POLÍTICA DE SERVICIOS DE VALOR AÑADIDO

PRESTADORES DE SERVICIOS DE VALOR AÑADIDO PARA EL ESTADO PERUANO

Servicio de Sellado de Tiempo

ECERNEP

Versión: 3.0	**Año: 2018**

Elaborado por:	**Revisado por:**	**Aprobado por:**
Jefe de la ECERNEP	Sub Gerente de Regulación Digital	Gerente de Registros de Certificación Digital

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	04/12/2017	Elaboración y Aprobación	GRCD-SGREGD	Aprobado
2.0	26/09/2018	Actualización	GRCD-SGREGD	Aprobado
3.0	29/10/2018	Actualización	GRCD-SGREGD	Aprobado

ÍNDICE

1. INTRODUCCIÓN

Un sello de tiempo o *Time-Stamping* ofrece evidencia de que un dato existió en un momento en particular y que no ha sido alterado desde ese momento. En la generación de evidencia digital confiable y accesible es necesario disponer de un método concertado para asociar los datos de fecha y hora a una transacción, de manera que dicha asociación sea verificable con posterioridad.

Una transacción típica es aquella en la que, disponiéndose de un documento firmado digitalmente, se requiere luego probar que la firma digital fue generada cuando el certificado digital del firmante era válido.

Un sello de tiempo o marca de tiempo, que es un registro de auditoría guardado en un lugar seguro por una tercera parte confiable, al aplicarse a una firma digital, prueba en primer término que ésta fue creada antes de la fecha y hora incluida en el sello de tiempo.

Adicionalmente, para probar que la firma digital se generó mientras el certificado digital del firmante era válido, debe verificarse el cumplimiento de las siguientes condiciones:

a) Que el sello de tiempo haya sido aplicado antes de la conclusión del periodo de validez del certificado del firmante.
b) Que el sello de tiempo haya sido aplicado mientras que el certificado del firmante no se encuentre cancelado o antes de la fecha de cancelación del certificado.

Por lo tanto, un sello de tiempo aplicado de esa manera prueba que una firma digital fue creada mientras el certificado digital del firmante era válido.

Debe considerarse que en la prestación del servicio de sellado de tiempo o de cualquier otro servicio de certificación digital o de confianza, como aquellos brindados por un Prestador de Servicios de Valor Añadido (PSVA) de la (IOFE), se debe contar con una política y declaración de prácticas de sellado de tiempo y ponerse a la disposición de sus usuarios potenciales publicándose para ello en el repositorio correspondiente.

El RENIEC, como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) de la Infraestructura Oficial de Firma Electrónica (IOFE) de acuerdo a designación dada en el artículo 46 del Reglamento de la Ley de Firmas y Certificados Digitales (en adelante "el Reglamento"), desarrolla en el presente documento denominado "Política de Servicios de Valor Añadido – Servicio de Sellado de Tiempo", aplicable a aquellos prestadores de servicios de valor añadido que operen bajo las jerarquías PKI del Estado Peruano cuya raíz autofirmada es emitida por la ECERNEP. Dicha política, en concordancia con lo señalado en el numeral 10 de la "Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", Versión 4.0 publicada por el INDECOPI como autoridad administrativa competente (AAC), observa los lineamientos establecidos en el RFC 3628, *Policy Requirements for Time-Stamping Authorities (TSAs).* Además, se encuentra alineada con la Política General

de Certificación (CP) de la jerarquía ECERNEP PERÚ CA ROOT 3 y será de cumplimiento para los Prestadores de Servicios de Valor Añadido (en adelante PSVA) bajo la modalidad de sellado de tiempo (en adelante PSVA-TSA) a los que la ECERNEP emita el certificado digital bajo la misma jerarquía.

2. VISIÓN GENERAL

Los requisitos de políticas aquí establecidos apuntan a servicios de sellado de tiempo usados en respaldo de las firmas digitales emitidas bajo el marco de la IOFE, al igual que los dados en la norma ETSI EN 319 421 lo hacen respecto de las firmas electrónicas calificadas en el ámbito de la Unión Europea. No obstante, pueden aplicarse a cualquier uso que requiera probar que determinado dato existió antes de un momento en particular.

Estos requisitos de políticas están basados en el uso de criptografía de llave pública, certificados de llave pública y fuentes de tiempo confiables. El presente documento puede ser utilizado como base para determinar la confiabilidad en un PSVA dedicado a la provisión de servicios de sellado de tiempo (denominado PSVA-TSA).

Este documento establece requisitos para la sincronización de los PSVA-TSA que emiten sellos de tiempo bajo el Tiempo Universal Coordinado (UTC) firmados digitalmente por sus Unidades de Sellado de Tiempo *(Time Stamping Units* o TSU), siguiendo los lineamientos técnicos que se indican en el RFC 3161 *Time-stamp protocol*, actualizada por el RFC 5816 *ESSCertIDv2 Update for RFC 3161* y la norma ETSI EN 419 422.

3. DEFINICIONES Y ABREVIATURAS

Ver Anexo 1

4. CONCEPTOS GENERALES

4.1. Servicio de Sellado de Tiempo (TSS)

El servicio de sellado de tiempo 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.

Esta subdivisión en particular es solo para el propósito de clarificar los requisitos especificados en el presente documento y no pone restricciones respecto de cualquier otra subdivisión que pueda darse en la implementación de servicios de sellado de tiempo.

4.2. Autoridad de Sellado de Tiempo (TSA)

Es la autoridad que emite sellos de tiempo en los que confían los usuarios de los servicios de sellado de tiempo, es decir, los suscriptores y los terceros que confían. En la IOFE, la TSA no se encuentra reconocida explícitamente bajo esta denominación como una entidad o autoridad prestadora de servicios de certificación como las EC o las ER; no obstante, se reconoce el servicio de sellado de tiempo como una variante de aquellos servicios que pueden brindar los PSVA. Los PSVA-TSA o los PSVA que operen brindando el servicio de sellado de tiempo como subordinados a la EC-PSVA de la jerarquía del Estado Peruano ECERNEP PERÚ CA Root 3, son responsables de brindar los servicios identificados en el numeral 4.1 Servicio de Sellado de Tiempo (TSS) y deben encontrarse acreditados ante la AAC de la IOFE. Cabe señalar que, 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.

En el presente documento se habla indistintamente de una TSA y de un PSVA-TSA.

Las TSA son responsables por la operación de una o más Unidades de Sellado de Tiempo TSU, las cuales en la práctica son las que crean y firman sellos de tiempo en su nombre. Las TSA responsables de la emisión de un sello de tiempo deben ser identificables (ver numeral 7.3.1, literal h)).

Las TSA pueden valerse de terceros para brindar parte de los servicios de sellado de tiempo. Sin embargo, éstas siempre mantienen la responsabilidad total y deben asegurarse que los requisitos en la presente política se cumplen. Por ejemplo, una

TSA puede subcontratar todos los componentes del servicio, incluyendo aquellos que generan sellos de tiempo usando las llaves de las unidades de sellado de tiempo (TSU). Sin embargo, la llave o llaves privadas usadas para generarlos pertenecen a la TSA por lo que esta mantiene una total responsabilidad por el cumplimiento de los requisitos en este documento.

Una TSA puede operar varias TSU identificables. Cada unidad tiene una llave diferente. Ver el Anexo F de la norma ETSI EN 319 421 para posibles implementaciones.

Una TSU se define como un conjunto de hardware y software que opera creando firmas y sellos de tiempo en nombre de una TSA, cada cual con un par de llaves y un certificado digital propios.

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

Esta sección explica la relación entre el rol de una política de sellado de tiempo y el rol de una declaración de prácticas de sellado de tiempo. No se pone restricción en cuanto a la forma de una política de sellado de tiempo o en la especificación de una declaración de prácticas.

4.4.1. Propósito

En general, la política de sellado de tiempo define “qué es a lo que uno se adhiere”, mientras que una declaración de prácticas de la TSA define “cómo se adhiere a”, es decir, los procesos que usará en la creación de sellos de tiempo y el mantenimiento de la precisión de su reloj. La relación entre la política de sellado de tiempo y la declaración de prácticas de sellado de tiempo es similar en naturaleza a la relación entre otras políticas de negocio, que definen requisitos del negocio, con las prácticas y procedimientos definidos por las unidades operativas sobre cómo estas políticas se implementarán.

El presente documento especifica una política de sellado de tiempo para cumplir con los requisitos generales para servicios de sellado de tiempo confiables bajo la jerarquía ECERNEP PERÚ CA Root 3 que gestiona el RENIEC. Las TSA deben especificar en sus declaraciones de prácticas cómo cumple con estos requisitos.

4.4.2. Nivel de especificidad

La declaración de prácticas de la TSA es más específica que una política de sellado de tiempo. Una declaración de prácticas de sellado de tiempo es una descripción más detallada de los términos y condiciones así como de las prácticas de negocios y operativas de una TSA en la emisión o en la gestión de servicios de sellado de tiempo. La declaración de prácticas de una TSA implementa las reglas establecidas por una política de sellado de tiempo y define cómo una TSA en particular cumple con los requisitos técnicos, organizacionales y procedimentales identificados en la política de sellado de tiempo

NOTA: Incluso documentación interna de nivel más bajo puede resultar apropiada para que una TSA detalle los procedimientos específicos necesarios para desarrollar las prácticas identificadas en la declaración de prácticas de sellado de tiempo.

4.4.3. Enfoque

El enfoque de una política de sellado de tiempo difiere significativamente del de una declaración de prácticas. La política se define independientemente de detalles del entorno operativo específico de una TSA, mientras que una declaración de prácticas responde a la estructura organizacional, procedimientos operacionales, instalaciones y entorno informático de una TSA en particular. Bajo este enfoque, una política de sellado de tiempo podría ser definida por el usuario de los servicios, mientras que la declaración de prácticas siempre es definida por el proveedor.

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

El presente documento define los requisitos de una política de sellado de tiempo básica para la emisión de sellos de tiempo soportados por certificados de llave pública, con una precisión de un (01) segundo o mejor. A su vez, el presente documento recoge los requisitos establecidos en la norma ETSI EN 319 421 incorporándose las adecuaciones necesarias de acuerdo al marco normativo y regulatorio de la IOFE del Perú, de manera que el Prestador de Servicios de Valor Añadido para el Estado Peruano bajo la modalidad de servicio de sellado de tiempo o TSA (PSVA-TSA) pueda operar bajo la jerarquía ECERNEP PERÚ CA ROOT 3 que gestiona el RENIEC.

NOTA 1: Sin medidas adicionales las terceras partes que confían pueden no ser capaces asegura la validez de un sello de tiempo más allá del periodo de validez del

certificado digital bajo el que fue emitido. Ver el Anexo D de la norma ETSI EN 319 421 en relación a la verificación de la validez de un sello de tiempo más allá del periodo de validez del certificado de una TSU.

Se puede emplear el OID definido en la norma EN 319 421, que no presenta dependencia del derecho europeo.

Si la TSA brinda una precisión mejor que un segundo y si todas sus TSU tienen esta característica, entonces dicha precisión deberá referirse en la declaración de libre divulgación correspondiente (ver numeral 7.1.2).

NOTA 2: Se requiere que los sellos de tiempo incluyan un identificador de la política que les es aplicable (ver numeral 7.3.1).

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).

En la declaración de libre divulgación a ponerse a disposición de los suscriptores y terceros que confían, debe también incluirse el identificador de la política de sellado de tiempo para indicar su conformidad con ésta.

5.3. Comunidad de usuarios y aplicabilidad

Bajo el ámbito de la IOFE, la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, Versión 4.0, determina en el numeral 2 de su Anexo 1 que “El marco de evaluación de los controles definidos para la Autoridad de Sellado de Tiempo está basado en la RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs), cuya equivalencia funcional en la Communidad Europea se define en el estándar ETSI 102 023.”, y por ende el cumplimiento de los lineamientos establecidos en la política de sellado de tiempo básica dada en la norma ETSI EN 319 421 que recoge el presente documento como actualización del referido estándar ETSI TS 102 023, será de aplicación a los PSVA-TSA del Estado Peruano.

Cabe señalar que dicha política está dirigida en principio a cumplir con los requisitos del sellado de tiempo para las firmas electrónicas cualificadas de validez de largo plazo en la Unión Europea, según se definen en la especificación técnica TS 101 733, aunque puede aplicarse de manera general a cualquier uso que requiera una calidad equivalente del servicio.

La política definida en la norma ETSI EN 319 421 puede aplicarse a servicios de sellado de tiempo de tipo público o para servicios en una comunidad cerrada; no obstante, el presente documento que recoge sus requisitos será usado por los Prestadores de

Servicios de Valor Añadido en la variante de servicio de sellado de tiempo (PSVA-TSA) que operen bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3 que gestiona el RENIEC.

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; las que podrán actuar por medios individuales o valiéndose de medios automatizados, equipos o servicios TI.

El procedimiento que debe seguirse para acceder al servicio de sellado de tiempo debe publicarse en el TUPA de la entidad pública que lo opera, debiendo haber sido acreditada para ello por la AAC de la IOFE; sin embargo, de forma alternativa, la entidad pública que opere el servicio podrá otorgarlo a otras entidades del Estado en mérito al criterio de colaboración entre entidades conforme al marco legal vigente (artículos 76° y 77° de la Ley 27444, Ley del Procedimiento Administrativo General), en cuyo caso las solicitudes serán recibidas a través de la mesa de partes institucional, luego de lo cual serán respondidas y/o atendidas conforme a criterio técnico y de viabilidad que en su oportunidad evalué la unidad orgánica a cargo de la gestión del servicio.

5.4. Conformidad

Las TSA que operen bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3 que gestiona el RENIEC deben usar el identificador para la política de sellado de tiempo conforme se determina en el numeral 5.2 Identificación.

Según se establece en la norma ETSI EN 319 421, las TSA podrán usar el identificador propio de la política de sellado de tiempo allí especificado o definir su propia política de sellado de tiempo, que incorpore los mismos requisitos o que establezca mayores exigencias. La política de sellado de tiempo desarrollada en el presente documento recoge el mismo nivel de exigencia de la política básica dada en la norma ETSI EN 319 421; su ámbito de aplicación comprende a las TSA que operan bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3, especificándose en ella algunos requisitos procedimentales propios de la IOFE y de su marco normativo y regulatorio.

Además, tal como se indica en el numeral 1.2 del Anexo 1 de las Guías de Acreditación para Entidades de Certificación, los certificados digitales de los TSU deben identificarse con OID correspondiente a la entidad que lo emite.

A efectos de determinarse la conformidad o cumplimiento de la TSA respecto de la política de sellado de tiempo desarrollada en el presente documento, ésta deberá encontrarse acreditada por la AAC de la IOFE como parte independiente. Una TSA que opera en conformidad con esta política deberá haber demostrado que cumple con las obligaciones definidas en el numeral 6.1 Obligaciones de la TSA y que ha implementado controles de acuerdo con los requisitos especificados en el numeral 7 REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA.

6. OBLIGACIONES Y RESPONSABILIDADES

6.1. Obligaciones de la TSA

6.1.1. Generalidades

La TSA debe asegurarse que todos los requisitos establecidos en el numeral 7 REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA han sido implementados en aplicación de la política de sellado de tiempo que ha sido elegida en términos de la confianza inherente a la misma.

Además, debe asegurarse que se cumplen a cabalidad los procedimientos descritos en esta política, incluso si se realiza la contratación de terceros para desarrollar alguna funcionalidad propia de la TSA.

La TSA debe asegurar también su adherencia a cualquier otra obligación indicada en el sello de tiempo ya sea que ésta se indique expresamente o se incorpore por referencia.

La TSA debe brindar sus servicios de sellado de tiempo de manera consistente con su Declaración de Prácticas de valor Añadido (VAPS) bajo la variante de servicios de sellado de tiempo la que se encuentra en completa conformidad con esta política de sellado de tiempo.

6.1.2. Obligaciones de la TSA con los suscriptores

La TSA bajo la jerarquía PKI ECERNEP PERÚ CA Root 3 debe cumplir con lo establecido en su VAPS y en sus términos y condiciones de uso, incluyendo lo referido a la disponibilidad y a la precisión de su servicio.

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 de la TSA que emite el sello de tiempo y comprobar el estado de dicho certificado mediante la CRL o el sistema OCSP provistos por la ECERNEP. Más allá de ello, el suscriptor solo estará obligado a cumplir con los requerimientos específicos que la TSA pudiese referir en sus términos y condiciones de uso siempre y cuando no se contravenga lo establecido en la Ley de Firmas y Certificados Digitales, su Reglamento, normas complementarias y supletorias, y en la CP de la ECERNEP.

NOTA: Es recomendable que, al obtener un sello de tiempo, el suscriptor del servicio verifique que se encuentra correctamente firmado y que la llave privada utilizada no se encuentra comprometida. Lo más usual es que esta recomendación dada en la norma ETSI EN 319 421 se implemente de manera automatizada en la aplicación que haga uso del sello de tiempo.

6.3. Obligaciones de los terceros que confían

Los términos y condiciones a ponerse a disposición de los terceros que confían deben, en cuanto a su confianza en el sello de tiempo, contemplar su obligación 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.

   NOTA: Si el momento en el que se desea hacer la verificación es posterior al período de validez del certificado digital correspondiente a la TSU de la TSA, ver el Anexo D de la norma ETSI EN 319 421 donde se ofrece orientación al respecto.

b) Tener en cuenta cualquier limitación en el uso del sello de tiempo, conforme a lo indicado en este documento, en la VAPS o en los términos y condiciones de uso.
c) Tener en cuenta cualquier otro requisito o precaución que publique la ECERNEP en su sitio web (http://www.reniec.gob.pe/repository/) 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.

6.4. Responsabilidades

En cuanto a la determinación de responsabilidades, la ECERNEP y las TSAs bajo la jerarquía PKI ECERNEP PERÚ CA Root 3 deben operar en concordancia con la Política General de Certificación de la ECERNEP, las políticas de sellado de tiempo detalladas en el presente documento, y bajo el marco normativo y regulatorio de la IOFE en lo que les sea aplicable como prestadores de servicios de certificación digital del Estado Peruano.

La ECERNEP y las TSA no son responsables por la veracidad o contenido de los datos a los que se aplique los sellos de tiempo generados por éstas.

Bajo ninguna circunstancia, la ECERNEP y las TSA serán responsables por cualquier pérdida, daños indirectos o consecuentes o pérdida de datos que se pudiesen presentar en procesos o sistemas dentro de los que se aplican los sellos de tiempo generados por éstas últimas. Además, no serán responsables por los daños que 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.

La ECERNEP y las TSA bajo ninguna circunstancia serán responsables por los daños que resulten de eventos de fuerza mayor o desastres naturales, recomendándose, no obstante, la divulgación de las provisiones hechas para la recuperación de tales desastres conforme se detalla en la

NOTA 1 del numeral 7.1.2 Declaración de Libre Divulgación de la TSA. Ante una situación de este tipo, tomarán medidas razonables para mitigar los efectos o daños a un periodo de tiempo razonable.

7. REQUISITOS SOBRE LAS PRÁCTICAS DE LA TSA

Las TSA deben implementar los controles para cumplir con los requisitos que se dan a continuación.

No es la intención que estos requisitos de políticas impliquen restricción alguna respecto del cobro por el servicio de sellado de tiempo.

Los requisitos están especificados en términos de objetivos de seguridad, seguidos por requisitos más específicos que permiten evidenciar cómo los controles posibilitan el cumplir con dichos objetivos en aquellos casos en los que resulta necesario brindar confianza respecto de dicho cumplimiento.

NOTA: Las características de los controles requeridas para cumplir con un objetivo resultan de un balance entre lograr la confianza necesaria y minimizar las restricciones en relación a las técnicas que una TSA puede emplear para la emisión de sellos de tiempo. En el numeral 7.4 Gestión y operación de la TSA, se refiere un mayor detalle de los requisitos de control. Debido a estas consideraciones la especificidad de los requisitos dados bajo ciertos tópicos puede variar.

La provisión de un sello de tiempo en respuesta a una solicitud se da a discreción de la TSA dependiendo de los acuerdos de nivel de servicio con el suscriptor del servicio.

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

7.1.1. Declaración de Prácticas de la TSA

Los procedimientos definidos y su implementación por la TSA bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3 son evaluados mediante un proceso de acreditación realizado por la AAC, dentro del marco de la IOFE. En la IOFE, y conforme a lo señalado en la Guía de Acreditación de Prestadores de Servicios de Valor Añadido, Versión 4.0, el PSVA bajo la variante de servicio de sellado de tiempo o TSA deben desarrollar y presentar una Declaración de Prácticas de Valor Añadido (VAPS) siguiendo los lineamientos dados en la norma ETSI EN 319 421 bajo cuyo alcance será acreditado. En consecuencia, para los fines del presente documento, las exigencias establecidas respecto de la Declaración de Prácticas de la TSA, conforme se le denomina en la norma ETSI EN 319 421, se considerarán hechas a la Declaración de Prácticas de Valor Añadido para el servicio de sellado de tiempo, tal como se denomina en la referida guía de acreditación.

La TSA debe asegurarse que su declaración de prácticas demuestra la confiabilidad necesaria para brindar servicios de sellado de tiempo.

En particular:

a) La TSA debe desarrollar un análisis de riesgos periódicamente, identificando los activos y las amenazas a dichos activos, determinando los controles de seguridad y procedimientos operacionales necesarios para mitigar los riesgos identificados.

b) La TSA debe tener una declaración de las prácticas y procedimientos que usa para cumplir con todos los requisitos identificados en esta política de sellado de tiempo.

   NOTA: La política definida en la norma ETSI EN 319 421 no establece un requisito en cuanto a la estructura de la Declaración de Prácticas de la TSA, no obstante, la presente política requiere que se desarrolle siguiendo su misma estructura a efectos de facilitar el análisis de la alineación correspondiente.

c) La Declaración de Prácticas de la TSA debe identificar las obligaciones de todas las organizaciones externas que brindan soporte a sus servicios, incluyendo aquellas políticas y prácticas que les son aplicables.

d) La TSA debe divulgar a todos los usuarios y terceros que confían su declaración de prácticas y otra información relevante, según resulte necesario, de manera que se verifique la conformidad del caso con la presente política de sellado de tiempo.

   NOTA: No se requiere a la TSA hacer públicos todos los detalles referidos a sus prácticas.

e) La TSA debe divulgar a todos los suscriptores del servicio y potenciales terceros que confían los términos y condiciones de uso de sus servicios de sellado de tiempo según se especifican en el numeral 7.1.2 Declaración de Libre Divulgación de la TSA.

f) La Declaración de Prácticas de la TSA debe ser aprobada por la Autoridad Administrativa Competente (AAC).

g) La Entidad Pública a cargo de la TSA debe velar porque las prácticas de sellado de tiempo declaradas se implementen adecuadamente. Además, los PSVA-TSA, siguen bajo la IOFE un proceso de acreditación por el que se valida su adhesión a los lineamientos de políticas dados por la norma ETSI EN 319 421, lo cual se recoge en el presente documento que es de aplicación a las PSVA-TSAs bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3, habiéndose introducido las adecuaciones del caso contemplando el marco normativo y regulatorio que corresponde.[1]

[1] La Infraestructura Oficial de Firma Electrónica (IOFE) opera bajo el marco de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, su reglamento y modificatorias. El INDECOPI como Autoridad Administrativa Competente de la IOFE ejerce funciones de auditoría y supervisión en el esquema, además de desarrollar, aprobar y publicar las guías de acreditación que son de aplicación a los prestadores de servicios de certificación, entre los que se encuentran los PSVAs de sellado de tiempo o TSAs conforme se denominan en la norma ETSI EN 319 421 y en el presente documento.

h) La TSA debe definir un proceso de revisión para las prácticas, incluyendo responsabilidades para el mantenimiento de la Declaración de Prácticas de la TSA.

i) La TSA debe hacer la debida notificación de los cambios que pretende efectuar en su declaración de prácticas. Para ello, siguiendo el procedimiento de aprobación conforme se describe antes en f), procede a ponerla a disposición de manera inmediata conforme se requiere en d).

7.1.2. Declaración de Libre Divulgación de la TSA

La TSA debe divulgar a todos sus suscriptores y potenciales terceros que confían los términos y condiciones referidos al uso de sus servicios de sellado de tiempo. Esta declaración debe especificar al menos lo siguiente respecto de la política de sellado de tiempo definida en el presente documento:

a) La información del contacto de la TSA.

b) La política de sellado de tiempo que se aplica. En el caso de las TSAs bajo la jerarquía PKI ECERNEP PERÚ CA Root 3 deberá aludirse al presente documento.

c) Al menos un algoritmo de hash que se utiliza para representar los datos objeto del sellado de tiempo. Bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3 el algoritmo utilizado es SHA-256.

d) El tiempo de vida esperado de la firma que usa para firmar el sello de tiempo. Considerando que las TSAs bajo la jerarquía PKI ECERNEP PERÚ CA Root 3 utilizan el algoritmo de hash SHA-256, el algoritmo de firma RSA y una longitud de llaves de 2048 bits, el tiempo esperado de vida es de al menos 6 años[2].

e) La precisión del tiempo utilizado en los sellos de tiempo con respecto a UTC es de ± 1 segundo para las PSVA-TSA que operan bajo la jerarquía PKI ECERNEP PERÚ CA ROOT 3.

f) Cualquier limitación respecto del uso del servicio de sellado de tiempo.

g) Las obligaciones de los suscriptores conforme se definen en el numeral 6.2 Obligaciones de los suscriptores, del presente documento.

h) Las obligaciones de los terceros que confían conforme se definen en el numeral 6.3 Obligaciones de los terceros que confían.

i) La información de cómo verificar el sello de tiempo de manera que se considere que el tercero que confía puede “razonablemente confiar” en el éste (ver numeral 6.3 Obligaciones de los terceros que confían) y sobre cualquier posible limitación respecto del periodo de validez.

j) Los PSVA-TSA deben almacenar los registros de eventos *(logs)* durante un periodo mínimo de diez (10) años, en conformidad con la legislación peruana.

[2] Cfr. sección 9.2 de la especificación ETSI TS 119 312:2014.

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 4.0 y a lo que disponga de acuerdo a sus atribuciones la AAC de la IOFE.

l) Limitaciones en la responsabilidad.

m) Procedimientos para la atención de quejas y la solución de disputas.

n) Los PSVA-TSA son auditados por la AAC en cuanto a la conformidad de sus servicios con los lineamientos y con los requisitos básicos de sellado de tiempo dados en el RFC 3628 o en la norma ETSI EN 319 421, los que son recogidos en el presente documento, contemplándose las adecuaciones del caso en cuanto al marco normativo y regulatorio de aplicación a la IOFE..

NOTA 1: Se recomienda que la TSA incluya en su declaración de libre divulgación la disponibilidad de su servicio, por ejemplo el tiempo medio entre fallas esperado, el tiempo medio de recuperación siguiendo a una falla y las provisiones hechas para la recuperación de desastres incluyendo servicios de respaldo.

Esta información se debe divulgar a través de medios de comunicación durables y en un lenguaje de fácil comprensión. Podrá transmitirse por medios electrónicos.

NOTA 2: Un modelo de declaración de libre divulgación que puede usarse como base para tal documento se encuentra en el Anexo D del RFC 3628. Alternativamente, esto puede proveerse como parte de un acuerdo entre el suscriptor del servicio y la tercera parte que confía. La declaración de libre divulgación de la TSA puede incluirse dentro de su declaración de prácticas siempre que ésta se encuentre a disposición de las partes.

7.2. Ciclo de vida de la gestión de llaves

7.2.1. Generación de las llaves de la TSA

La TSA se debe asegurarse que las llaves criptográficas se generan en circunstancias bajo control.

En particular:

a) La generación de las llaves de firma de la TSU se debe llevar a cabo en un entorno con seguridad física (ver numeral 7.4.4) por personal en roles de confianza (ver numeral 7.4.3) bajo, al menos, control dual. El personal autorizado para desarrollar esta función debe limitarse a aquel que se establece que lo haga bajo las prácticas de la TSA.

b) La generación de las llaves de firma de la TSU debe llevarse a cabo en un módulo criptográfico certificado conforme a Common Criteria, perfiles de

protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda[3]; o según el estándar ISO/IEC 19790[4] nivel 3, como mínimo, o el estándar FIPS 140-2 nivel 3[5], como mínimo

c) El algoritmo de generación de llaves del TSU debe ser SHA-256, la longitud de la llave de firma resultante debe ser 2048 bits y el algoritmo de firma usado para la firma de sellos de tiempo debe ser Sha256WithRSA

7.2.2. Protección de las llaves privadas de la TSU

La TSA debe asegurar que las llaves privadas de la TSU permanecen confidenciales y mantienen su integridad.

En particular:

a) La llave privada de firma de la TSU debe mantenerse y ser usada en un módulo criptográfico certificado conforme a Common Criteria, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda; o según el estándar ISO/IEC 19790 nivel 3, como mínimo, o el estándar FIPS 140-2 nivel 3, como mínimo.

   NOTA: No se recomienda el respaldo de llaves privadas de las TSU para minimizar los riesgos de que se vean comprometidas.

b) En los casos en los que las llaves de la TSU se respalden, su copiado, almacenamiento y recuperación debe llevarse a cabo solo por personal en roles de confianza usando, al menos, control dual dentro de un entorno con seguridad física (ver numeral 7.4.4). El personal autorizado para llevar a cabo esta función debe limitarse a aquel que se establece que lo haga bajo las prácticas de la TSA.
c) Cualquier copia de respaldo de las llaves privadas de firma de las TSU debe protegerse para asegurar su confidencialidad a través del módulo criptográfico antes de almacenarse fuera de aquel dispositivo.

7.2.3. Distribución de las llaves públicas de la TSU

La TSA debe asegurarse que la integridad y autenticidad de las llaves públicas de verificación de firma de las TSU y cualquier parámetro asociado a éstas se mantiene durante su distribución a las terceras partes que confían.

En particular:

[3] Cfr. sección 6.5.2 de ETSI EN 319 411-1. Estos perfiles de protección actualizan las antiguas especificaciones CEN CWA 14167, partes 2 a 5, referenciados en el Anexo 11 de la Guía de Acreditación.
[4] Esta norma es equivalente a FIPS 140-2, en el ámbito internacional.
[5] FIPS valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

a) Las llaves públicas de verificación de firma de las TSU se deben poner a disposición de las terceras partes que confían en un sello de tiempo.

NOTA: En el RFC 3628 se señala que los certificados de las TSU pueden ser emitidos por una entidad de certificación operada por la misma organización que opera la TSA o emitidos por otra autoridad. En el caso de los certificados de las TSU que corresponden a las TSA bajo la Jerarquía ECERNEP PERÚ CA ROOT 3 es la ECERNEP quien emite estos certificados.

b) El certificado digital para la verificación de la firma de las TSU debe ser emitido por la ECERNEP operando bajo la Política General de Certificación de la ECERNEP, la misma que brinda el nivel de seguridad exigido en la norma EN 319 421 y en la presente Política de Servicios de Valor Añadido de Servicio de Sellado de Tiempo, o superior.

7.2.4. Regeneración de las llaves de las TSU

El tiempo de vida de los certificados de las TSU no debe ser más largo que el periodo de tiempo reconocido como adecuado para el algoritmo y longitud de clave elegidos y considerados adecuados para su emisión (ver literal c del numeral 7.2.1).

NOTA 1: Las siguientes consideraciones adicionales son de aplicación al limitarse dicho tiempo de vida:

- El numeral 7.4.10 Cumplimiento de requisitos legales requiere que los registros concernientes a los servicios de sellado de tiempo se mantengan por un periodo de tiempo apropiado, el que al menos es de un año luego de la expiración de la validez de las llaves de firma de las TSU. Mientras más largo sea el periodo de validez de los certificados de las TSU, más largo será el tiempo que dichos registros deberán mantenerse.
- Al comprometerse la llave privada de una TSU, entonces mientras más largo sea el tiempo de vida del certificado de la TSU más será la cantidad de sellos de tiempo emitidos que se vean afectados.

NOTA 2: El compromiso de la clave de la TSU no solo depende de las características del módulo criptográfico utilizado sino también de los procedimientos usados al inicializar el sistema y exportar la llave (cuando esta función es soportada).

7.2.5. Fin del ciclo de vida de la TSU

Los PSVA-TSA deben garantizar que las llaves privadas de sus TSU no puedan usarse en un tiempo posterior al fin de su ciclo de vida (validez).

En particular:

a) Procedimientos operacionales o técnicos deben encontrarse implementados para garantizar que se dispone de una nueva clave cuando la llave de una TSU expira.
b) Las llaves privadas de firma de las TSUs, o cualquier parte de una llave, incluyendo cualquier copia, deben destruirse de tal manera que las claves privadas no se pueden recuperar.
c) El sistema de generación de sellos de tiempo debe rechazar cualquier intento de emisión si la clave privada de firma ha expirado.

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

Los PSVA-TSA debe garantizar la seguridad del hardware criptográfico a lo largo de su ciclo de vida.

En particular, la TSA garantiza que:
a) El hardware criptográfico para la firma de sellos de tiempo no es adulterado durante su transporte;
b) El hardware criptográfico para la firma de sellos de tiempo no es adulterado durante su almacenamiento;
c) La instalación, activación y duplicado de las claves de firma de las TSU debe efectuarse en el hardware criptográfico solo por personal en roles de confianza usando, al menos, control dual en un entorno que disponga de seguridad física (ver numeral 7.4.4);
d) El hardware criptográfico para la firma de sellos de tiempo funciona correctamente; y
e) Las claves privadas de firma de la TSU almacenadas en el módulo criptográfico son borradas al producirse el retiro o reemplazo de un dispositivo.

7.3. Sellado de tiempo

7.3.1. Sello de tiempo

La TSA debe garantizar que los sellos de tiempo son emitidos con seguridad y que incluyen la fecha y hora correctas.

En particular:
a) El sello de tiempo debe incluir el OID de la política de sellado de tiempo;
b) Cada sello de tiempo debe tener un identificador único;
c) Los valores de fecha y hora que la TSU utiliza en el sello de tiempo deben al menos ser trazables hasta uno de los valores de tiempo real distribuidos por un laboratorio UTC (k).

NOTA 1: El *Bureau International des Poids et Mesures* (BIPM) computa 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 incluidos en el sello de tiempo deben sincronizarse con el UTC con la precisión definida en ésta política y, si está presente, con la precisión definida en el sello de tiempo mismo;
e) Si el reloj del proveedor de sellos de tiempo se detecta (ver literal c del numeral 7.3.2) como fuera de la precisión definida (ver literal e del numeral 7.1.2), entonces los sellos de tiempo no deben emitirse.
f) Los sellos de tiempo deben incluir una representación (por ejemplo un hash) de los datos que se están sellando tal como han sido provistos por el solicitante del servicio;
g) El sello de tiempo debe ser firmados usando una llave generada exclusivamente para este propósito.

NOTA 2: En el RFC 3161 se define un protocolo para sellos de tiempo y en la EN 319 422[6] se define un perfil. El primero es reconocido en la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, Versión 4.0, dentro de los estándares cuyo uso "promueve la confianza del usuario y…propugna el reconocimiento transnacional de certificados". En el RFC 3628 se menciona erróneamente al RFC 3631 en lugar del RFC 3161.

NOTA 3: En el caso de presentarse una serie de solicitudes a aproximadamente el mismo tiempo, bastará que su atención se dé dentro del tiempo de precisión establecido para el reloj de la TSU, no siendo obligatoria su atención en un orden específico.

h) El sello de tiempo debe incluir:
   - Donde sea aplicable, un identificador del país en el cual la TSA se encuentra establecida;
   - Un identificador para la TSA;
   - Un identificador para la unidad que emite los sellos de tiempo.

7.3.2. Sincronización del reloj con el UTC

La TSA debe garantizar que su reloj esté sincronizado con el UTC dentro de la precisión declarada.

En particular:

[6] EN 319 422 es la norma que actualiza y sucede a la especificación técnica TS 101 861.

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.
b) Los relojes de las TSU deben protegerse contra amenazas que pudiesen resultar en cambios no detectados que puedan afectar su calibración.

NOTA 1: Las amenazas pueden incluir la manipulación por personal no autorizado y otras que se pudiesen producir a través de radiofrecuencia o choques eléctricos.

c) La TSA debe garantizar que, si la fecha y hora a incorporarse en un sello de tiempo se desvía o se sale de sincronización con UTC, esto se detecta (ver literal e del numeral 7.3.1).

NOTA 2: Los terceros que confían son informados de tales eventos.

d) La TSA debe garantizar que se mantiene la sincronización del reloj cuando se produce *leap second* el cual es notificado por el organismo correspondiente. El cambio a contemplarse se produce durante el último minuto del día en el que se haya previsto que ocurra el mismo. Debe mantenerse un registro de la fecha y hora exactas (dentro de la precisión declarada) de cuando este cambio ocurre. Ver anexo C de la norma EN 319 421 para más detalles.

NOTA 3: 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.

7.4. Gestión y operación de la TSA

7.4.1. Gestión de la seguridad

La TSA debe garantizar que los procedimientos administrativos y de gestión que se aplican son adecuados y corresponden a las mejores prácticas reconocidas.

De manera particular:

a) La TSA debe mantener responsabilidad por todos los aspectos de la provisión de servicios de sellado de tiempo bajo el alcance de la presente política, ya sea que sus funciones sean o no tercerizadas a subcontratistas. Las responsabilidades de los terceros se definen claramente por la TSA y se efectúan arreglos apropiados para garantizar que implementan con certeza los controles que requiere la TSA. La TSA retiene responsabilidad por la difusión de sus prácticas relevantes a todas las partes involucradas.
b) Los gestores de la TSA deben brindar dirección sobre la seguridad de la información a través de un comité de gestión de alto nivel adecuado 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 necesaria para administrar la seguridad en la TSA debe recibir mantenimiento permanente. Cualquier cambio que impacte en el nivel de seguridad provisto debe ser aprobado por el comité de gestión de seguridad de la información de la TSA.

NOTA 1: Ver ISO/IEC 27002 para una guía en la gestión de la seguridad de la información incluyendo la infraestructura de seguridad de la información, el comité de gestión de seguridad de la información y las políticas de seguridad de la información.

d) Los controles de seguridad y los procedimientos operacionales para las instalaciones, sistemas y activos de la información de la TSA deben encontrarse documentados, implementados y reciben mantenimiento de manera adecuada.

NOTA 2: La documentación presente (comúnmente llamada política de seguridad de sistema o manual) debe identificar todas las amenazas potenciales relacionadas a los servicios brindados y las medidas requeridas para evitar o reducir los efectos de dichas amenazas, de acuerdo con el Análisis de Riesgos (ver literal a del numeral 7.1.1). Debe describir las reglas, directivas y procedimientos de cómo se garantiza el servicio y la seguridad.

e) La TSA debe garantizar que la seguridad de la información se mantiene cuando la responsabilidad sobre ciertas funciones de la TSA ha sido tercerizada a otra entidad u organización.

7.4.2. Clasificación y gestión de activos

La TSA debe garantizar que su información y otros activos reciben un nivel apropiado de protección.

En particular, la TSA debe mantener un inventario de todos sus activos y establece una clasificación para los requisitos de protección que les corresponde, la que guarda consistencia con el análisis de riesgos efectuado.

7.4.3. Seguridad del personal

La TSA debe garantizar que el personal y las prácticas para su contratación optimizan y dan soporte a la confiablidad de sus operaciones.

En particular:

a) La TSA debe emplear personal que posee el conocimiento especializado, la experiencia y las calificaciones necesarias en concordancia con los servicios ofrecidos y apropiados para la función de trabajo a realizar.

NOTA 1: El personal de la TSA debería ser capaz de cumplir con los requisitos de "conocimiento especializado, la experiencia y las calificaciones" mediante el entrenamiento formal y certificaciones, experiencia real o una combinación de ambas.

NOTA 2: El personal empleado por una TSA incluye personas naturales contratadas para llevar a cabo funciones para el desarrollo de los servicios de sellado de tiempo. Aquel personal que se dedique solo al monitoreo de servicios de la TSA no necesita ser personal propio de la TSA.

b) Los roles y responsabilidades de seguridad, según se especifica en la política de seguridad de la TSA, deben documentarse en descripciones de los puestos de trabajo. Los roles de confianza, en los cuales depende la seguridad de las operaciones de la TSA, están claramente identificados.
c) El personal de la TSA (ya sea temporal o permanente) debe contar con descripciones del puesto de trabajo definidas contemplando la separación de tareas y sus privilegios mínimos, encontrándose determinada la sensibilidad del puesto según la criticidad de las tareas desarrolladas y concordantemente con los niveles de acceso asignados, lo que a su vez se acompaña de una revisión de antecedentes personales, entrenamiento y conocimiento del puesto adecuados. Donde resulte apropiado, debe establecerse una diferenciación entre funciones generales y funciones específicas de la TSA. Bajo este contexto, deberían contemplarse asimismo requisitos para el personal en cuanto a habilidades y experiencia.
d) El personal debe desarrollar procesos y procedimientos administrativos y de gestión alineados con los procedimientos de gestión de seguridad de la información de la TSA (ver numeral 7.4.1).

NOTA 3: Ver NTP-ISO/IEC 27002 por guía.

Los siguientes controles adicionales deben aplicarse al personal de gestión de la TSA:

e) Se debe contratar personal de gestión que posee:
   - Conocimientos de la 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.
f) Todo el personal en roles de confianza debe encontrarse libre de conflictos de intereses que pueden perjudicar la imparcialidad de las operaciones de la TSA.
g) Los roles de confianza incluyen roles que involucran 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 de la TSA debe ser designado formalmente para puestos de confianza por altos directivos responsables de la seguridad.

i) La TSA no debe designar para roles de confianza o de gestión a cualquier persona que se sepa ha 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.

7.4.4. Seguridad física y del entorno

La TSA debe garantizar que el acceso físico a los servicios críticos se encuentre bajo control y que los riesgos físicos a sus activos se encuentren minimizados.

En particular (general):

a) Tanto respecto de la provisión de sellos de tiempo como de otros aspectos de la gestión del servicio:
   - El acceso físico a las instalaciones que tienen que ver con los servicios de sellado de tiempo debe limitarse a individuos debidamente autorizados.
   - Debe contarse con controles implementados para evitar la pérdida, daño o compromiso de activos y la interrupción de actividades de negocios.
   - Debe contarse con controles para evitar el compromiso o robo de información y de las instalaciones para su procesamiento.

b) Deben aplicarse controles de acceso al módulo criptográfico en cumplimiento de los requisitos de seguridad establecidos para el mismo según los numeral 7.2.1 Generación de las llaves de la TSA y 7.2.2 Protección de las llaves privadas de la TSU.

c) Los siguientes controles adicionales deben aplicarse a la gestión del sellado de tiempo:
   - Las instalaciones para la gestión del sellado de tiempo deben operarse en un entorno que ofrece protección física a los servicios de su compromiso a través del acceso no autorizado a los sistemas o a datos.
   - La protección física se debe lograr a través de la creación de perímetros de seguridad claramente definidos (por ejemplo, barreras físicas)

alrededor de las áreas donde se gestiona el sellado de tiempo. Cualquier área de las instalaciones que sea compartida con organizaciones distintas se encontrará fuera de este perímetro.

- Controles ambientales y físicos deben implementarse para proteger las instalaciones que alojan los recursos de sistemas, los recursos de sistemas mismos y las instalaciones usadas para dar soporte a sus operaciones. La política de seguridad para los sistemas relacionados con la gestión del sellado de tiempo, en lo relacionado a aspectos físicos y ambientales, contemplan como mínimo el control de acceso físico, la protección contra desastres naturales, factores de seguridad ante incendios, fallas en los servicios públicos de soporte (por ejemplo, energía eléctrica y telecomunicaciones), colapso de la estructura, fugas de agua, protección contra el robo, ruptura e ingreso, y recuperación de desastres.
- Debe implementarse controles para prevenir el retiro no autorizado de equipos, información, medios de almacenamiento de datos y software relacionados con los servicios de sellado de tiempo.

NOTA 1: Ver ISO/IEC 27002 para obtener guía sobre la seguridad física y ambiental.

NOTA 2: Otras funciones pueden desarrollarse dentro de la misma área segura en la medida que el acceso se encuentre limitado a personal autorizado.

7.4.5. Gestión de operaciones

La TSA debe garantizar que los componentes de sus sistemas son seguros y correctamente operados, contando con un riesgo de fallas minimizado.

En particular:

a) La integridad de los componentes de los sistemas y de la información de la TSA debe protegerse contra virus, software malicioso o no autorizado.
b) Los reportes de incidentes y los procedimientos de respuesta deben emplearse de tal forma que el daño por incidentes de seguridad y malfuncionamientos se minimiza.
c) Los medios de almacenamiento de datos utilizados en los sistemas confiables de la TSA deben manipularse con seguridad para protegerlos del daño, robo, acceso no autorizado y obsolescencia.

NOTA 1: Cada miembro del personal con responsabilidades de gestión es responsable del planeamiento y de la implementación efectiva de la política de sellado de tiempo y de las prácticas que se le asocian según se encuentran documentadas en la declaración de prácticas de la TSA.

d) Deben establecerse e implementarse procedimientos para todos los roles de confianza y administrativos que impactan en la provisión de los servicios de sellado de tiempo.

Manipulación y seguridad de los medios de almacenamiento de datos

e) Todos los medios de almacenamiento de datos deben manipularse de forma segura en concordancia con los requisitos del esquema de clasificación de la información (ver numeral 7.4.2). Los medios de almacenamiento que contienen datos sensibles deben desecharse de forma segura cuando no se les requiere más.

Planeamiento de sistemas

f) La demanda de capacidad debe monitorearse y deben realizarse proyecciones de la capacidad futura requerida para garantizar el disponer de adecuadas potencia de proceso y capacidad de almacenamiento.

Reporte de incidentes y respuesta a incidentes

g) La TSA debe actuar de manera oportuna y coordinada para responder rápidamente a incidentes y para limitar el impacto de las brechas de seguridad. Todos los incidentes deben reportarse tan pronto como es posible luego de sucedidos.

Los siguientes controles adicionales deben aplicarse a la gestión de sello de tiempo:

Procedimientos operacionales y responsabilidades

h) Las operaciones de seguridad de la TSA deben separarse de otras operaciones.

NOTA 2: Las responsabilidades sobre las operaciones de seguridad de la TSA incluyen:

- Procedimientos operacionales y responsabilidades
- Planeamiento y aceptación de sistemas de seguridad
- Protección de software malicioso
- Limpieza de las instalaciones
- Gestión de redes
- Monitoreo activo de reportes de auditoría, análisis y seguimiento de eventos
- Manipulación y seguridad de medios de almacenamiento de datos
- Intercambio de datos y software

Estas operaciones deben gestionarse por personal de confianza de la TSA, pero pueden ser llevadas a cabo por personal operativo no especializado (bajo supervisión), según se define dentro de la política de seguridad apropiada y en la documentación de roles y responsabilidades.

7.4.6. Gestión de acceso a los sistemas

La TSA debe garantizar que el acceso a sus sistemas se encuentra limitado a individuos debidamente autorizados

En particular:

a) Controles (por ejemplo, firewalls) deben implementarse para proteger los dominios internos de red de la TSA del acceso no autorizado, incluyendo el acceso de suscriptores al servicio o terceras partes.

   NOTA 1: Los firewalls se configuran también excluyéndose los protocolos y accesos no requeridos para la operación de la TSA.

b) La TSA debe garantizar una eficaz administración de acceso para los usuarios (esto incluye a operadores, administradores y auditores) manteniéndose la seguridad del sistema, incluyendo la gestión de cuentas de usuarios, la auditoría y la modificación oportuna o eliminación de acceso.
c) La TSA debe garantizar que el acceso a las funciones vinculadas con la gestión de la información y las aplicaciones de software está restringida de acuerdo con la política de control de acceso y que los sistemas de la TSA brindan suficientes controles de seguridad computacional para la separación de los roles de confianza identificados de acuerdo a las prácticas de la TSA, incluyendo la separación de las funciones de gestión de la seguridad y funciones operativas. De manera particular, el uso de programas utilitarios del sistema se encuentra restringido y estrictamente controlado.
d) El personal de la TSA debe ser identificado y autenticado apropiadamente antes de usar aplicaciones críticas relacionadas con el sellado de tiempo.
e) El personal debe responder por las acciones que efectúa, por ejemplo la retención o manipulación de registros de eventos *(logs).*

Los siguientes controles adicionales son aplicados a la gestión del sellado de tiempo:

f) La TSA debe asegurarse que los componentes de la red local (por ejemplo, los routers) se mantienen en un entorno con seguridad física y que sus configuraciones son auditadas periódicamente en cuanto al cumplimiento de los requisitos especificados por la TSA.

g) Debe brindarse un monitoreo continuo e instalación de alarmas que posibilitan a la TSA la detección, registro y respuesta de una manera oportuna ante cualquier intento no autorizado y/o irregular para acceder a sus recursos.

NOTA 2: Esto puede basarse, por ejemplo, en sistemas de detección de intrusos y en instalaciones de monitoreo y alarma para el control de acceso.

7.4.7. Mantenimiento y despliegue de sistemas confiables

La TSA puede usar sistemas confiables y productos protegidos contra modificaciones como los que cumplen los requisitos de la especificación técnica CEN/TS 419 261.

7.4.8. Compromiso de los servicios de la TSA

La TSA debe garantizar que en el caso de eventos que afecten la seguridad de los sus servicios, incluyendo el compromiso de las llaves privadas de firma de la TSU o la detección de una pérdida de calibración, esta información relevante se pone en conocimiento de los suscriptores del servicio y de los terceros que confían.

En particular:

a) El plan de recuperación de desastres de la TSA debe contemplar el compromiso o sospechado compromiso de las claves privadas de firma de la TSU, el cual podría haber afectado a los sellos de tiempo emitidos.
b) En caso de un compromiso o sospechado compromiso, o de la pérdida de calibración, la TSA debe poner a disposición de todos los suscriptores del servicio y terceros que confían una descripción del compromiso ocurrido.
c) En el caso del compromiso de las operaciones de una TSU (por ejemplo, el compromiso de su llave), el sospechado compromiso o pérdida de calibración, la TSU no debe emitir sellos de tiempo hasta que se tomen medidas para recuperarse del compromiso.
d) En caso de un compromiso mayor de las operaciones de la TSA o pérdida de calibración, en la medida de lo posible, la TSA debe poner a disposición de todos los suscriptores del servicio y terceras partes que confían la información para identificar los sellos de tiempo afectados, a menos que esto viole la privacidad de los usuarios de la TSA o la seguridad de los servicios de la TSA.

NOTA: En caso de que la llave privada se vea comprometida, un registro de auditoría de todos los sellos de tiempo generados por la TSA debe brindar un medio para discriminar entre sellos de tiempo antiguos genuinos y falsos. Disponer de dos sellos de tiempo de TSA diferentes puede ser otra manera de enfrentar esta situación.

7.4.9. Terminación de la TSA

La TSA debe asegurarse que cualquier potencial interrupción del servicio de sellado de tiempo a sus suscriptores y a los terceros que confían se minimice al producirse el cese los servicios de sellado de tiempo, y de manera particular garantiza que se mantenga disponible de manera continua la información requerida para verificar la corrección de los sellos de tiempo.

En particular:

a) Antes de que la TSA concluya sus servicios de sellado de tiempo, como mínimo debe ejecutar los siguientes procedimientos:

- La TSA debe poner a disposición de todos los suscriptores y terceros que confían la información concerniente a su terminación.
- La TSA debe concluir la autorización a todos sus subcontratistas para actuar en su nombre llevando a cabo cualquier función relacionada con el proceso de emisión de sellos de tiempo.
- La TSA debe transferir sus obligaciones a una parte confiable para el mantenimiento del registro de eventos y los archivos de auditoría o logs (ver numeral 7.4.10 Cumplimiento de requisitos legales) necesarios para demostrar su correcta operación por un periodo razonable.
- La TSA debe mantener o transferir a una parte confiable su obligación de poner a disposición su llave pública o sus certificados a las terceras partes que confían por un periodo razonable de tiempo.
- Las llaves privadas de la TSU, incluyendo las copias de respaldo, se deben destruir de manera tal que no puedan recuperarse.

b) La entidad de la Administración Pública que gestiona una TSA deberá tomar las previsiones para disponer de los recursos necesarios, de manera que se pueda cumplir con dichos requisitos mínimos.

c) La TSA debe establecer entre sus prácticas las provisiones hechas para la conclusión de sus servicios. Estas deben incluir:
   - Notificación a las entidades afectadas.
   - Transferencia de las obligaciones de la TSA a otras partes.

d) La TSA debe tomar pasos para la cancelación de los certificados de las TSU.

7.4.10. Cumplimiento de requisitos legales

La TSA debe garantizar el cumplimiento de los requisitos legales establecidos en el Perú. En particular:

a) En lo referente a la Ley Nº 27269, Ley de firmas y certificados digitales, su Reglamento y modificatorias.

b) En lo referente a la Ley Nº 29733, Ley de protección de datos personales, su Reglamento y modificatorias.

c) Se toman medidas técnicas y organizacionales contra el procesamiento ilegal o no autorizado de datos personales o contra su pérdida accidental, destrucción o daño.
d) La información proporcionada por los usuarios a la TSA se protege completamente de su divulgación a menos que se tenga un acuerdo al respecto o por orden judicial o por cualquier otra exigencia legal.

Bajo la presente política se exige el cumplimiento de la normativa local sobre protección de datos personales existente en el Perú.

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

La TSA debe asegurarse que toda la información relevante concerniente a la operación de los servicios de sellado de tiempo se registra por un periodo especificado de tiempo, en particular para el propósito de proporcionar evidencia en procesos judiciales.

En particular:

General

a) Se debe documentar los eventos y datos específicos *(logs)* a ser registrados por la TSA.
b) La confidencialidad e integridad de registros actuales y archivados en relación con la operación de los servicios de sellado de tiempo debe preservarse.
c) Los registros concernientes a la operación de los servicios de sellado de tiempo deben archivarse completa y confidencialmente en concordancia con las prácticas de negocios divulgadas.
d) Los registros concernientes con la operación de los servicios de sellado de tiempo se deben poner a disposición si son requeridos para el propósito de ofrecer evidencia de su correcta operación en caso de requerirse en procesos judiciales.
e) El tiempo preciso de eventos significativos referidos al entorno, gestión de claves y sincronización del reloj de la TSA debe registrarse.
f) Los registros referidos a los servicios de sellado de tiempo deben mantenerse por un periodo de tiempo luego de la expiración de la validez de las llaves de firma de los TSUs conforme resulte apropiado para brindar evidencia en procesos judiciales y en conformidad con lo establecido en la declaración de prácticas de la TSA (ver numeral 7.1.2 Declaración de Libre Divulgación de la TSA).
g) Los eventos deben registrarse secuencialmente *(logs)* de manera que no pueden ser borrados o destruidos con facilidad (excepto si son transferidos a media de almacenamiento de datos de larga durabilidad) dentro del periodo de tiempo requerido para que se mantengan).

NOTA: Esto puede lograrse, por ejemplo, usando media de almacenamiento de datos que son solo de escritura, un registro de cada media de almacenamiento de datos en uso y mediante la utilización de respaldo de información fuera del sitio de operaciones.

h) Cualquier información registrada acerca de los suscriptores debe mantenerse confidencial excepto cuando exista un acuerdo con el suscriptor del servicio para su publicación.

Gestión de llaves de la TSU

i) Se debe llevar registro secuencial *(logs)* de todos los eventos relacionados con el ciclo de vida de las llaves de la TSU.
j) Se debe llevar registro secuencial *(logs)* de todos los eventos relacionados con el ciclo de vida de los certificados de la TSU (de ser apropiado).

Sincronización del reloj

k) Se debe llevar registro secuencial *(logs)* de todos los eventos relacionados con la sincronización del reloj de la TSU con el UTC. Esto incluye información concerniente a la recalibración o sincronización normal de los relojes usados para el sellado de tiempo.
l) Se debe llevar registro secuencial *(logs)* de todos los eventos relacionados con la detección de pérdida de sincronización.

7.5. Aspectos organizacionales

La TSA debe garantizar que su organización es confiable.
En particular, respecto a que:

a) Las políticas y procedimientos bajo los cuales opera la TSA no deben ser discriminatorios.
b) La TSA debe hacer sus servicios accesibles a todos los solicitantes cuyas actividades caen dentro de su campo declarado de operación y que acceden a cumplir con sus obligaciones conforme se encuentran especificadas en la declaración de prácticas de la TSA.
c) La TSA es operada por una persona jurídica en concordancia con las leyes del Perú.
d) La TSA tiene un sistema o sistemas de gestión de la calidad y de la seguridad de la información apropiados para los servicios de sellado de tiempo que brinda.
e) La TSA tiene arreglos adecuados para cubrir responsabilidades que surgen de sus operaciones y/o actividades.
f) Tiene la estabilidad financiera y los recursos requeridos para operar en conformidad con la presente política.

NOTA 1: Esto incluye los requisitos para la conclusión de la TSA identificados en el numeral 7.4.9 Terminación de la TSA.

g) Emplea el personal suficiente con la necesaria educación, entrenamiento, conocimiento técnico y experiencia en relación al tipo, alcance y volumen de trabajo requeridos para brindar servicios de sellado de tiempo.

NOTA 2: El personal empleado por una TSA incluye personas naturales contratadas para llevar a cabo funciones para el desarrollo de los servicios de sellado de tiempo. Aquel personal que se dedique solo al monitoreo de servicios de la TSA no necesita ser personal propio de la TSA.

h) Tiene políticas y procedimientos para la resolución de reclamos y disputas recibidas de clientes u otras partes sobre la prestación de los servicios de sellado de tiempo o cualesquiera otras materias relacionadas.
i) Tiene apropiadamente documentados acuerdos vigentes y contratos en ejecución por los que la prestación de servicios involucra la subcontratación, tercerización u otros arreglos con terceras partes.

8. CONSIDERACIONES DE SEGURIDAD

Al verificar sellos de tiempo es necesario para el verificador asegurarse que el certificado de la TSU es confiable y no se encuentra cancelado. Esto quiere decir que la seguridad de la TSU depende de la seguridad de la entidad de certificación que emitió su certificado digital tanto en lo referido a su emisión propiamente dicha como a la provisión de información precisa sobre su estado de cancelación.

Cuando un sello de tiempo es verificado como válido en un instante de tiempo dado, esto no quiere decir que permanecerá válido en el futuro. Cada vez que se verifica un sello de tiempo dentro del periodo de validez del certificado de la TSU, debe verificarse nuevamente contra la información actualizada del estado de cancelación, dado que en caso de compromiso de la llave privada de la TSU, todos los sellos de tiempo generados por la ésta quedan invalidados. El Anexo D de la norma EN 319 421 brinda información sobre la verificación de sellos de tiempo a largo plazo.

Al utilizar sellos de tiempo dentro de aplicaciones, se requiere también tener en cuenta la seguridad de las mismas. En particular, al aplicar sellos de tiempo es necesario asegurarse que se mantiene la integridad de los datos antes de la aplicación del sello de tiempo. El solicitante debería asegurarse que el valor del resumen (hash) incorporado en el sello de tiempo realmente corresponda con el hash de los datos.

9. BIBLIOGRAFÍA Y REFERENCIAS

[Ley Nº 27269]	Ley de Firmas y Certificados Digitales de 26 de mayo de 2000
[Reg. Ley Nº 27269]	Reglamento aprobado por Decreto Supremo Nº 052-2008-PCM de 18 de julio de 2008 y sus modificatorias
[Guía PSVA]	"Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", Versión 4.0, Rev. 2016
[RFC 3161]	Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001
[RFC 2119]	Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
[TF.460-5]	ITU-R Recommendation TF.460-5 (1997): Standard-frequency and time-signal emissions
[TF.536-1]	ITU-R Recommendation TF.536-1 (1998): Time-scale notations
[FIPS 140-2]	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
[ISO 15408]	ISO/IEC 15408 (1999) (parts 1 a 3): Information technology - Security techniques and Evaluation criteria for IT security
[Dir 95/46/EC]	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[Dir 99/93/EC]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
[ISO/IEC 27002]	ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls
[RFC 3161]	Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001
[X.208]	CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988
[EN 319 421]	ETSI EN 319 421 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (descarga gratuita en http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/).
[EN 319 422]	ETSI EN 319 422 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (descarga gratuita en http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/).
[EN 319 401]	ETSI EN 319 401 V2.1.1 (2016-02). Electronic Signatures and

Infrastructures (ESI); General Policy Requirements for Trust Service Providers (descarga gratuita en http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/).

[eIDAS] Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (descarga gratuita en http://data.europa.eu/eli/reg/2014/910/oj).

[AdES] ETSI EN 319 102-1 V1.1.1 (2016-05). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation (descarga gratuita en http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/).

[CAdES] ETSI EN 319 122-1 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures (descarga gratuita en http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/).

CEN/TS 419221-1:2016. Protection Profiles for TSP cryptographic modules - Part 1: Overview.

CEN/TS 419221-2:2016. Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup.

CEN/TS 419221-3:2016. Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services.

CEN/TS 419221-4:2016. Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup.

CEN/TS 419261:2015. Security requirements for trustworthy systems managing certificates and time-stamps

Anexo 1

A. Acrónimos

- **AAC:** Autoridad Administrativa Competente
- **OID:** Identificador de Objeto
- **PSVA:** Prestador de Servicios de Valor Añadido
- **PSVAEP:** Prestador de Servicios de Valor Añadido para el Estado Peruano
- **TI:** Tecnologías de la Información
- **TSA:** Autoridad de Sellado de Tiempo
- **TSS:** Servicio de Sellado de tiempo
- **TSU:** Unidad de Sellado de tiempo
- **UTC:** Tiempo Universal Coordinado
- **VAPS:** Declaración de Prácticas de Valor Añadido

B. Definiciones

Para las siguientes definiciones, se ha tomado como referencia las 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.

Para los propósitos del presente documento, se presenta a continuación un listado de definiciones que toma como base aquellas incluidas en el RFC 3628 bajo una traducción propia:

- **Autoridad de Sellado de Tiempo.**- Del inglés *Time Stamping Authority* o TSA, es la autoridad que, según la norma EN 319 421, emite sellos de tiempo. En el caso de la IOFE, el servicio de sellado de tiempo es una variante de los servicios que puede brindar un Proveedor de Servicios de Valor Añadido debidamente acreditado por la Autoridad Administrativa Competente. Bajo la IOFE la TSA no es reconocida específicamente con esta denominación como una autoridad o entidad prestadora de servicios de certificación o como una entidad prestadora de servicios de confianza.
- **Declaración de la TSA para divulgación.-** Del inglés *TSA Disclosure Statement,* es un conjunto de declaraciones acerca de políticas y prácticas de una TSA que de manera particular requieren ser comunicadas con un mayor énfasis o difundirse a los suscriptores del servicio o partes que confían, por ejemplo para cumplir así con requisitos regulatorios.
- **Declaración de prácticas de la TSA.-** Declaración de las prácticas que una TSA emplea para la emisión de sellos de tiempo. En el caso de la IOFE, la denominación del documento equivalente sería la Declaración de Prácticas de Valor Añadido bajo la variante de servicios de sellado de tiempo.
- **Parte que confía o tercero que confía.-** Receptor de un sello de tiempo que confía en el mismo.
- **Política de sellado de tiempo.-** Conjunto de reglas identificadas que indican la aplicabilidad de un sello de tiempo a una comunidad particular y/o clase de aplicación con requisitos comunes de seguridad.
- **Sello de tiempo.-** Objeto de datos que vincula la representación de un dato a un momento en particular, estableciendo así evidencia de que este dato existió antes de dicho momento.
- **Sistema TSA.**- Conjunto de elementos de tecnologías de la información y componentes organizados para dar soporte a la provisión de servicios de sellado de tiempo.
- **Suscriptor del servicio.-** Entidad que requiere los servicios provistos por un Proveedor de Servicios de Valor Añadido bajo la modalidad de sellado de tiempo, TSA, la cual ha explícita o implícitamente aceptado los términos y condiciones para su prestación.
- **Unidad de sellado de tiempo.-** Del inglés *Time Stamping Unit* o TSU, es un conjunto de hardware y software gestionado como una unidad y que tiene una única clave de firma de sellos de tiempo activa en determinado momento.
- **UTC (k).-** Escala de tiempo producida por el laboratorio "k" en estricto acuerdo con UTC, con la meta de alcanzar una precisión de más o menos 100 ns (ver la Recomendación ITU-R TF.536-1). Una lista de los laboratorios UTC(k) se da en la sección 1 de la Circular T distribuida por BIPM y disponible en su sitio WEB (http://www.bipm.org/).
- **Tiempo Universal Coordinado.-** Abreviado UTC, es una escala de tiempo basada en el segundo según se define en la Recomendación ITU-R TF.460-5.