedan ser verificados durante más de los 10 años que indica la norma.

a) La fecha y hora en la que fue generado el sello de tiempo proveniente de un laboratorio UTC(k).
b) La fecha y hora incluidas en el sello de tiempo se sincroniza con el UTC con una desviación no mayor a ± 1 segundos.
c) Si el reloj del PSVA-TSA-RENIEC se detecta como fuera de tiempo por una desviación de al menos 0.5 segundos, inmediatamente se lanza una alerta al correo electrónico ntp@pkiep.reniec.gob.pe.
d) El sello de tiempo es firmado únicamente utilizando llaves privadas emitidas exclusivamente para dicho propósito.
e) El sistema de generación de sellos de tiempo rechaza cualquier intento de emisión de sellos cuando la el periodo de validez de la llave privada ya expiró.
f) El sello de tiempo incluye el OID de la Declaración de Prácticas alineada a la Política de Valor Añadido.
g) Cada sello de tiempo tiene un identificador único.
h) El sello contiene un resumen hash de los datos sellados

7.7.2. Sincronización del reloj con el UTC

El PSVA-TSA-RENIEC cuenta con un servidor horario que cumple con el protocolo NTP y su reloj se mantiene sincronizado con el UTC dentro del nivel de precisión de ± 0.5 segundo.

En particular:

a) La calibración de los relojes de las TSU se mantiene de forma tal que no debe esperarse que se salgan de la precisión declarada, ya que el PSVA-TSA-RENIEC cuenta con dos (02) servidores horarios NTP.
b) La precisión de los relojes es de ± 0.5 segundos con respecto al UTC.
c) Los relojes del PSVA-TSA-RENIEC se protegen contra amenazas que pudiesen resultar en cambios no detectados que puedan afectar su calibración.
d) El PSVA-TSA-RENIEC detecta que la fecha y hora del equipo se encuentra calibrado antes de aplicar el sello.
e) Cuando se detecta que el sello de tiempo tiene fecha y hora fuera de calibración, se detiene la emisión de sellos.
f) Cuando se produce un *leap second*[7], notificado por el organismo correspondiente, se mantiene la sincronización de los relojes.

7.8. Seguridad física y del entorno

a) La TSA-RENIEC mantiene controles de seguridad físicos para impedir y prevenir el acceso a personas no autorizadas a los módulos criptográficos, como se indica en el numeral 7.6 Controles criptográficos.
b) Controles adicionales tales como:

[7] Un *leap second* es un ajuste al UTC añadiendo un segundo extra al último segundo de un mes UTC. La primera preferencia se da al final de diciembre y junio, la segunda preferencia se da al final de marzo y setiembre.

- Perímetro cerrado, piso y techo de concreto, sin ventanas y con puerta sólida.
- Personal de seguridad que sólo permite el ingreso a personas autorizadas. En caso de visitas, estas ingresan escoltadas por personal del PSVA-TSA-RENIEC.
- Los equipos y servidores computacionales necesarios para la operación del PSVA-TSA-RENIEC en un área de acceso biométrico restringido.
- Medidas de prevención ante desastres naturales (inundación, terremoto, entre otros) y ante desastres accidentales creados por el hombre (incendios, explosiones, disturbios civiles).
- Se cuenta con procedimientos para el traslado de equipos y medidas de seguridad para el envío de información.

c) Se cuenta con un Plan de Contingencia que permite continuar con la operación del negocio.

7.9. Seguridad de las operaciones

a) Se encuentran identificadas la capacidad actual de demanda de sellos de tiempo y los requerimientos para ampliar la capacidad en un futuro.
b) Para la emisión de sellos de tiempo, se utiliza software que cumple con el RFC 3161.
c) El PSVA-TSA-RENIEC no realiza desarrollo de software.
d) Se documenta el control de cambios en caso se requiera actualizar o cambiar el software o hardware del PSVA-TSA-RENIEC.
e) Los servidores donde se aloja el software del PSVA-TSA-RENIEC cuenta con protección contra virus y software malicioso.
f) Los equipos y servidores computacionales necesarios para la operación del PSVA-TSA-RENIEC en un área de acceso biométrico restringido
g) Los equipos se renuevan para contar con las versiones actuales y se les realiza mantenimientos preventivos y correctivos.
h) Los procedimientos se establecen para todos los roles de seguridad y confianza del PSVA-TSA-RENIC.
i) Se aplican los parches de seguridad en los servidores cada vez que se encuentran disponibles
j) No se aplican los parches de seguridad si introducen nuevas vulnerabilidades en mayor número que las ventajas de aplicarlos.
k) Se documentan las razones en caso no se apliquen los parches de seguridad.
l) La TSA mantiene responsabilidad por todos los aspectos de la provisión de servicios de sellado de tiempo bajo el alcance de la presente Declaración de Prácticas
m) Los medios de almacenamiento de datos utilizados en los sistemas confiables de la TSA son manipulados con seguridad para protegerlos del daño, robo, acceso no autorizado y obsolescencia.
n) Todos los medios de almacenamiento de datos se manipulan de forma segura, en concordancia con los requisitos del esquema de clasificación de la información (ver numeral 7.4 Gestión de activos).

7.10. Seguridad de red

La red tiene las siguientes características:

a) Protegida por controles, tales como, redes segregadas, firewalls, sistemas de detección de intrusos, antivirus y DMZ.
b) Los servicios y puertos que no se requieren, se encuentran desactivados.
c) Solamente los roles de confianza tienen acceso a las zonas seguras y de alta seguridad.
d) El PSVA-TSA-RENIEC trabaja con redes segregadas, con segmentos de red aislados de otras áreas de trabajo del RENIEC.
e) Se aplican los mismos controles de seguridad a todos los sistemas segregados en la misma zona de red.
f) Se realizan auditorías y revisión de controles periódicamente.
g) El hardware crítico para la operación del PSVA-TSA-RENIEC se encuentra en una zona segura, con control de acceso biométrico.
h) Se trabaja con redes dedicadas separadas para la administración y la operación del PSVA-TSA-RENIEC.
i) El servidor donde se encuentra el software de sellado de tiempo se utiliza exclusivamente para dicho fin.
j) Se separan el hardware y software de producción de los utilizados para pruebas y capacitaciones.
k) Se realiza una evaluación de vulnerabilidades desde la red interna y redes externas, periódicamente. Esta evaluación es realizada por un especialista en la materia, que no trabaja en la entidad.
l) Se realiza un test de penetración desde la red interna y redes externas, periódicamente. Esta evaluación es realizada por un especialista en la materia, que no trabaja en la entidad.
m) Se guardan las evidencias de los tests de penetración realizados.

7.11. Gestión de incidentes

a) Todas las actividades concernientes al acceso de sistemas, prendido y apagado de los servidores, login de los usuarios, uso de los sistemas y servicios se encuentra registrada en el archivo log de cada servidor.
b) Solo personal de confianza puede acceder a los archivos log de los sistemas con información sensible
c) Se cuenta con un sistema de monitoreo que emite alertas cuando el servicio no se encuentra disponible.
d) En caso de incidentes, el PSVA-TSA-RENIEC responderá mediante correo electrónico a la cuenta identidaddigital@reniec.gob.pe, en un plazo de 48 horas.
e) El personal en roles de confianza se encarga de monitorear las alertas de eventos de seguridad potencialmente críticos y se asegura de que se resuelvan según los lineamientos de seguridad de la información.
f) En caso se detecte una brecha de seguridad o pérdida de integridad, por ejemplo, compromiso de la llave TSU o pérdida de calibración, se notifica a

los suscriptores del servicio y terceros que confían dentro de las 24 horas de la detección.

g) Mediante las auditorías internas y externas, se realiza la revisión de los logs de los sistemas del PSVA-TSA-RENIEC.
h) Las vulnerabilidades críticas se resuelven dentro de las 48 horas de su hallazgo.
i) Para las vulnerabilidades encontradas se realiza una de las siguientes acciones, según su impacto potencial:
   - Crear e implementar un plan para mitigar la vulnerabilidad;
   - Documentar los hechos que determinan que la vulnerabilidad no requiere solución.
j) Las soluciones y reportes de incidentes se realizan de tal manera que se minimizan los daños de seguridad de información y el mal funcionamiento del servicio.

7.12. Registro de evidencia

a) Se guardan los archivos log de los eventos de las operaciones del PSVA-TSA-RENIEC, incluyendo los relacionados al ciclo de vida de las llaves y certificados TSU.
b) Se almacenan los registros relacionados a la sincronización de los relojes, incluyendo información de recalibración.
c) Se almacenan registros relacionados a la detección de pérdidas de sincronización.
d) Toda los datos y registros concernientes al PSVA-TSA-RENIEC, se almacena por un periodo de 10 años, de tal forma que no son fácilmente borrados o destruidos.
e) Se mantienen la información archivada asegurando confidencialidad e integridad.
f) Los archivos logs de los servidores del PSVA-TSA-RENIEC se encuentran disponibles para el personal de confianza autorizado.
g) Se realiza registro del tiempo preciso de los eventos significativos de gestión de llaves TSU y sincronización del reloj.
h) La hora y fecha utilizadas en los registros se sincronizan con el UTC al menos una vez al día.

7.13. Gestión de continuidad del negocio

En caso de compromiso de las llaves privadas de TSU y perdida de calibración del reloj:

a) Se cuenta con un plan de recuperación de desastres que incluye el compromiso real y potencial de las llaves privadas de TSU y pérdida de calibración del reloj de TSU.
b) Se procederá según el literal f) del numeral 7.11
c) No se emitirán nuevos sellos de tiempo hasta que se tome las acciones correctivas.

d) Se brindará información no confidencial, a los suscriptores y terceros, que les permite identificar los sellos que fueron afectados.

7.14. Terminación de la TSA y sus planes

a) Al término del servicio PSVA-TSA-RENIEC, se cancelan todos los certificados vigentes.
b) El plan de terminación o cese de operaciones se realizará conforme al Artículo 39° del Reglamento de la Ley de Firmas y Certificados Digitales (N° 27269).
c) Se publicará la terminación del servicio mediante el portal PKI.
d) Antes de la terminación del servicio se transferirán las obligaciones, los logs y registros a una autoridad confiable.
e) Antes de la terminación del servicio las llaves privadas de la TSU y sus copias de respaldo serán destruidas de manera que no se puedan recuperar.

7.15. Cumplimiento

a) El PSVA-TSA-RENIEC opera en cumplimiento de las normas europeas ETSI EN 319 421 y 319 401.
b) Se brinda el servicio a todas las entidades que cumplan con lo indicado en el numeral 4.4 Suscriptor del servicio, de manera no discriminatoria.

8. Requerimientos adicionales para sellos cualificados

No aplica para el PSVA-TSA-RENIEC.

9. Auditoría

Las auditorías o evaluaciones anuales de conformidad verifican, como mínimo, los registros, archivos, procedimientos y controles implementados por el PSVA-TSA-RENIEC.
El auditor debe ser autorizado por la AAC, ser independiente y no haber realizado trabajos para PSVA-TSA-RENIEC dentro del periodo de dos años anteriores a la auditoría.

10. Aspectos legales de la operación del PSVA-TSA-RENIEC

10.1. Políticas de reembolso

No aplica

10.2. Cobertura de seguros de responsabilidad civil

El PSVA-TSA-RENIEC cuenta con una Póliza de Seguros de Responsabilidad Civil contra terceros, la que es de aplicación bajo todos los ámbitos de las operaciones que desarrolla la entidad en conformidad con los roles y funciones que le han sido atribuidos bajo el marco legal regulatorio vigente, cumpliéndose de este modo con la obligación señalada en el artículo 38° del Reglamento de la Ley de Firmas y Certificados Digitales.

10.3. Información confidencial y/o privada

El PSVA-TSA no almacena, registra o divulga información confidencial y/o privada de los suscriptores del servicio ni de los terceros que confían.

10.4. Notificaciones y comunicaciones entre participantes

Toda notificación o comunicación con el PSVA-TSA-RENIEC se hará mediante correo electrónico o por escrito dirigido a la dirección.

- Contacto: Sub Gerente de Certificación e Identidad Digital.
- Dirección de correo electrónico: identidaddigital@reniec.gob.pe
- Dirección: Jr. Bolivia 109, Centro Cívico, Cercado de Lima
- Número de teléfono: 3152700

Las comunicaciones producirán sus efectos cuando se envíe el acuse de recibo o el escrito se presente a mesa de partes del RENIEC, en la dirección a la que se refiere el párrafo precedente.

10.5. Conformidad de la Ley aplicable

- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones.
- Guía de Acreditación de Prestadores de Servicio de Valor Añadido.
- Ley N° 29733, Ley de Protección de Datos Personales.

10.6. Exención de garantía

El PSVA-TSA-RENIEC está exento del pago de indemnización alguna, en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en el numeral 10.7.

10.7. Indemnizaciones

El PSVA-TSA-RENIEC dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo del PSVA-TSA-RENIEC, cumpliendo así con lo dispuesto en el artículo 38º del Reglamento de la Ley de Firmas y Certificados Digitales.

10.8. Fuerza mayor

El PSVA-TSA-RENIEC en ningún caso será responsable por daños o perjuicios causados por catástrofes naturales, casos de guerra, actos de terrorismo y/o sabotaje u otros actos de fuerza mayor. Sin perjuicio de lo expuesto, el PSVA-TSA-RENIEC dentro de lo posible, asegurará la continuidad del negocio y recuperación ante desastres.

11. CONSIDERACIONES DE SEGURIDAD

Durante la verificación de los sellos de tiempo es necesario que el certificado de la TSU haya sido emitido por una entidad confiable y acreditada dentro del marco de la IOFE bajo la Jerarquía ECERNEP PERÚ CA Root 3. Además, es necesario verificar que no se encuentra revocado. Esto quiere decir que su seguridad recae sobre la entidad que administra este certificado digital y la entidad emisora, tanto en la emisión del certificado como en la información de estado de revocación.

Cuando un sello de tiempo es verificado como válido en un instante de tiempo en particular, esto no quiere decir que permanecerá válido en el futuro. Cada vez que se verifica un sello de tiempo emitido dentro del periodo de validez del certificado de la TSU, es necesario verificar también el estado de revocación del certificado, provisto por la CRL de la EC-PSVA, administrada y publicada por la ECERNEP. En Anexo D de la norma ETSI EN 319 421 brinda información sobre verificación de sellos de tiempo a largo plazo.

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.

12. BIBLIOGRAFÍA

- Ley N°27269 Ley de Firmas y Certificados Digitales
- Reglamento de la Ley de Firmas y Certificados Digitales
- RFC 3161
- ETSI EN 319 421
- Guía de Acreditación de Prestador de Servicios de Valor Añadido

Anexo 01

A. Acrónimos

- AAC: Autoridad Administrativa Competente
- ETSI European Telecommunications Standards Institute
- ISO *International Organization for Standardization*
- NTP Norma Técnica Peruana
- OCSP *Online Certificate Status Protocol*
- (Protocolo del estado en línea del certificado)
- OID: Identificador de Objeto
- PKI *Public Key Infrastructure* (Infraestructura de Clave Pública)
- PSVA Prestador Servicios de Valor Añadido
- RFC *Request for Comment*
- SHA *Secure Hash Algorithm*
- TSA: Autoridad de Sellado de Tiempo
- TSA-RENIEC: Autoridad de Sellado de tiempo del Registro Nacional de Identificación y Estado Civil
- TSS: Servicio de Sellado de tiempo
- TSU: Unidad de Sellado de tiempo
- UTC: Tiempo Universal Coordinado

B. Definiciones

Se ha tomado como referencia las definiciones establecidas en el D.S. N° 052-2008-PCM "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 a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.
- Acuse de Recibo.- Son los procedimientos que registran la recepción y validación de la Notificación Electrónica Personal recibida en el domicilio electrónico, de modo tal que impide rechazar el envío y da certeza al remitente de que el envío y la recepción han tenido lugar en una fecha y hora determinada a través del sello de tiempo electrónico.
- Agente Automatizado.- Son los procesos y equipos programados para atender requisitos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
- Autenticación.- Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.
- Autoridad Administrativa Competente (AAC).- 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 presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI. Certificado Digital.- Es el documento

credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:

- La suspensión consiste en inhabilitar la validez de un certificado digital por un periodo de tiempo establecido en el momento de la solicitud de suspensión, dicho periodo no puede superar la fecha de expiración del certificado digital.
- La modificación de la información contenida en un certificado sin la re-emisión de sus claves.
- La re-emisión consiste en generar un nuevo par de claves y un nuevo certificado, correspondiente a una nueva clave pública pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.

- Código de verificación o resumen criptográfico (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:
  - El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.
  - Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.
  - Sea improbable por medios técnicos, que se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.
- Declaración de Prácticas de Certificación (CPS).- Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.
- Declaración de Prácticas de Registro o Verificación (RPS).- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación**.**
- Declaración de Prácticas de Valor Añadido.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define las prácticas y procedimientos que emplea en la prestación de sus servicios.
- Dirección de correo electrónico.- Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.
- Documento: Es cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

  Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.
- Documento oficial de identidad.- Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:
  - Documento Nacional de Identidad (DNI);

  - Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,
  - Pasaporte, si se trata de personas naturales extranjeras no residentes.

- Domicilio electrónico.- Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes. Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas. En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación Digital. El acceso a este domicilio se realiza empleando un certificado digital de autenticación.
- Entidad de Certificación.- Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
- Entidad de Certificación Extranjera.- Es la Entidad de Certificación que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.
- Entidades de la Administración Pública.- Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.
- Entidad de Registro o Verificación.- Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
- Entidad final.- Es el suscriptor o propietario de un certificado digital.
- Estándares Técnicos Internacionales**.-** Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.
- Estándares Técnicos Nacionales.- Son los estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.
- Equivalencia funcional.- Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

- Expediente electrónico.- El expediente electrónico se constituye en los trámites o procedimientos administrativos en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.
- Gobierno Electrónico.- Es el uso de las Tecnologías de Información y Comunicación para redefinir la relación del gobierno con los ciudadanos y la industria, mejorar la gestión y los servicios, garantizar la transparencia y la participación, y facilitar el acceso seguro a la información pública, apoyando la integración y el desarrollo de los distintos sectores.
- Hardware Security Module (HSM).- Traducido al español significa módulo de seguridad de hardware. Es un módulo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. Aporta aceleración en las operaciones criptográficas.
- Identificador de objeto (OID).- Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).
- Infraestructura Oficial de Firma Electrónica (IOFE).- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, 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;
    - La identidad de su autor, lo que es regulado conforme a Ley.

  El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.
- Integridad.- Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
- Interoperabilidad.- Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas:
    - Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.
    - Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.
    - Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.
- Ley.- Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

- Lista de Certificados Digitales Cancelados (CRL).- Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.
- Mecanismos de firma digital.- Es un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma digital. Dichos mecanismos varían según el nivel de seguridad que se les aplique.
- Medios electrónicos.- Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar documentos electrónicos.
- Medios electrónicos seguros.- Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.
- Medios telemáticos.- Es el conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.
- Neutralidad tecnológica.- Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.
- Niveles de seguridad.- Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.
- No repudio.- Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.
- En el ámbito del artículo 2º de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).
- Nombre Común - Common Name (CN).- Es un atributo que forma parte del Nombre Distinguido (Distinguished Name - DN).
- Nombre de Dominio totalmente calificado - Fully Qualified Domain Name (FQDN).- Es el identificador que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo que puede identificar de forma única a un equipo servidor (o arreglo de estos) en el internet.
- Nombre Diferenciado (X.501) - Distinguished Name (DN).- Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la Entidad de Certificación. En inglés se denomina “Distinguished Name”.

- Nombre distinguido.- Es equivalente a Nombre diferenciado.
- Norma Marco sobre Privacidad.- Es la norma basada en la normativa aprobada en la 16º Reunión Ministerial del APEC, que fuera llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004, la cual forma parte integrante de las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.
- Par de claves.- En un sistema de criptografía asimétrica comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
- Políticas de Certificación.- Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual se establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.
- Prácticas de Certificación.- Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva.
- Prácticas de Registro o Verificación.- Son las prácticas que establecen las actividades y requisitos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
- Prestador de Servicios de Certificación.- Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.
- Prestador de Servicios de Valor Añadido.- Es la entidad pública o privada que brinda servicios que incluyen la firma digital y el uso de los certificados digitales. El presente Reglamento presenta dos modalidades:
    - Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.
    - Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación electrónico, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.
- Prestador de Servicios de Valor Añadido para el Estado Peruano.- Es la Entidad pública que brinda servicios de valor añadido, con el fin de permitir la realización de las transacciones públicas de los ciudadanos a través de medios electrónicos que garantizan la integridad y el no repudio de la información (Sistema de Intermediación Digital) y/o registran la fecha y hora cierta (Sello de Tiempo).
- Reconocimiento de Servicios de Certificación Prestados en el Extranjero.- Es el proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.
- Reglamento.- Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

- Servicio de Valor Añadido.- Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, y conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónico dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.
- Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés).- Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la Autoridad de Certificación sobre el estado de un certificado.
- Sistema de Intermediación Digital.- Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

  • Sistema Web ("World Wide Web"): Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.
- Suscriptor.- Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
- Tercero que confía o tercer usuario.- Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.
- Titular.- Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
- Usuario final.- En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.

Anexo 02 - Declaración de Libre Divulgación

Tipo	Descripción	Requerimientos específicos
Declaración de Libre Divulgación	La Declaración de Libre Divulgación constituye un resumen de la Declaración de Prácticas de Valor Añadido del PSVA-TSA-RENIEC orientada a los suscriptores del servicio. Para una descripción completa, revisar la Declaración de Prácticas de Valor Añadido.	La Declaración de Prácticas de Servicios de Valor Añadido ha sido desarrollada conforme a la Política del Servicios de Valor Añadido de la ECERNEP, lo especificado en el RFC3628 y la norma ETSI EN 319 421.
Información de contacto del PSVA-TSA-RENIEC	Toda notificación o comunicación con el PSVA-TSA-RENIEC se hará mediante correo electrónico o por escrito dirigido a la dirección. • Contacto: Sub Gerente de Certificación e Identidad Digital. • Dirección de correo electrónico: identidaddigital@reniec.gob.pe • Dirección: Jr. Bolivia 109, Centro Cívico, Cercado de Lima • Número de teléfono: 3152700 Las comunicaciones producirán sus efectos cuando se envíe el acuse de recibo o el escrito se presente a mesa de partes del RENIEC, en la dirección a la que se refiere el párrafo precedente.	10.3 Información confidencial y/o privada El PSVA-TSA no almacena, registra o divulga información confidencial y/o privada de los suscriptores del servicio ni de los terceros que confían. Notificaciones y comunicaciones entre participantes
Tipos de sellos de tiempo y uso	El PSVA-TSA-RENIEC emite sellos de tiempo no cualificados, para ser usados con o sin firma digital	Se utiliza algoritmo de hashing SHA256 y el algoritmo de firma RSAWithSHA256 para la emisión del sello con los certificados que tienen un tiempo de validez de 12 años (ver numeral 7.6.5)
Limitación de confianza	Tal como se indica en el numeral 7.3, entre otras cosas: • El PSVA-TSA-RENIEC asegura la confianza en la provisión del servicio mediante la gestión apropiada de sus activos y sensibilizaciones o capacitaciones a su personal sobre Seguridad de la información, al menos una vez al año.	Los sellos de tiempo emitidos por el PSVA-TSA-RENIEC, que operan bajo la jerarquía ECERNEP PERU CA ROOT 3, se encuentra en

		conformidad con el estándar NTP que establece la precisión mínima respecto al UTC de ± 1 segundo. Además, se almacenan los logs por un periodo de al menos 10 años.
Obligaciones de los suscriptores del servicio	Según el numeral 6.5.2, las obligaciones de la TSA con los suscriptores son: • Cumplir los términos y condiciones descritos en el contrato o convenio celebrado con la PSVA-TSA-RENIEC. • Utilizar un software de firma confiable y acreditado dentro de la IOFE que realice la verificación del certificado que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL provista por el PSVA-TSA-RENIEC.	
Obligación de verificar el estado del certificado del TSU	Según se indica en el numeral 6.6, los terceros que confían están obligados, entre otras cosas, a: • Utilizar un software de firma confiable y acreditado dentro de la IOFE que realice la verificación del certificado que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL provista por el PSVA-TSA-RENIEC.	La URL para consulta la CRL que emite el EC-PSVA, se indican en la extensión *CRLDistributionPoints* del certificado del TSU (ver numeral 1)
Limitación de responsabilidad	El PSVA-TSA-RENIEC no será en ningún caso responsable cuando se encuentra en alguna de las siguientes circunstancias: • Estado de guerra, desastre natural o cualquier otra causa de fuerza mayor, incluida el funcionamiento defectuoso de los servicios de las redes telemáticas de los ISP (Proveedores de Internet), fluido eléctrico o equipos informáticos de terceros. • Por el uso que se pueda realizar de los certificados digitales, en especial por el contenido de los mensajes o documentos firmados o cifrados	
Acuerdos aplicables y declaración de prácticas	Los documentos tales como la Política de Valor Añadido y su Declaración de Prácticas se encuentran disponibles en la URL: **http://www.reniec.gob.pe/repository/** **https://pki.reniec.gob.pe/repositorio/**	El OID de la Declaración de Prácticas de Valor Añadido es 1.3.6.1.4.1.35300.2.1.3.2.0.105.1000.0, tal como se indica en el numeral 5.2.

Política de Privacidad	No aplica	
Política de reembolso	No aplica	
Ley Aplicable, quejas y resolución de disputas	Tal como se indica en el numeral 10.5, las leyes y normas aplicables son: • Ley N° 27444, Ley del Procedimiento Administrativo General. • Ley N° 27269, Ley de Firmas y Certificados Digitales, su reglamento, normas complementarias y sustitutorias. • Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones. • Guía de Acreditación de Prestadores de Servicio de Valor Añadido. • Ley N° 29733, Ley de Protección de Datos Personales. Además, como se indica en el numeral 6.2, literal g, en caso de consultas, reclamos o disputas relacionados con el Servicio de Valor Añadido-Sellado de Tiempo brindado por la TSA-RENIEC, remitirlo al correo identidaddigital@reniec.gob.pe	
TSA y repositorio de acreditaciones	El PSVA-TSA-RENIEC se encuentra acreditado en el marco de la IOFE como Prestador de Servicios de Valor Añadido. Se publican las resoluciones de acreditación y evaluaciones de seguimiento en https://pki.reniec.gob.pe/acreditaciones/	La Autoridad Administrativa Competente se encarga de acreditar y evaluar al PSVA-TSA-RENIEC anualmente, de acuerdo a la Guía de Acreditación para Prestadores de Servicio de Valor Añadido.