DECLARACIÓN DE PRÁCTICAS DE VALOR AÑADIDO

PRESTADORES DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

Servicio de Sellado de Tiempo

TSA-RENIEC

Versión: 1.0	**Año: 2017**

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

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	15/12/2017	Elaboración y Aprobación	GRCD/SGCID	Aprobado

1. 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 en el RFC3628 se definen los lineamientos para elaborar la Política y Declaración de Prácticas de una 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 PERÚ CA ROOT 3.

2. VISIÓN GENERAL

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

3. DEFINICIONES Y ABREVIATURAS

Ver Anexo 1

4. CONCEPTOS GENERALES

4.1. 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: controla y monitorea la operación de los servicios para asegurar que sean provistos de acuerdo a lo especificado por el Prestador de Servicios de Valor Añadido de sellado de tiempo (PSVA-TSA). Este componente es responsable de la activación o desactivación de la provisión del servicio. Por ejemplo, la administración se asegura de que el reloj usado para el sellado de tiempo esté correctamente sincronizado con el UTC.

4.2. Autoridad de Sellado de Tiempo (TSA)

Es la autoridad que emite sellos de tiempo en los que confía. Tal como se indica en la Política de Servicios de Valor Añadido – Servicio de Sellado de tiempo, en la hoy derogada directiva de firmas electrónicas de la Unión Europea, a las TSA se les considera proveedores de servicios de certificación, mientras que en el nuevo Reglamento que la sustituye, se les considera prestadores de servicios de confianza, pudiendo cualificar su servicio, inclusive de forma completamente independiente a la emisión de certificados.

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 PERÚ CA Root 3 y es responsable de brindar los servicios identificados en el numeral

4.2.1. Servicio de Sellado de Tiempo (TSS).

La PSVA-TSA-RENIEC realiza 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.

La PSVA-TSA-RENIEC publica los certificados digitales de sus TSU en la URL: https://www.reniec.gob.pe/repository/

4.3. Suscriptor del servicio

El suscriptor del servicio puede ser una organización compuesta por varios usuarios finales o un usuario final individual.

Cuando el suscriptor del servicio es una organización, algunas de las obligaciones que corresponden a dicha organización tendrán que aplicarse también a los usuarios finales que la conforman. En cualquier caso, la organización será responsable de aquellas obligaciones que los usuarios finales que la conforman no cumplan correctamente y en consecuencia se espera que la misma les informe adecuadamente.

4.4. 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.

4.4.1.Propósito

El presente documento es una declaración de “CÓMO uno se adhiere” a los requisitos establecidos en la Política Declaración de Prácticas de Valor añadido y de CÓMO se implementa el servicio de sellado de tiempo.

Además, el presente documento también incluye la Declaración de Libre Divulgación del PSVA-TSA-RENIEC.

4.4.2.Nivel de especificidad

El presente documento define cómo la PSVA-TSA-RENIEC, en particular, cumple con los requisitos técnicos, organizacionales y procedimentales identificados en la Política de Servicios de Valor Añadido - Servicio de Sellado de Tiempo.

4.4.3.Enfoque

El presente documento responde a las operaciones, instalaciones y entorno informático del PSVA-TSA-RENIEC.

5. POLÍTICAS DE SELLADO DE TIEMPO

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, concordando con lo señalado en el numeral 4.4 Políticas de Sellado de Tiempo y Declaración de Prácticas de la TSA.

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.

5.2. Identificación

El identificador de objetos (OID, según la ITU-T Recommendation X.208) de la política de sellado de tiempo básica definida en la norma ETSI EN 319 421 es: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

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 que cuentan con la autorización respectiva de la TSA para hacer uso del servicio y por los terceros que confían, pudiendo tratarse tanto de personas naturales como jurídicas de la administración pública; las que podrán actuar por medios individuales o valiéndose de medios automatizados, equipos o servicios TI.

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 el numeral 1.3.6 de la Política General de Certificación de la ECERNEP.

5.4. Conformidad

El PSVA-TSA-RENIEC, que opera bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3 que gestiona el RENIEC utiliza el identificador para la política de sellado de tiempo conforme se determina en el numeral 5.2 Identificación.

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 requerimientos 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 la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo. El RENIEC gestiona el servicio Sellado de Tiempo por sí mismo. Si se realizara la contratación de terceros para algún servicio relacionado con el PSVA-TSA-RENIEC mediante un documento contractual y se realizaría bajo los requerimientos detallados en el numeral 7.

Se provee la presente Declaración de Prácticas para evidenciar el cumplimiento de todos los servicios en completa conformidad con la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo.

6.1.2. Obligaciones de la TSA con los suscriptores

El PSVA-TSA-RENIEC está obligado a:

- Emitir sellos de tiempo en concordancia con la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo, la Ley de Firmas y Certificados Digitales y su reglamento, las Guías de Acreditación del Prestador de Servicios de Valor Añadido (modalidad TSA).
- 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 operacionales y técnicos del PSVA-TSA-RENIEC

6.1.3. Obligación de la TSA-RENIEC con los terceros que confían

- Informar terceros que confían del cese de actividades y mecanismos habilitados para la validación de sus sellos de tiempo existentes.
- Publicar este documento y los relacionados al servicio, garantizando el acceso a la versión actual y las anteriores.

- Divulgar las condiciones del servicio como se indica en el numeral 7.1.2
- Informar sobre el cese de sus actividades y los mecanismos habilitados para la validación de sellos existentes

6.2. Obligaciones de los suscriptores

El suscriptor está obligado a utilizar un software de firma confiable y acreditado dentro de la IOFE. El software debe realizar la verificación del certificado que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL o el sistema OCSP provistos por el PSVA-TSA-RENIEC.

6.3. Obligaciones de los terceros que confían

Los terceros que confían están obligados a:

a) Verificar que el sello de tiempo haya sido creado correctamente y que la llave privada utilizada no se encontraba comprometida en el momento de la verificación, debiendo para esto contar con un software de verificación confiable acreditado por la AAC dentro del marco de la IOFE.
b) Tener en cuenta cualquier limitación en el uso del sello de tiempo, conforme a lo indicado en este documento
c) Tener en cuenta cualquier otro lineamiento indicado o publicado por el PSVA-TSA-RENIEC en su sitio web https://pki.reniec.gob.pe//generacion-de-sellos-de-tiempo/

6.4. Responsabilidades

El RENIEC opera su TSA en concordancia con la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo, la Política General de Certificación de la ECERNEP y todos los documentos normativos correspondientes.

El RENIEC no se hace responsable por la veracidad o contenido de los datos sellados por el PSVA-TSA-RENIEC.

Bajo ninguna circunstancia, el RENIEC será responsable 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 o tercero que confía respecto a los términos y condiciones de uso aplicables, incluyendo el exceso en el límite establecido para las transacciones.

El RENIEC, bajo ninguna circunstancia, será responsable por los daños que resulten de eventos de fuerza mayor o desastres naturales, conforme se detalla en el numeral 7.1.2 del presente documento. El RENIEC tomará las medidas razonables para mitigar los efectos o daños en un periodo de tiempo razonable, según sea el daño.

7. REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA

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

7.1.1. Declaración de Prácticas de la TSA

El PSVA-TSA-RENIEC se encuentra acreditado por la AAC, dentro del marco de la IOFE.

El PSVA-TSA-RENIEC brinda el servicio de sellado de tiempo conforme a lo siguiente:

a) Se desarrollan análisis de riesgos periódicamente, identificando los activos y las amenazas a dichos activos, determinando los controles de seguridad necesarios para mitigar los riesgos identificados
b) El PSVA-TSA-RENIEC realiza el presente documento para cumplir con todos los requisitos identificados en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo de la ECERNEP.
c) El servicio de sellado de tiempo del PSVA-TSA-RENIEC opera bajo los lineamientos dados por el RFC 3161 *Time Stamp Protocol.*
d) Los servicios son realizados dentro de las instalaciones del RENIEC, por personal de la institución. En caso de que se requiera servicios de terceros, se divulgará a los usuarios y terceros que confían.
e) La PSVA-TSA-RENIEC divulga a todos los usuarios y terceros que confían, los términos y condiciones de uso respecto a su servicio de sellado de tiempo, según lo que se indica en el numeral 7.1.2
f) El PSVA-TSA-RENIEC publica únicamente la versión de Declaración de Prácticas aprobada por la AAC
g) El RENIEC es la Entidad Pública a cargo del PSA-TSA-RENIEC y quien vela por que las prácticas sean implementadas conforme a los lineamientos de la ECERNEP. Además, el PSVA-TSA-RENIEC se encuentra acreditado por la AAC, dentro del marco de la IOFE.
h) Los documentos relacionados a la TSA-RENIEC son administrados, revisados y corregidos por la Sub Gerencia de Certificación Digital de la Gerencia de Certificación y Registro Digital del RENIEC. Posteriormente, son aprobados en la acreditación por personal designado de la AAC

7.1.2. Declaración de Libre Divulgación de la TSA

a) Las consultas relacionas al servicio de sellado de tiempo y al presente documento pueden ser dirigidas a la cuenta de correo electrónico identidadigital@reniec.gob.pe
b) El PSVA-TSA-RENIEC, como parte de la jerarquía ECERNEP PERÚ CA ROOT 3, se adhiere e implementa lo indicado en la Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo.
c) 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.
d) El tiempo de vida del sello de tiempo es de al menos doce (12) años.

e) 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.
f) El PSVA-TSA-RENIEC no se hace responsable por la veracidad o contenido de los datos sellados utilizando los certificados de sus TSU.
g) Las obligaciones de los suscriptores se detallan en el numeral 6.2 del presente documento
h) Las obligaciones de los terceros que confían se detallan en el numeral 6.3
i) El tercero que confía puede verificar el sello de tiempo utilizando la TSL emitida por Indecopi (en la que se encuentra el certificado raíz de la jerarquía ECERNEP PERÚ CA ROOT 3) y la CRL emitida por el PSVA-TSA-RENIEC. Sin embargo, el PSVA-TSA-RENIEC solamente garantiza la integridad y confianza del sello de tiempo dentro del periodo de validez del certificado del TSU que estampó dicho sello.
j) La TSA-RENIEC almacena los registros durante un periodo mínimo de diez (10) años, en conformidad con la legislación peruana.
k) La prestación del servicio de sellado de tiempo se encuentra sujeta a lo establecido por la legislación peruana, en particular, a la Ley 27269, Ley de Firmas y Certificados Digitales, su reglamento, normas complementarias y sustitutorias; de igual manera, a la Guía de Acreditación de Prestadores de Servicios de Valor Añadido, Versión 3.3 y a lo que disponga de acuerdo a sus atribuciones la AAC de la IOFE.
l) El PSVA-TSA-RENIEC no se hace responsable por la veracidad o contenido de los datos sellados utilizando los certificados de sus TSU.
m) Las quejas o disputas pueden ser dirigidas a la cuenta de correo identidaddigital@reniec.gob.pe indicando el nombre completo del usuario del servicio, su número de DNI, la entidad a la que pertenece y un resumen de su queja.
n) El PSVA-TSA-RENIEC declara que el servicio de sellado de tiempo se realiza conforme a lo establecido en esta Declaración de Prácticas, lo especificado en el RFC 3628 y el RFC 3161.

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.

7.2. Ciclo de vida de la gestión de llaves

7.2.1. Generación de las llaves de la TSA

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

a) En un entorno que cuenta con seguridad de acceso físico mediante control biométrico dual (dos personas), en presencia del Oficial de Seguridad de la Información y registrando en acta y logs el procedimiento realizado. Este procedimiento es realizado por personal especializado y de confianza.

b) En un módulo criptográfico HSM certificado y operando bajo los estándares FIPS 140-2 nivel 3. El algoritmo y tamaño de llaves se describen en el numeral 5.2.1 Perfil del certificado TSA-RENIEC.
c) El algoritmo de generación de llaves es RSA con un tamaño de 2048 bits

7.2.2. Protección de las llaves privadas de la TSU

La TSA-RENIEC almacena sus llaves privadas en los 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. Las llaves privadas se encuentran protegidas mediante control multipersonal.

En caso se requiera contar con las llaves firmadoras en otro módulo criptográfico, se generan nuevas llaves en el nuevo módulo criptográfico.

7.2.3. Distribución de las llaves públicas de la TSU

Los certificados digitales de los TSU del PSVA-TSA-RENIEC, que incluyen la llave pública, son distribuidos en el repositorio correspondiente https://www.reniec.gob.pe/repository/

Los certificados del PTSVA-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.

7.2.4. Regeneración de las llaves de la TSU

La llave privada de las TSU serán emitidas nuevamente 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 el PSVA-TSA-RENIEC lo requiera para poder seguir brindando un servicio de sellado de tiempo con un periodo de validez razonable.

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, se generan nuevos certificados cada año, permitiendo que lo anteriores sigan disponibles solamente para verificación, pero no para generar nuevos sellos de tiempo.

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 la TSU

El PSVA-TSA-RENIEC garantiza que la llave privada asociada a una TSU no puede ser utilizada en un tiempo posterior al fin de la validez del certificado digital asociado, o cuando se encuentra en la lista CRL o en el sistema OCSP.

Específicamente, no podrá ser usada después de dos (02) años después de su generación para emitir nuevos sellos de tiempo.

El ciclo de vida de una TSU está asociado al ciclo de vida del certificado digital que le corresponde.

El PSVA-TSA-RENIEC garantiza que sus sistemas de emisión y gestión de sellos de tiempo no aceptan peticiones que involucren a llaves privadas de TSU caducas o canceladas.

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

Los módulos criptográficos HSM son trasladados, si se requiere, por personal del PSVA-TSA-RENIEC con roles autorizados para la inicialización y puesta en marcha, con los controles de seguridad física y lógica adecuados. Toda manipulación, traslado o configuración es registrada y archivada como registro de auditoría.

En caso, se requiera el reemplazo de un módulo criptográfico HSM, por cualquier motivo, 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 el formato establecido por la recomendación RFC 3161 y que cuentan con fecha y hora correcta. En particular, cada sello de tiempo contiene:

a) El OID de la Política de Servicios de Valor Añadido –Servicio de Sellado de Tiempo y de la presente Declaración de Prácticas.
b) Un número de serie único
c) La fecha y hora en la que fue generado el sello de tiempo proveniente de un laboratorio UTC (k)

NOTA 1: El *Bureau International des Poids et Mesures* (BIPM) estima el UTC sobre la base de sus representantes locales UTC (k) que forman parte de un conjunto de relojes atómicos en institutos nacionales de meteorología y observatorios nacionales astronómicos alrededor del mundo. El BIPM disemina el UTC a través de su Circular T mensual (lista 1). La misma se encuentra disponible en el sitio web de BIPM (www.bipm.org) y permite identificar a todos aquellos institutos con escalas de tiempo UTC (k) reconocidas.

d) La fecha y hora incluidas en el sello de tiempo se sincroniza con el UTC con una desviación no mayor a ± 1 segundos.

e) Si el reloj del PSVA-TSA-RENIEC se detecta como fuera de tiempo por una desviación de 0.5 segundos, inmediatamente se lanza una alerta a la lista ntp@pkiep.reniec.gob.pe para que los especialistas del PSVA-TSA-RENIEC procedan con las acciones correctivas.
f) Un resumen del dato (hash) a ser sellado, tal cual fue provisto por el solicitante y un identificador (OID) del algoritmo de hashing utilizado.
g) El sello de tiempo es emitido utilizando la llave privada de uno de los TSU del PSVA-TSA-RENIEC.
h) El sello de tiempo incluye los identificadores siguientes:
   - Identificador del país: El valor "PE" en el atributo C (country) del SubjectDN del TSU firmante
   - Identificador para la TSA: OID de Política de Servicios de Valor Añadido, OID de Declaración de Prácticas, OID de perfil de certificado correspondiente al TSA-RENIEC.
   - Identificador para la TSU que emite los sellos de tiempo: Número de serie y Fingerprint del certificado que emite el sello.

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 la 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.

En particular:

a) La calibración de los relojes de las TSUs 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 (además de cuatro (04) servidores alternativos del proyecto pool.ntp.org, todos se encuentran en el servicio de alerta CHRONY.
b) Los relojes de las TSU deben protegerse contra amenazas que pudiesen resultar en cambios no detectados que puedan afectar su calibración.
c) Al detectar una desviación de ± 0.5 segundos inmediatamente se lanza una alerta a la lista ntp@pkiep.reniec.gob.pe para que los especialistas del PSVA-TSA-RENIEC procedan con las acciones correctivas.

d) Cuando se produce *leap second,* notificado por el organismo correspondiente, se retira el servidor horario que se encuentra con desviación del balanceo de servidores horarios del PSVA-TSA-RENIEC.

7.4. Gestión y operación de la TSA

7.4.1. Gestión de la seguridad

a) El PSVA-TSA-RENIEC es responsable por todos los aspectos de la provisión del servicio de sellado de tiempo. No terceriza servicios.
b) Los gestores de la TSA brindan dirección sobre la seguridad de la información a través del comité de seguridad que es responsable de determinar la política de seguridad de la información de la TSA. La TSA debe garantizar la publicación y comunicación de esta política a todo el personal al que impacta.
c) La infraestructura de seguridad de la información de la PSVA-TSA-RENIEC se encuentra alineada las normas siguientes:
    - NTP-ISO/IEC 27001, EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, o el estándar internacional ISO/IEC 27001
    - NTP-ISO/IEC 17799, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, o el estándar internacional ISO/IEC 27002.
    - ISO/IEC 15408 “Information technology - Security techniques - Evaluation criteria for IT security”.

d) Los controles de seguridad se cumplen según las normas mencionadas en el literal c.
e) El PSVA-TSA-RENIEC no terceriza ninguna función del servicio de sellado de tiempo. En caso se realizará la tercerización de alguna función, el PSVA-TSA-RENIEC garantiza que dicho tercero cumpla con las certificaciones de calidad y seguridad de la información correspondiente.

La implementación de la seguridad se realiza conforme a lo indicado en las siguientes normas técnicas:

7.4.2.Gestión y clasificación de activos

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

7.4.3.Seguridad del personal

a) El PSVA-TSA-RENIEC selecciona a sus trabajadores según su formación académica, experiencia laboral y conocimiento especializado en servicios PKI, en especial en TSA.
b) Se asignan, de manera oficial, los roles de confianza, incluyendo sus funciones, riesgos y responsabilidades y se documentan en los contratos de trabajo u otro documento pertinente.
c) El personal del PSVA-TSA-RENIEC cuenta con la descripción de su puesto de trabajo en su contrato, orden de servicio u otro documento pertinente.
d) Todos los procedimientos administrativos o técnicos se realizan bajo el lineamiento de del ISO/IEC 27001 de Seguridad de la Información.

e) El personal del PSVA-TSA-RENIEC cuenta con las siguientes características
f) Conocimientos de la tecnología de sellado de tiempo.
   - Conocimientos de tecnología de sellado de tiempo.
   - Conocimientos de mecanismos para la calibración o sincronización de los relojes de las TSU con el UTC.
   - Familiaridad con procedimientos de seguridad para el personal con responsabilidades de seguridad.
   - Experiencia con seguridad de la información y evaluación de riesgos.
g) Los roles de confianza incluyen las siguientes responsabilidades
   - Oficiales de seguridad: responsables de manera general por gestionar la implementación de las prácticas de seguridad.
   - Administradores de sistemas: autorizados a instalar, configurar y dar mantenimiento a los sistemas confiables para el sellado de tiempo.
   - Operadores de sistemas: responsables de operar los sistemas confiables de la TSA sobre una base día a día. Autorizados a llevar a cabo el respaldo de datos y su restauración.
   - Auditores de sistemas: Autorizados a visualizar los archivos y los registros de auditoría *(logs)* de los sistemas confiables de la TSA.
h) 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
e) 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.

7.4.4.Seguridad física y del entorno

a) La TSA-RENIEC mantiene controles de seguridad físicos para impedir y prevenir el acceso a personas no autorizadas
b) Se cuenta con control de acceso multipersonal para acceder a la llave privada.
c) Controles adicionales tales como:

   - Perímetro cerrado, piso y techo de concreto, sin ventanas y con puerta sólida cortafuegos blindada.
   - Personal de seguridad que sólo permite el ingreso a personas autorizadas
   - Zonas de alta seguridad con activos críticos restringidas con acceso biométrico
   - Medidas de prevención ante desastres naturales (inundación, terremoto, entre otros) y ante desastres accidentales creados por el hombre (incendios, explosiones, disturbios civiles).

- Ambientes separados para:
  - Área Operacional: Contiene los equipos y servidores computacionales necesarios para la operación de la ECEP-RENIEC *online*, gestión de certificados de entidad final, repositorios y servicios de verificación de estado de certificado en línea. El área operacional se extiende a través de un sitio principal y otro de contingencia, disponiéndose en ambos de controles equivalentes.
  - Área Restringida: Contiene la información confidencial y crítica con acceso solamente al personal autorizado mediante verificación biométrica doble (dos personas). En esta área se resguarda el módulo criptográfico que contiene las llaves privadas de la ECEP-RENIEC *offline*.

7.4.5. Gestión de operaciones

El PSVA-TSA-RENIEC asegura:

aplica los controles necesarios para que sus componentes se encuentren seguros y sean operados con un mínimo riesgo de falla.

La TSA-RENIEC implementa controles que afectan a todas las operaciones que involucran la emisión y control de sellos de tiempo, copias de seguridad.

7.4.6. Gestión de acceso a los sistemas

Los sistemas responsables de emisión y control de los sellos de tiempo se encuentran protegidos por medidas físicas y lógicas, limitando el acceso solo al personal autorizado.

El área donde se encuentran los componentes de hardware de los sistemas se encuentra desocupada; es decir, sin personal y con control de acceso biométrico doble.

7.4.7. Mantenimiento y despliegue de sistemas confiables

Dentro de la operación del PSVA-TSA-RENIEC, se utilizan solamente productos confiables y protegidos contra modificaciones. Los HSM donde se alojan las llaves privadas de los TSU tienen certificación FIPS 140-2 Nivel 3 y están configurados de modo que se requiere control de acceso multipersonal.

7.4.8. Compromiso de los servicios de la TSA

En caso de 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 de sus operaciones. En particular, asegura que la información requerida para la validación de sus sellos de tiempo siga vigente, activa y accesible hasta la expiración del último certificado digital de TSA emitido.

En caso de terminación de la TSA-RENIEC, se realizarán las siguientes acciones:

- Informar a todos los suscriptores y terceros que confían del cese de actividades y mecanismos habilitados para la validación de sus sellos de tiempo existentes.
- Comunicar a la AAC, con no menos de treinta (30) días calendario de anticipación, el cese de actividades y los mecanismos habilitados para la validación de sus sellos de tiempo existentes.

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 indicados en el RFC 3161, la Ley de Firmas y Certificados Digitales y su reglamento, y la normativa local sobre protección de datos personales existente en Perú.

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

La TSA-RENIEC crea, archiva y controla registros de los eventos derivados de sus operaciones (logs), de acuerdo a una clasificación de dichos registros.

7.5. Aspectos organizacionales

La TSA-RENIEC se encuentra administrada por el Registro Nacional de Identificación y Estado Civil (RENIEC).

8. AUDITORÍAS DE CONFORMIDAD Y OTRAS EVALUACIONES

8.1. **Frecuencia y circunstancias de evaluación**

La TSA-RENIEC está sujeta a una auditoría o evaluación de conformidad, según lo regulado por la AAC.

El resultado de estas auditorías o evaluaciones de conformidad están publicadas por la TSA-RENIEC en la dirección https://pki.reniec.gob.pe/acreditaciones/

8.2. **Identidad/Calificaciones de auditores**

Las personas que llevan a cabo la auditoria o evaluación de conformidad son designadas por la AAC, de acuerdo a su normativa. Es potestad de la AAC evaluar y reconocer a un auditor como personal calificado.

8.3. **Relación del auditor con la entidad auditada**

La TSA-RENIEC verifica que no exista ninguna relación entre la entidad y el auditor que pueda derivar en conflicto de intereses, de acuerdo a la normativa legal vigente sobre el tema.

8.4. **Elementos cubiertos por la evaluación**

Las auditorías o evaluaciones de conformidad verifican, como mínimo, los siguientes aspectos considerados como críticos:

- Alineación de la Declaración de Practicas de Valor Añadido -TSA a las Políticas de Servicio de Valor Añadido y a las Guías de Acreditación de la IOFE.
- Revisión de la vigencia de la certificación ISO/IEC 27001:2013

8.5. **Acciones a ser tomadas frente a deficiencias**

La TSA-RENIEC toma acciones frente a los hallazgos encontrados por los auditores.

8.6. **Publicación de resultados**

La AAC publica los resultados de las auditorías o evaluaciones de conformidad realizadas dentro de la IOFE.

9. ASPECTOS LEGALES DE LA OPERACIÓN DE LA TSA-RENIEC

9.1. **Responsabilidad Financiera**

9.1.1.Cobertura de seguro

La 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 27° del Reglamento de la Ley de Firmas y Certificados Digitales.

9.1.2.Otros activos

La TSA-RENIEC, para la prestación del servicio de Valor Añadido-Sellado de Tiempo a su cargo, cuenta con el respaldo económico del RENIEC.

9.1.3.Políticas de reembolso

La política de reembolso del RENIEC, en su calidad de Prestador de Servicios de Valor Añadido-Sellado de Tiempo, se encuentra establecida en el contrato.

9.1.4.Exención de garantías

La TSA-RENIEC está exenta del pago de indemnización alguna en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en el numeral 9.1.5 Indemnizaciones del presente documento.

9.1.5.Indemnizaciones

La 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 de la TSA-RENIEC, cumpliendo así con lo dispuesto en el artículo 27 del Reglamento de la Ley de Firmas y Certificados Digitales.

9.2. **Limitaciones a la responsabilidad**

La 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.

9.3. **Término y terminación**

9.3.1.Término

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC de la IOFE, y su periodo de vigencia es de 05 años al ser este el plazo de las acreditaciones otorgadas por la AAC de acuerdo a la legislación vigente. Esto sin perjuicio que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia del RENIEC o determinación de la AAC. Se contemplará que la validez de tal documentación estará sujeta a la continuidad de la acreditación.

9.3.2.Terminación

En caso de cese de actividades de la TSA-RENIEC, ésta informará a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones con una anticipación mínima de treinta (30) días calendario.

9.3.3.Efecto de terminación y supervivencia

Las obligaciones y restricciones que establecen en esta Declaración de Prácticas de Servicio de Valor Añadido, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, nacidas bajo la vigencia del presente documento, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.4. **Procedimiento sobre resolución de disputas**

En caso, el reclamo 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

9.5. Notificaciones y comunicaciones individuales con los participantes

Toda notificación o comunicación con la 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.

9.6. Cláusulas misceláneas

9.6.1.Acuerdo Íntegro

Los titulares y/o suscriptores de certificados digitales, así como los terceros que confían deben observar en su totalidad el contenido del presente documento, así como las actualizaciones que se realice sobre el mismo, las cuales estarán disponibles en la siguiente dirección:
http://www.reniec.gob.pe/repository/
https://pki.reniec.gob.pe/repositorio/

9.6.2.Fuerza Mayor

La ECEP-RENIEC, en ningún caso será responsable por daños o perjuicios causados por:

- Catástrofes naturales;
- Casos de guerra;
- Actos de terrorismo y/o sabotaje;
- Otros actos de fuerza mayor.

Sin perjuicio de lo expuesto, la ECEP-RENIEC, dentro de lo posible, asegurará la continuidad del negocio y recuperación ante desastres.

10. 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.

11. 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 1

A. Acrónimos

- **TSA: Autoridad de Sellado de Tiempo**
- **TSU: Unidad de Sellado de tiempo**
- **UTC: Tiempo Universal Coordinado**
- **AAC: Autoridad Administrativa Competente**
- **TSA-RENIEC: Autoridad de Sellado de tiempo del Registro Nacional de Identificación y Estado Civil**
- **TSS: Servicio de Sellado de tiempo**
- **OID: Identificador de Objeto**

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 de Autoridad:** Es un certificado digital de una entidad confiable y acredita que emite certificados digitales subordinados. En esta CP, se tienen tres niveles de autoridades (Raíz, ECEP y Clases de ECEP)
- **Cancelación de certificado digital (*).-** Anulación definitiva de un certificado digital a petición del suscriptor, un tercero o por propia iniciativa de la autoridad de certificación

en caso de duda de la seguridad de las claves o por cualquier motivo permitido y debidamente sustentado descritos en la Declaración de Prácticas de Registro o Verificación.

- **Certificación Cruzada.-** Es el acto por el cual una Entidad de Certificación acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.
- **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.
- **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.
- **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.-** 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.
- **Identidad digital):** Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.
- **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.
- **Notificación electrónica personal.-** En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.
- **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 de Intermediación Electrónico.-** 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 electrónica, autenticación y canales seguros.
- **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.
- **Usabilidad.-** En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación digital de manera efectiva, eficiente y satisfactoria.
- **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.