SERVICIO DE VALOR AÑADIDO
AUTORIDAD DE SELLADO DE TIEMPO
CLIENTE DEDICADO SUNAT

POLÍTICA DE SELLADO DE TIEMPO
Y
DECLARACIÓN DE PRÁCTICAS DE SELLADO DE TIEMPO

PST - DPST

SGTSA.1-PO-01

Versión 1.1

Contenido

1. INTRODUCCIÓN 5

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

1.1. VISIÓN GENERAL 5
1.2. PRINCIPIO DEL SERVICIO DE SELLADO DE TIEMPO DE SOFTNET 6
1.3. IDENTIFICACIÓN DE DOCUMENTO 6
1.4. PARTICIPANTES DEL SERVICIO DE SELLADO DE TIEMPO 7
1.4.1. Autoridades de certificación 7
1.4.2. Autoridades de sellado de tiempo 7
1.4.3. Suscriptores 8
1.4.4. TERCEROS qUE CONFÍAN 8
1.4.5. Otros participantes 8
1.5. ADMINISTRACIÓN DE LA POLÍTICA 8
1.5.1. Organización que administra el documento. 8
1.5.2. Persona de contacto 8
1.6. DEFINICIONES Y ACRÓNIMOS 9
2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO 10
2.1. REPOSITORIOS 10
2.2. PUBLICACIÓN DE INFORMACIÓN 10
2.3. HORA O FRECUENCIA DE PUBLICACIÓN 10
2.4. CONTROLES DE ACCESO EN REPOSITORIOS 11
3. DISPOSICIONES GENERALES 11
3.1. OBLIGACIONES DE LA TSA 11
3.2. OBLIGACIONES DEL SUSCRIPTOR 11
3.3. OBLIGACIONES DE LA PARTE QUE CONFÍA 11
3.4. OBLIGACIONES DE LAS AC QUE PROPORCIONAN LOS CERTIFICADOS TSU 12
3.5. DECLARACIÓN DE PRÁCTICA DE SELLADO DE TIEMPO (DPST) 12
3.6. TÉRMINOS DE USO (TOU) 12
3.7. CONFORMIDAD CON LOS REQUISITOS LEGALES 13
3.7.1. Ley aplicable 13
3.7.2. Solución de litigios 13
3.7.3. Propiedad intelectual de las infraestructuras DE SOFTNET 13
3.7.4. Información personal 13
3.8. ENMIENDAS 14
3.8.1. Procedimiento de enmienda 14
3.8.2. Mecanismos de notificación y periodo 14
3.8.3. Circunstancias bajo las cuales se debe cambiar el OID 14
4. REQUISITOS OPERACIONALES 14
4.1. GESTIÓN DE LAS SOLICITUDES TST 14
4.2. REGISTRO DE AUDITORÍA 14
4.3. GESTIÓN DEL CICLO DE VIDA DE CLAVE PRIVADA 15
4.4. SINCRONIZACIÓN DE RELOJ 15
4.5. TOKEN DE SELLO DE TIEMPO (TST) 16
4.5.1. Contenido de un TST 16
4.5.2. Firma TST 16
4.6. COMPROMISO DE LA TSA 16
4.6.1. Plan de recuperación en un desastre 16
4.6.2. Comunicación 17
4.6.3. Interrupción de la generación de TST 17
4.6.4. Información sobre la validez de TST 17
4.6.5. Alerta 17
4.7. TÉRMINO DE LA TSA 17
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS. 18
5.1. CONTROLES FÍSICOS 18
5.1.1. Ubicación del sitio y construcción 18
5.1.2. Acceso físico 18

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

5.1.3. Energía y aire acondicionado. 19
5.1.4. Exposiciones al agua 19
5.1.5. Prevención y protección contra incendios. 19
5.1.6. Almacén de datos 19
5.1.7. Deposito de basura 19
5.1.8. Copia de seguridad fuera del sitio 19
5.2. CONTROLES DE PROCEDIMIENTO 19
5.2.1. Roles confiables 19
5.2.2. Número de personas requeridas por tarea 20
5.2.3. Identificación y autenticación para cada rol. 20
5.2.4. Roles que requieren separación de funciones 20
5.2.5. Análisis de riesgos. 20
5.2.6. Sistema de gestión de acceso 20
5.2.7. Gestión de operaciones 21
5.2.8. mplementación y mantenimiento de sistemas confiables 22
5.2.9. Informe de incidentes y respuesta 22
5.3. CONTROLES DE PERSONAL 23
5.3.1. Requisitos de calificación, experiencia y autorización 23
5.3.2. Procedimientos de verificación de antecedentes 23
5.3.3. Requisitos de entrenamiento 23
5.3.4. Frecuencia de reentrenamiento y requisitos 23
5.3.5. Frecuencia y secuencia de rotación laboral 23
5.3.6. Sanciones por acciones no autorizadas. 24
5.3.7. Requisitos de contratista independiente 24
5.3.8. Documentación entregada al personal 24
6. CONTROLES TÉCNICOS DE SEGURIDAD. 24
6.1. PRECISIÓN DE TIEMPO 24
6.2. GENERACIÓN DE LA CLAVE 24
6.3. CERTIFICACIÓN DE CLAVES TSU 24
6.4. PROTECCIÓN DE CLAVES PRIVADAS DE TSU 25
6.5. COPIA DE SEGURIDAD DE CLAVES PRIVADAS DE TSU 25
6.6. DESTRUCCIÓN DE CLAVES PRIVADAS DE TSU 25
6.7. ALGORITMOS OBLIGATORIOS 25
6.8. VERIFICACIÓN TST 25
6.9. PERIODO DE VALIDEZ DE LOS CERTIFICADOS TSU 25
6.10. PERÍODO DE USO DE CLAVES PRIVADAS DE TSU 25
7. CERTIFICADO Y PERFILES TST 26
7.1. PERFIL DE CERTIFICADO 26
7.2. PERFIL TST 27
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 27
8.1. FRECUENCIA O CIRCUNSTANCIAS DE LA EVALUACIÓN. 27
8.2. IDENTIDAD / CALIFICACIONES DEL EVALUADOR 27
8.3. RELACIÓN DEL ASESOR CON LA ENTIDAD EVALUADA 28
8.4. TEMAS CUBIERTOS POR LA EVALUACIÓN 28
8.5. ACCIONES TOMADAS COMO RESULTADO DE DEFICIENCIA 28
8.6. COMUNICACIÓN DE RESULTADOS. 28
9. OTROS ASUNTOS LEGALES Y COMERCIALES 28
9.1. RESPONSABILIDADES. 28
9.2. POLÍTICA DE REEMBOLSO. 29
9.3. COBERTURA DEL SEGURO. 29
9.4. AVISOS INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES. 29
10. CONFORMIDAD 29
HISTORIAL DE CAMBIOS 30

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

1. INTRODUCCIÓN

SOFT & NET SOLUTIONS S.A.C., en adelante SOFTNET, es una empresa peruana fundada en el 2007, dedicada a proveer soluciones integrales en alta tecnología con preponderancia en identidad digital, automatización de procesos, facturación electrónica y gestión de proyectos. Como parte de sus planes de expansión en la prestación de servicios, en el año 2023 se constituye como Entidad de Certificación y como Autoridad de Sellado de Tiempo, con lo cual es de las pocas empresas peruanas en brindar todas las variedades de productos y servicios que homologa INDECOPI a través de sus diversos procedimientos de acreditación dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE)

Como Autoridad de Sellado de Tiempo - TSA, SOFTNET provee los servicios de emisión de sellado de tiempo, utilizando una infraestructura periódicamente auditada, propia y a Clientes Dedicados en este caso especifico para SUNAT, cumpliendo con los requisitos y controles de la certificación ISO 27001.

1.1. Visión general

SOFTNET, siendo una Autoridad de Sellado de Tiempo (TSA), ofrece a sus clientes un Servicio de Sellado de Tiempo (SST) a través de una solución PKI proporcionada por **CAMERFIRMA**, proveedor de servicios de certificación y de sellado de tiempo. Los componentes de dicha solución se encuentran instalados en equipos de propiedad de SOFTNET en el centro de datos de **CenturyLink en Santiago de Surco y en contingencia en su sede de San Isidro en Lima, Perú.** La administración del software de sellado de tiempo de **CAMERFIRMA** que emplea SOFTNET, es verificada anualmente por auditores autorizados conforme a eIDAS y estándares ETSI.

El presente documento desarrolla la Política de sellado de tiempo de SOFTNET (PST). Describe el SST de SOFTNET y especifica los compromisos de SOFTNET como TSA con respecto a este servicio de sellado de tiempo. El presente documento también describe las obligaciones y requisitos de los suscriptores y las partes que confían.

Un token de sello de tiempo (TST) generado por el SST de SOFTNET proporciona evidencia de la existencia de un valor hash en una fecha y hora determinadas. Los TST son generados y firmados digitalmente por la TSA mediante el uso de Unidades de Sellado de Tiempo (TSU).

Este documento tiene como objetivo especificar los compromisos de SOFTNET cuando, actuando como TSA, entrega y gestiona TST, así como las obligaciones de otros participantes.

Este documento también incluye la Declaración de práctica de sellado de tiempo (DPST) de SOFTNET, la cual presenta los mecanismos y procedimientos implementados para alcanzar el objetivo de seguridad de la PST y, en particular, el proceso que debe seguir una TSU al generar TST y mantener la precisión de la hora de sus sistemas a partir de la sincronización con el CAMERFIRMA Time Server. SOFTNET que actúa como TSA puede configurar varias TSU para administrar su SST.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

La Entidad de Certificación (EC) que emite los certificados para las TSU de la TSA también pertenece a SOFTNET. Sus especificaciones se describen en la Política de certificación y la Declaración de práctica de certificación (PC y DPC) de la EC de SOFTNET.

Esta PST y DPST no exige de ningún vínculo entre el hash a ser provisto de sello de tiempo y el contenido de los datos electrónicos originales. Sólo el suscriptor del SST de SOFTNET es responsable de esta coincidencia.

SOFTNET también ha publicado los Términos de uso para los suscriptores de su SST.

Dentro de este PST y DPST, el día y la hora de cada TST se sincronizan con la hora universal coordinada (UTC) con una precisión de menos de un segundo. Este TSP aplica el formato TST estándar especificado en el documento [RFC 3161].

1.2. Principio del servicio de sellado de tiempo DE SOFTNET

El SST establece evidencia de que existe un dato en un momento particular. De esta manera, une una representación inequívoca de un dato (es decir: su valor hash junto con un identificador de algoritmo hash) a un tiempo particular. Un TST realiza inequívocamente este enlace; un TST es una estructura firmada que incluye en particular:

- el valor hash y el algoritmo hash del dato con marca de tiempo; fecha y hora universal (UTC);
- el identificador del certificado TSU que ha generado el TST;
- el identificador de SOFTNET que actúa como TSA (dentro del certificado de sello de tiempo);
- el identificador de la EC que ha firmado las claves privadas instaladas en las TSU.

El SST de SOFTNET aprovecha la Infraestructura de clave pública (PKI) de su EC, la misma que es proporcionada por **AC CAMERFIRMA**, como su proveedor de servicios de certificación.

Este servicio de certificación permite a la EC de SOFTNET emitir los certificados para sus TSU así como para las TSU de otras entidades que requieran implementar una TSA bajo la jerarquía de la EC de SOFTNET.

El sistema de sincronización de reloj del SST de SOFTNET, el cual es proporcioando por **CAMERFIRMA** a través del Servidor de Tiempo, le permite garantizar al suscriptor la entrega de un TST con una precisión de menos de un segundo con respecto a UTC.

La TSA de SOFTNET opera actualmente una TSU, y mediante el presente deja constancia de un Cliente Dedicado SUNAT,. Cada TSU firma el TST en nombre de la TSA, utilizando una clave privada dedicada, cuya clave pública correspondiente ha sido previamente certificada por la EC y ER de SOFTNET. Por lo tanto, cada TSU que opere SOFTNET tiene su propio certificado de sellado de tiempo.

1.3. Identificación de documento

Este documento corresponde a la Política de sellado de tiempo y Declaración de práctica de sellado de tiempo (PST y DPST) de SOFTNET, el cual declara cumplir con los lineamientos del

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

CAMERFIRMA Time-Stamping Policy (TSP) and Time Stamping Practice Statement (TSPS), por tratarse de su proveedor de servicios de certificación y sellado de tiempo. Este TSP / TSPS se identifica, dentro del marco de documentación de la arquitectura de confianza, por un número de identificación único: _____

Este OID se construye de la siguiente manera:

OID	Descripción
1.3.6.1.4.1.17326	Entidad de Certificación
1.3.6.1.4.1.17326.10.2.1.0.1	Política de Camerfirma
1.3.6.1.4.1.17326.10.13.1.3.1	Política de Sello

Los TST que cumplen con esta política se refieren a ella mediante el uso de este identificador único (OID). Su valor se incluye en el campo "Política" de los TST. Otros elementos más significativos (nombre, número de versión, fecha de actualización) también pueden identificarlo.

OID de política TST predeterminado: 1.3.6.1.4.1.17326.10.13.1.3.1

OID de política TST personalizado: _____

(X indica el número secuencial para OID de políticas personalizadas).

1.4. Participantes del servicio de sellado de tiempo

1.4.1. Autoridades de certificación

Dentro de un SST, los certificados de TSU son suministrados por una EC acreditada. Estos certificados permiten a las Partes confiantes identificar la TSA.

1.4.2. Autoridades de sellado de tiempo

Una autoridad de sellado de tiempo y un proveedor de servicios de sellado de tiempo son dos nociones que se unen naturalmente.

El Proveedor de servicios de sellado de tiempo (PSST) es una persona o entidad responsable de operar el Servicio de sellado de tiempo (SST), esto es, para administrar / generar Tokens de sello de tiempo (TST), para gestionar las solicitudes de los Suscriptores y cumplir los requisitos de las partes confiantes.

- El PSST incluye al menos una TSA pero podría tener varias dependiendo de su organización. Los certificados de TSU identificarán el TSSP y la TSA correspondiente.
- **CAMERFIRMA** como PSST de SOFTNET, administra la TSA a cargo del SST de SOFTNET, que tiene una o más TSU, con al menos una Política / Identificador de Política (OID).
- La TSA de SOFTNET funciona bajo la responsabilidad de su PSST.

La TSA es administrada por la Autoridad de Política **CAMERFIRMA**. La Autoridad de Política está compuesta por representantes de la gerencia ejecutiva, operaciones PKI y legales.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

El Responsable de la TSA de SOFTNET aprueba la PST y los documentos relacionados con el SST proporcionados por SOFTNET. El Responsable de la TSA tiene la autoridad final y la responsabilidad de:

- especificar y aprobar la infraestructura y las prácticas del SST;
- aprobar este documento;
- garantizar la aplicación persistente de la PST y DPST establecido por la TSA en el ámbito de los requisitos funcionales, organizativos y técnicos;
- asegurar la aplicación persistente del cumplimiento de la implementación de TSU con el PSST;
- publicar la PST y DPST y los Términos de uso, y sus revisiones a los suscriptores y partes confiantes a través del sitio web.

1.4.3. Suscriptores

Un suscriptor es una entidad que requiere los servicios prestados por la TSA y que ha aceptado sus términos de uso.

1.4.4. Terceros que Confian

Un tercero o una parte que Confía es una persona o entidad que actúa confiando en un TST generado bajo esta política por la TSA de SOFTNET. Una Parte que confía puede, o no ser, también un Suscriptor.

1.4.5. Otros participantes

No aplica.

1.5. Administración de la política

1.5.1. Organización que administra el documento.

SOFT & NET SOLUTIONS S.A.C

Calle Germán Schreiber 184, Of. 802, San Isidro, Lima, Perú

Teléfono: +511 421 2777

Correo electrónico: informes@soft-net.com.pe

Sitio web: www.soft-net.com.pe

1.5.2. Persona de contacto

Nombre: Leonel José García Jáuregui

Cargo: Director Comercial y de Negocios

Dirección de correo electrónico: lgarcia@soft-net.com.pe

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

1.6. Definiciones y acrónimos

Definiciones

Auditor

Persona encargada de auditar los eventos del SST.

Lista de revocación de certificados (CRL)

La Lista de revocación de certificados es una lista, firmada digitalmente por la EC, que contiene todos los identificadores de los certificados que han sido revocados antes de su fecha de vencimiento.

Valor de hash

Resultado de una función hash que caracteriza un dato; es una cadena de bits con una longitud fija para una función hash específica (por ejemplo, 256 bits para SHA-256).

Proveedor de alojamiento

Entidad que aloja la plataforma técnica del servicio en un entorno seguro y con acceso a la red de alta disponibilidad.

Servicio de sellado de tiempo (SST)

Conjunto de operaciones necesarias para realizar la generación y gestión de TST.

Sistema de sellado de tiempo

Conjunto compuesto por todas las TSU junto con los componentes de administración y supervisión utilizados para proporcionar el SST.

Token de sello de tiempo (TST)

Objeto de datos que une una representación de un dato a un tiempo particular, expresado en tiempo universal (UTC), estableciendo así evidencia de que el dato existía en ese momento.

Unidad de sellado de tiempo (UST o TSU, por sus siglas en inglés)

Conjunto de hardware y software utilizado para crear un TST, caracterizado por un identificador de la Unidad de Sellado de Tiempo certificado por una EC, y que tiene una clave de firma TST designada.

Acrónimo	Descripción
DPST	Declaración de Prácticas de Sellado de Tiempo
EC	Entidad de Certificación
CRL	Certificate Revocation List
NTP	Network Time Protocol

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

Acrónimo	Descripción
OID	Object Identifier
PST	Política de Sellado de Tiempo
PSST	Proveedor de Servicio de Sellado de Tiempo
SST	Servicio de Sellado de Tiempo
ToU	Términos de Uso
TSA	Time-Stamping Authority
TSP	Time-Stamping Policy
TSPS	Time-Stamping Practice Statement
TSS	Time-Stamping Service
TSSP	Time-Stamping Service Provider
TST	Time-Stamp Token / Token de Sello de Tiempo
TSU	Time-Stamping Unit

2. Responsabilidades de publicación y repositorio

2.1. Repositorios

SOFTNET, como TSA, pone a disposición de las partes que confían esta PST y DPST. Este documento está disponible en Internet, en el sitio web de SOFTNET.

www.soft-net.com.pe/

2.2. Publicación de información.

La información publicada es la siguiente:

- este TSP / TSPS;
- los Términos de uso correspondientes;
- los certificados de las TSU.

2.3. Hora o frecuencia de publicación

Se publicará una nueva PST y DPST cuando haya una nueva versión principal aprobada.

Los certificados TSU se publican como máximo 24 horas después de su generación y necesariamente antes de su uso efectivo.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

GERENCIA GENERAL SOFT&NET SOLUTIONS S.A.C.

2.4. Controles de acceso en repositorios

La información publicada está disponible en el sitio web de SOFTNET y cualquier persona puede leerla libremente. La PST y los Términos de uso son de fácil acceso para cualquiera que desee una copia de ellos en el sitio web de SOFTNET.

Las adiciones, la eliminación y las modificaciones de esta información se limitan al personal autorizado de SOFTNET, a través del control de acceso.

3. Disposiciones generales

3.1. Obligaciones de la TSA

- SOFTNET debe cumplir con los requisitos y los procedimientos definidos en esta PST y DPST.
- SOFTNET debe cumplir con cualquier obligación adicional indicada en el TST de manera directa o incorporada por referencia.
- SOFTNET debe suministrar un SST de acuerdo con su PST y DPST.
- SOFTNET debe cumplir con todos sus compromisos de conformidad con sus Términos de uso.
- SOFTNET debe garantizar la emisión técnica de los TST.
- SOFTNET debe garantizar que se aplique su PST y DPST y que se cumplan los requisitos especificados en el presente documento.

3.2. Obligaciones del suscriptor

El suscriptor debe aceptar y cumplir con los Términos de uso del SST de SOFTNET.

El suscriptor también debe verificar que el certificado de la TSU que entrega un TST sea válido cuando se realiza la solicitud de sello de tiempo.

3.3. Obligaciones de la Parte QUE CONFÍA

La Parte que confía debe verificar que el TST se haya firmado correctamente y que el certificado TSU correspondiente no esté revocado en el momento de la verificación, utilizando las CRL publicadas por la EC de SOFTNET.

La Parte que confía también debe verificar que las solicitudes de TST sean emitidas realmente por una TSU de SOFTNET. Para hacerlo, la Parte que confía debe verificar que el TST incluye una referencia a una TSU de SOFTNET.

Finalmente, la Parte que confía debe tener en cuenta las limitaciones de uso de TST descritas en este documento y los Términos de uso correspondientes.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

3.4. Obligaciones de las AC que proporcionan los certificados TSU

Los certificados TSU deben ser emitidos por una EC que haya sido calificada de acuerdo con la Política de certificados de SOFTNET. Los certificados TSU no se emitirán directamente bajo la EC raíz o una intermedia que firme EC subordinadas.

3.5. Declaración de práctica de sellado de tiempo (DPST)

SOFTNET asegura que tiene la confiabilidad necesaria para proporcionar un SST y describe dentro de este documento, cómo se implementa este SST. Este documento garantiza que:

1. SOFTNET y CAMERFIRMA, esta última como su proveedor de servicios de certificación digital y sellado de tiempo, llevan a cabo una evaluación de riesgos para evaluar los activos comerciales y las amenazas a esos activos con el fin de determinar los controles y procedimientos operativos necesarios;
2. SOFTNET tiene una declaración de prácticas y procedimientos utilizados para abordar todos los requisitos identificados en el presente documento;
3. La PST y DPST identifica las obligaciones y los requisitos de implementación que deben cumplir la TSA, los Socios, los Suscriptores y la Parte dependiente, en el ámbito de SST de SOFTNET;
4. SOFTNET proporciona a los suscriptores y partes que confían la parte pública de su PST y DPST (incluyéndolo en sus Términos de uso) para que puedan evaluar su conformidad con este documento.
5. SOFTNET implementa una organización relevante para la aprobación de su PST y DPST, y la verificación de conformidad entre esta declaración y esta PST y DPST;
6. La TSA asegura que las prácticas se implementen adecuadamente;
7. SOFTNET define un procedimiento de control periódico **propio y con alcance a sus Clientes Dedicados** para verificar que sus prácticas cumplan con su PST y DPST;
8. SOFTNET tiene como objetivo la certificación del cumplimiento de la presente PST y DPST entregado por un organismo de certificación independiente (INDECOPI).

Posteriormente, cualquier enmienda iniciada por SOFTNET y que pueda afectar el cumplimiento de su PST y DPST será nuevamente sometida a la opinión de un organismo de certificación independiente (INDECOPI).

3.6. Términos de uso (ToU)

SOFTNET proporciona sus ToU a sus suscriptores. Los suscriptores deben respetar las cláusulas contenidas en estos ToU.

Estos ToU son públicos y están disponibles en el sitio web de SOFTNET.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

3.7. Conformidad con los requisitos legales

3.7.1. Ley aplicable

La TSA será utilizada por los suscriptores y las partes confiantes de acuerdo con las leyes y reglamentos de la jurisdicción en la que se utilizan o se basan. La ley aplicable a los efectos de este documento será la Ley de Perú, que sustituirá en caso de contradicciones.

A fin de obtener el reconocimiento legal de sus sellos de tiempo, SOFTNET, como Autoridad de sellado de tiempo, cumple los requerimientos establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales -Ley27269.

3.7.2. Solución de litigios

En caso de litigio entre las partes como resultado de la interpretación, la aplicación y / o la ejecución del contrato, y en ausencia de un acuerdo mutuo entre las partes antes mencionadas, la única jurisdicción competente es Perú.

3.7.3. Propiedad intelectual de las infraestructuras DE SOFTNET

En cuanto a la propiedad intelectual, los productos operados para proporcionar el SST pertenecen a **CAMERFIRMA**.

Los suscriptores o partes que confían de estos servicios no tienen derechos de propiedad intelectual sobre estos diversos elementos. Cualquier uso o reproducción, total o parcial, de estos elementos y / o información dentro de, por cualquier medio, está estrictamente prohibido y es una falsificación punible bajo la legislación relativa a la propiedad intelectual, a menos que CAMERFIRMA, o SOFTNET en su representación, haya dado previamente su consentimiento por escrito para dicho uso o reproducción.

3.7.4. Información personal

Los certificados emitidos bajo la EC de SOFTNET serán utilizados por los suscriptores y las partes confiantes solo de acuerdo con las leyes y regulaciones de la jurisdicción en la que se usan o se basan, de acuerdo con las definiciones hechas en la sección 3.7.1 anterior. Se informa a los suscriptores que los datos personales que proporcionan pueden ser transferidos y procesados por SOFTNET y sus socios involucrados en los intercambios dados, de conformidad con la PC y DPC de SOFTNET.

Los suscriptores son informados de que tienen derecho a acceder, corregir y eliminar los datos que les conciernen contactando a SOFTNET.

En particular, no tienen derecho a recopilar o utilizar de manera inapropiada los datos personales a los que acceden y, en general, a actuar de una manera que pueda ser perjudicial para la vida privada o la reputación personal.

SOFTNET está obligado a mantener la confidencialidad de la información provista por los Suscriptores, a menos que el Suscriptor permita su divulgación o lo exija la regulación o la adjudicación.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

3.8. Enmiendas

3.8.1. Procedimiento de enmienda

SOFTNET es responsable, a través del Responsable de la TSA de SOFTNET, de la creación, la aprobación, el mantenimiento y las modificaciones de la actual PST y DPST.

Cuando el Responsable de la TSA de SOFTNET aprueba una nueva versión del presente documento, y luego de su aprobación por la Autoridad Administrativa Competente (INDECOPI), se publicará en el sitio web de SOFTNET y reemplazará los términos de la versión anterior.

3.8.2. Mecanismos de notificación y periodo

La nueva versión de la PST y DPST se notifica a través de su publicación en el sitio web de CAMERFIRMA de tal manera que este disponible para todos los suscriptores y partes confiantes del SST de SOFTNET.

A menos que se indique lo contrario, la nueva versión de la PST y DPST entrará en vigencia inmediatamente después de su publicación y permanecerá vigente hasta que entre en vigencia una nueva versión.

3.8.3. Circunstancias bajo las cuales se debe cambiar el OID

Si el Responsable de la TSA de SOFTNET determina que es necesario un cambio de OID, la nueva versión indicará el nuevo OID.

El Responsable de la TSA de SOFTNET sigue siendo el único juez que determina si es necesario un cambio de OID.

4. Requisitos operacionales

4.1. Gestión de las solicitudes TST

SOFTNET proporciona un servicio para la gestión de las solicitudes TST. Las condiciones específicas de este servicio se describen en los ToU aceptados por los suscriptores.

4.2. Registro de auditoría

A menos que se mencione lo contrario, SOFTNET asegura que toda la información apropiada con respecto a la operación de su SST se mantenga siete (7) años después de que la TSU correspondiente se haya dado de baja, principalmente para proporcionar evidencia en caso de investigación legal.

Los registros de auditoría cubren eventos relacionados con:

- generación de TST;
- administración del SST: gestión de contexto, importación de certificados, estado del servicio;
- operación y sincronización del reloj interno;
- ciclo de vida de las claves del TSU;

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

- ciclo de vida del certificado de TSU;
- cualquier tipo de evento que pueda afectar la operación de la TSU.

Cada registro de auditoría contiene una fecha y hora precisas del evento.

La confidencialidad del registro de auditoría se garantiza mediante una gestión adecuada del acceso físico, del sistema y de la red. La integridad está garantizada criptográficamente.

La gestión de estos registros cumple con la gestión de la información clasificada de CAMERFIRMA, como el proveedor de servicios de certificación digital y sellado de tiempo de SOFTNET.

4.3. Gestión del ciclo de vida de clave privada

SOFTNET asegura que las claves de firma privadas de la TSU no se usen después del final de su ciclo de vida.

La TSU destruye la clave privada cuando se alcanza el período de uso de la clave. Las claves TSU no se renuevan.

SOFTNET asegura que el número de TSU en funcionamiento en un momento dado es suficiente para proporcionar un servicio confiable.

4.4. Sincronización de reloj

SOFTNET, a través de su proveedor CAMERFIRMA, asegura que sus relojes estén sincronizados con la hora universal (UTC) con la precisión declarada de un segundo.

Más específicamente:

1. la calibración de la TSU se mantiene de modo que no se espere que los relojes se desvíen de la precisión declarada;
2. los relojes de la TSU están protegidos contra las amenazas relacionadas con su entorno que podrían conducir a una desincronización con respecto al tiempo UTC fuera de la precisión declarada;
3. SOFTNET asegura que su proveedor CAMERFIRMA puede detectar una desviación del reloj interno de la TSU cuando sale de los límites de la precisión declarada;
4. si el reloj de una de las TSU se detecta fuera de la precisión declarada, los TST ya no se generarán hasta que se corrija;
5. SOFTNET asegura, mediante su proveedor CAMERFIRMA, que la sincronización del reloj se mantiene cuando se produzca un segundo intercalado (leap second) cuando sea notificado por el organismo apropiado. El cambio para tener en cuenta el segundo intercalar se producirá durante el último minuto del día en que está programado que ocurra el segundo intercalar. Cuando se produce este cambio, se realiza un registro del tiempo exacto (dentro de la precisión declarada).

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

4.5. Token de sello de tiempo (TST)

SOFTNET asegura que los TST se generan de forma segura e incluyen la hora correcta.

4.5.1. Contenido de un TST

En respuesta a una solicitud de Suscriptor, SOFTNET proporciona un TST que cumple con RFC 3161, que contiene los campos según el perfil de TST provisto en la Sección 7.2.

4.5.2. Firma TST

Las firmas se basan en los algoritmos de la clave (definidos en la Sección 6.7).

Todos los algoritmos de firma se utilizan junto con el algoritmo hash SHA-256 o un algoritmo hash que es igualmente o más resistente a un ataque de colisión.

4.6. Compromiso de la TSA

En el caso de eventos que afecten la seguridad del SST y que puedan afectar los TST generados, SOFTNET garantiza que se proporcione la adecuada información a los suscriptores y partes que confían.

El compromiso de la TSA podría ser causado por:

- el compromiso de las claves privadas de TSU;
- el compromiso de la clave privada de la EC de SOFTNET utilizada para generar los certificados TSU;
- un problema operacional.

SOFTNET ha tenido en cuenta en su Plan de recuperación ante desastres el posible compromiso de su SST.

4.6.1. Plan de recuperación en un desastre

El Plan de recuperación ante desastres aborda el compromiso de la clave de firma privada de TSU, ya sea real o sospechosa, o la pérdida de calibración de un reloj de TSU, lo que podría afectar los TST emitidos.

SOFTNET garantiza que se hayan tomado todas las medidas necesarias para evitar incidentes operativos.

El proveedor de servicios de certificación digital y sellado de tiempo de SOFTNET, CAMERFIRMA, y SOFTNET, en lo que le atañe, actualizan constantemente su Plan de recuperación de desastres para cubrir y garantizar el mejor servicio posible contra las siguientes amenazas:

- compromiso de clave privada; fallas de red;
- indisponibilidad de personal calificado;
- problemas con la calibración del reloj;
- falla de los componentes de hardware.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

GERENCIA GENERAL SOFT&NET SOLUTIONS S.A.C.

En términos más generales, los incidentes en el SST se manejarán de acuerdo con el procedimiento de gestión de incidentes vigente en CAMERFIRMA y SOFTNET.

4.6.2. Comunicación

En caso de un compromiso, real o sospechoso, o la pérdida de calibración de una TSU, que podría afectar los TST generados, SOFTNET notificará los detalles a través de su sitio web.

4.6.3. Interrupción de la generación de TST

En caso de un compromiso, real o sospechado, o la pérdida de calibración de una TSU, que podría afectar los TST generados, SOFTNET toma todas las medidas necesarias para garantizar que esta TSU no genere más TST hasta que se tomen medidas para restaurar la situación.

4.6.4. Información sobre la validez de TST

En caso de un compromiso importante de la operación de SOFTNET o pérdida de calibración que pueda afectar los TST emitidos, siempre que sea posible, SOFTNET pondrá a disposición de todos los suscriptores y partes confiables información que pueda usarse para identificar el TST que pueda haber sido afectado, a menos que esto viole la seguridad del SST.

4.6.5. Alerta

En caso de compromiso, real o sospechoso, de su SST, SOFTNET notificará directamente y sin demora los datos de contacto proporcionados con SOFTNET.

4.7. TÉRMINO DE LA TSA

SOFTNET define los procedimientos para manejar el término de su TSA. A través de estos procedimientos, SOFTNET asegura que las interrupciones potenciales para los suscriptores y las partes que confían se minimicen en caso de que el SST cese su actividad. En particular, SOFTNET asegura que se proporcionará toda la información necesaria para verificar la exactitud de los TST, incluso después de la finalización de su SST.

Antes de la terminación de su SST, se realizarán los siguientes procedimientos:

- SOFTNET notificará a todos sus suscriptores y partes confiantes sobre la próxima terminación mediante la publicación de esta información en su sitio web;
- SOFTNET terminará la autorización de todos los subcontratistas para actuar en su nombre en el desempeño de cualquier función relacionada con el proceso de emisión de TST;
- SOFTNET transferirá las obligaciones a un "organismo confiable" (INDECOPI) para mantener registros de eventos y archivos de auditoría necesarios para demostrar su correcto funcionamiento durante un período razonable;
- SOFTNET mantendrá sus obligaciones de poner a disposición sus claves públicas o certificados a las partes que confían por un período razonable;
- las claves privadas de la TSU se destruirán para que no se puedan recuperar, de acuerdo con el procedimiento descrito en la sección 4.3.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

SOFTNET toma todas las medidas necesarias para cubrir los costos para cumplir con los requisitos mínimos en caso de quiebra o por otras razones por las que no pueda cubrir los costos por sí solo.

Las disposiciones hechas para la terminación del servicio incluyen:

- Notificación a suscriptores y partes que confían;
- Transferencia de obligaciones de SOFTNET a un organismo confiable identificado (INDECOPI), mencionado anteriormente.

5. Instalaciones, gestión y controles operativos.

5.1. Controles físicos

5.1.1. Ubicación del sitio y construcción

SOFTNET contrata el alojamiento de sus equipos en el centro de datos de CenturyLink en Lima, Perú.

5.1.2. Acceso físico

El acceso a las instalaciones del SST está estrictamente restringido al personal autorizado que figura en una lista de acceso. Estas autorizaciones son enviadas al proveedor de alojamiento de SOFTNET y se actualiza un libro de registro cada vez que se realiza el mantenimiento en el equipo del SST. Este libro de registro contendrá la siguiente información:

- la fecha y hora de la operación;
- el apellido y el nombre de las personas presentes; la descripción de la operación de mantenimiento;
- la fecha y hora del final de la operación; La firma de las personas presentes. Además, el acceso físico está restringido mediante la implementación de mecanismos para controlar el acceso a las zonas de alta seguridad del proveedor de alojamiento. Estos mecanismos implican que los administradores autorizados poseen tarjetas de acceso, llaves de acceso y/o reforzado por un lector biométrico.

Los perfiles de acceso a una zona son definidos y mantenidos por la TSA y transferidos al proveedor de alojamiento, CenturyLink.

Las áreas seguras de SOFTNET se auditan periódicamente para verificar que los sistemas de control de acceso estén siempre operativos y en funcionamiento. Los sistemas de monitoreo y registro se implementan en todos los sitios para todas las áreas seguras. Esto se refuerza con el hecho que el proveedor de alojamiento principal, cuenta con acreditaciones vigentes de las ISO 9001, 14001, BS OHSAS 18001, 20000-1 y 27001

Los controles de acceso se aplican a todas las zonas seguras.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

5.1.3. Energía y aire acondicionado.

Los controles de emergencia son operados por el proveedor de alojamiento para que la interrupción del suministro de energía o una falla en el aire acondicionado no ponga en peligro los compromisos de SOFTNET en términos de disponibilidad.

5.1.4. Exposiciones al agua

La especificación del perímetro de seguridad tiene en cuenta los riesgos relacionados con la exposición al agua. Los controles de protección son operados por el proveedor de alojamiento para evitar riesgos residuales (rotura de tubería, por ejemplo).

5.1.5. Prevención y protección contra incendios.

Las áreas aseguradas se benefician de la prevención y protección adecuadas contra la exposición al fuego.

5.1.6. Almacén de datos

Los medios se almacenan de forma segura. Los medios de respaldo se almacenan de forma segura en una ubicación separada de la ubicación de medios original.

Todas las áreas de almacenamiento de medios están protegidas contra incendios, exposición al agua y daños.

El SST guarda los documentos en papel en locales cerrados con llave y los almacena en una caja fuerte en la que los medios de apertura son conocidos únicamente por el oficial autorizado de la TSA y el personal autorizado.

5.1.7. Deposito de basura

Los materiales enumerados como confidencialmente sensibles están sujetos a destrucción, o pueden usarse nuevamente en un contexto operativo similar al mismo nivel de sensibilidad.

5.1.8. Copia de seguridad fuera del sitio

Para garantizar una recuperación que cumpla con sus compromisos después de un incidente, SOFTNET implementa copias de seguridad de información y funciones críticas.

SOFTNET garantiza que las copias de seguridad se exporten fuera del sitio de producción y estén protegidas en cuanto a confidencialidad e integridad.

5.2. Controles de procedimiento

5.2.1. Roles confiables

Se definen los siguientes roles de confianza:

- Responsable de Seguridad de la TSA: tiene la responsabilidad de todos los aspectos de seguridad del SST.
- Administrador del sistema TSA: instala, configura y mantiene los sistemas confiables del SST.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

- Operador del sistema TSA: responsable de operar la TSU en el día a día.
- Auditor del sistema TSA: responsable del análisis diario de los registros de auditoría.

Las operaciones y las supervisiones son realizadas por personal de SOFTNET y CAMERFIRMA.

La administración del software de sello de tiempo de CAMERFIRMA instalado en los equipos de SOFTNET para su SST, es realizada de manera remota por personal de CAMERFIRMA desde su sede asignada.

SOFTNET tendrá acceso de usuario al software de sello de tiempo para revisión de informes y configuraciones.

SOFTNET puede brindar el servicio de sellado de tiempo a sus clientes a través de su API.

5.2.2. Número de personas requeridas por tarea

La TSA aplica procedimientos para garantizar que se requieran varias personas en un rol de confianza para realizar tareas delicadas.

5.2.3. Identificación y autenticación para cada rol.

Los controles de identificación y autenticación se definen para apoyar las implementaciones de la política de control de acceso y la responsabilidad de las operaciones. La política de control de acceso limita el acceso al personal autorizado según sea necesario.

El personal en funciones de confianza es designado por el Responsable de la TSA de SOFTNET, con notificaciones escritas a las personas interesadas.

5.2.4. Roles que requieren separación de funciones

SOFTNET y CAMERFIRMA garantizan que los procedimientos de seguridad estén separados de los procedimientos de explotación estándar y que siempre se realicen bajo la supervisión de un personal en un rol de confianza.

5.2.5. Análisis de riesgos.

Se realiza un análisis de riesgos en el SST para identificar las amenazas en el TSU.

5.2.6. Sistema de gestión de acceso

Identificación y autenticación

Los sistemas, las aplicaciones y las bases de datos identifican y autentican de manera única a los operadores y administradores. Cualquier interacción entre el sistema y un operador es posible solo después de una identificación y autenticación exitosas. Para cualquier interacción, el sistema verifica la identidad del personal operativo.

La información de autenticación se almacena de manera que solo puedan acceder usuarios autorizados.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

Control de acceso

Los perfiles y los derechos de acceso al equipo TSA se especifican y documentan, así como los procedimientos de registro / baja del personal operativo.

Los sistemas, las aplicaciones y las bases de datos pueden distinguir y administrar los derechos de acceso para cada usuario en los objetos sujetos a la administración de derechos, a nivel de usuario, a nivel de grupo, o ambos. Es posible:

- negar a los usuarios o grupos de usuarios el acceso a un objeto;
- limitar el acceso del usuario a un objeto a las operaciones que no modifican este objeto;
- conceder derechos de acceso a un objeto con el nivel de granularidad del usuario individual.

Alguien que no sea un usuario autorizado no puede otorgar ni negar derechos de acceso a un objeto. Asimismo, solo los usuarios autorizados pueden crear nuevos usuarios y suprimir o suspender usuarios existentes.

Administración y operación

El uso de herramientas de utilidad está restringido y controlado.

5.2.7. Gestión de operaciones

Planificación del sistema

La carga de los sistemas se monitorea y se realizan proyecciones de los requisitos de capacidad futuros para garantizar que haya disponible una potencia de procesamiento y almacenamiento adecuados.

Protección contra códigos maliciosos

El monitoreo, la detección y la prevención se implementan en cada componente del SST para proporcionar protección contra software malicioso.

Controles de seguridad de red

Los controles implementados cumplen con la estrategia de gestión de riesgos de SOFTNET, en los temas que le competen, y de CAMERFIRMA, para sistemas de información. El SST es implementado sobre una red protegida por firewall. Estos firewalls están configurados para aceptar solo conexiones que son estrictamente necesarias.

Las comunicaciones de red que transfieren información confidencial están protegidas contra escuchas.

Los controles de seguridad se implementan para proteger los componentes locales del sistema de información del acceso no autorizado.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

Manejo de medios y seguridad

Todos los medios sensibles del SST están sujetos a procedimientos de mantenimiento para garantizar la disponibilidad de funciones e información.

Las condiciones de finalización de la vida útil (destrucción y eliminación de desechos) de los equipos se documentan para garantizar la no divulgación de información confidencial que puedan incluir.

Intercambio de información

Los controles de seguridad se implementan para garantizar la autenticación del origen, la integridad y la confidencialidad, cuando sea necesario, de los datos intercambiados entre las partes involucradas en el proceso.

5.2.8. Implementación y mantenimiento de sistemas confiables

El SST utiliza componentes confiables. En particular, las TSU cumplen con los requisitos reglamentarios. El Responsable de la TSA es notificado de cualquier cambio sustancial del sistema.

Las versiones están sujetas a una actualización de los procedimientos operativos. Se implementan controles de las operaciones de mantenimiento.

Rendimiento adecuado de las aplicaciones

Las infraestructuras de desarrollo y prueba están separadas de las infraestructuras operativas del SST.

Los criterios de aceptación y validación de nuevos sistemas, actualizaciones y nuevas versiones están documentados y se realizan las pruebas apropiadas antes de la aceptación y el paso de producción.

5.2.9. Informe de incidentes y respuesta

El monitoreo de la operación es posible a través de los registros de auditoría.

Cualquier mal funcionamiento de la TSU se notifica inmediatamente al supervisor y al operador de la plataforma CAMERFIRMA. Estas notificaciones se refieren especialmente a:

- Inicio / parada de servicios;
- Desincronización de los relojes SST;
- Problemas de red de SST.

Cada evento se almacena en una base de datos desde la cual se pueden rastrear todos los eventos de servicio, incluidos los incidentes. Si ocurre un incidente, CAMERFIRMA, como el proveedor de servicios de certificación digital y sellado de tiempo de SOFTNET, actuará de manera apropiada para reaccionar rápidamente, limitar el impacto de la exposición a la seguridad y restablecer el servicio en el mejor tiempo posible.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

5.3. Controles de personal

SOFTNET y CAMERFIRMA han documentado la seguridad de la información para los recursos humanos. SOFTNET en particular declara que el personal en un rol de confianza del SST se selecciona cuidadosamente y se informa claramente de las operaciones y las reglas a seguir.

5.3.1. Requisitos de calificación, experiencia y autorización

Cualquier persona en un rol de confianza está sujeta a una cláusula de confidencialidad, administrada por SOFTNET. Ella garantiza que las habilidades profesionales del personal en Roles de confianza cumplan con los requisitos de sus funciones. La administración de SOFTNET, en lo que le compete, tiene la experiencia adecuada y está familiarizado con los procedimientos de seguridad. Cualquier persona en un rol de confianza es informada de su responsabilidad a través de su descripción de trabajo y / o procedimientos relacionados con la seguridad del sistema y el control del personal.

El personal que trabaja en el SST de SOFTNET posee el conocimiento apropiado de:

- tecnología de sellado de tiempo;
- tecnología de firma digital;
- mecanismos de calibración o sincronización de los relojes TSU con UTC;
- procedimientos de seguridad, para personal con responsabilidades de seguridad;
- Seguridad de la información y evaluación de riesgos.

5.3.2. Procedimientos de verificación de antecedentes

SOFTNET realiza una verificación de antecedentes policiales antes de contratar personal nuevo, para garantizar la idoneidad con el puesto abierto.

5.3.3. Requisitos de entrenamiento

El personal está capacitado con respecto al software y hardware en uso y con respecto a la aplicación de procedimientos internos.

5.3.4. Frecuencia de reentrenamiento y requisitos

Cada cambio de sistemas, procedimientos u organización da como resultado información o capacitación del personal operativo cuando este cambio impacta el trabajo de esta categoría de personal.

El personal operativo está capacitado en gestión de incidentes y escalada.

5.3.5. Frecuencia y secuencia de rotación laboral

No aplica.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

5.3.6. Sanciones por acciones no autorizadas.

Las sanciones en caso de acciones no autorizadas se enumeran en una carta del área responsable y a través del documento sobre seguridad de la información para los recursos humanos. Todo el personal de SOFTNET está informado de estas sanciones.

5.3.7. Requisitos de contratista independiente

Los requisitos para los subcontratistas están sujetos a contratos.

Los compromisos incluyen contratos relacionados con el suministro de servicios, acuerdos de confidencialidad y estatutos de TI.

5.3.8. Documentación entregada al personal

El personal es informado de las reglas de seguridad relacionadas con su rol tan pronto como son nombrados. La persona a cargo de una función operativa en el SST recibe procedimientos relacionados.

6. Controles técnicos de seguridad.

6.1. Precisión de tiempo

Los relojes TSU se administran y supervisan a través de servidores de tiempo de referencia de CAMERFIRMA. Estos servidores son autónomos y están sincronizados con los servidores de referencia UTC (k). Los mecanismos utilizados permiten que el sistema resista ataques destinados a desincronizar fuentes de tiempo, incluso ataques importantes contra señales de radio o satélite.

SOFTNET asegura que los TST generados por su SST tengan una precisión con respecto al tiempo UTC de menos de un segundo.

6.2. Generación de la clave

SOFTNET garantiza que todas las claves criptográficas se generen en un entorno controlado. Específicamente, las claves de firma de TSU se generan dentro de un módulo de sellado de tiempo.

La generación de claves criptográficas TSU se realiza dentro de los módulos de seguridad de hardware. Las claves privadas de TSU nunca se exportan fuera de estos módulos.

Las generaciones clave se basan en los algoritmos clave admitidos (definidos en la Sección 6.7).

6.3. Certificación de claves TSU

Una solicitud de certificado de TSU se transmite a la EC de SOFTNET, de acuerdo con las reglas definidas en la Política de Certificación correspondiente.

Los certificados entregados por la EC se ajustan al perfil definido en la Política de certificación. La TSA cumple con sus obligaciones definidas en la Política de Certificación de la EC.

La TSA verifica, al importar un certificado en una TSU, que proviene de la EC de SOFTNET.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

6.4. Protección de claves privadas de TSU

SOFTNET garantiza que las claves privadas de TSU se mantengan confidenciales y garantiza su integridad.

Específicamente, las claves de firma de TSU se guardan y utilizan dentro del módulo de sellado de tiempo.

6.5. Copia de seguridad de claves privadas de TSU

SOFTNET prohíbe el archivo y la copia de seguridad de las claves privadas de TSU.

6.6. Destrucción de claves privadas de TSU

SOFTNET asegura que las claves privadas de TSU se destruyan al final de su ciclo de vida.

6.7. Algoritmos obligatorios

La TSA de SOFTNET:

1. acepta valores hash generados por los suscriptores y utiliza algoritmos hash de conformidad con los requisitos reglamentarios. Los algoritmos hash aceptados son los siguientes: SHA-256, SHA-384 y SHA-512
2. emite TST firmados con algoritmos y longitudes de clave de conformidad con los requisitos reglamentarios. SOFTNET garantiza el uso de una longitud mínima de clave de certificados de módulo de 2.048 bits para algoritmos RSA / DSA y una longitud mínima de clave de 256 bits para algoritmos ECC. El algoritmo de firma utiliza una función hash que pertenece a la familia SHA-2.

6.8. Verificación TST

SOFTNET garantiza que las Partes que confían puedan obtener la información necesaria para verificar la firma digital de los TST. SOFTNET se asegura especialmente de que los certificados de TSU estén disponibles, ya sea adjuntos a los TST o desde el sitio web de SOFTNET.

6.9. Periodo de validez de los certificados TSU

Un certificado TSU es válido por un máximo de 135 meses. SOFTNET garantiza que el algoritmo y el tamaño de la clave sean adecuados para este período de validez.

6.10. Período de uso de claves privadas de TSU

La clave privada vinculada al certificado TSU y que firma TST tiene un período de uso de un año. Sin embargo, los suscriptores y las partes confiables pueden verificar la validez de los TST por lo menos hasta que caduque el certificado TSU después de su generación.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7. Certificado y perfiles TST

7.1. Perfil de certificado

Campos base

Version	V3
Serial Number	Unique Non-Sequential CSPRNG Number and is greater than zero.
Signature Algorithm	SHA-256, SHA-384 or SHA-512 with RSA Encryption or ECDSA with SHA-256, SHA-384 or SHA-512
Issuer: CN	<Issuing CA Common Name>
Issuer: O	<Issuing CA Organization name>
Issuer: OU	<Issuing CA Organization unit>
Issuer: C	<Issuing CA Country>
Valid From	Start date expressed in UTC format
Valid To	Start date expressed in UTC format
Public Key	RSA 2048, 4096 (OR) ECC curves NIST P-256, P-384, or P-521
Subject: CommonName	Common Name of TSA
Subject: OrganizationName	Legal Name of TSA Organization
Subject: OrganizationalUnitName	Variable Information representing TSU
Subject: CountryName	Country of TSA
Key Usage	Critical=TRUE digitalSignature
Enhanced Key Usage	id-kp-timeStamping
Certificate Policies	Critical=FALSE 1. Policy ID= 1.3.6.1.5.5.7.2.1 (User Notice, Time Stamping Certificate) 2. Policy ID= 1.3.6.1.4.1.17326.10.13.1.3.1 (CPS), http://policy2021.camerfirma.com
Subject Key Identifier	Critical=FALSE 160-bit hash (SHA-1)
Authority Key Identifier	Critical=FALSE 160-bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.CAMERFIRMA.com?<IssuerName>.crl

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7.2. PERFIL TST

Version	Version 1
policy	Policy OID as per Section 1.2 of this document.
messageImprint	OID of the hash algorithm and the hash value of the data to Timestamp. **Note**: this information is provided by the Subscriber in the request.
serialNumber	160-bit number uniquely identifying the TST
genTime	Time-stamp date in ASN.1 Generalized Time format
accuracy	Accuracy of 1 second
ordering	Flag set to FALSE
nonce	Value sent back identically if contained in the request
tsa	DN Details of the TSU **Note:** This field is the same as the "subject" of the certificate used to sign the TST.
extensions	Not used

8. Auditoría de cumplimiento y otras evaluaciones

8.1. Frecuencia o circunstancias de la evaluación.

SOFTNET deberá cumplir con las auditorías de cumplimiento según lo siguiente:

- Mínimo de una auditoría anual realizada por un auditor calificado identificado en la Sección 8.2.
- Mínimo una auditoría anual, denominada "auditoría interna", realizada por CAMERFIRMA, o un profesional identificado y / o aprobado por CAMERFIRMA.

SOFTNET también realizará auditorías adecuadas por parte de su auditor interno o externo para:

- Cualquier calificación (nueva / renovación) por un regulador.
- Cualquier cambio importante en este TSP / TSPS, según lo identifique el Responsable de la TSA de SOFTNET.

8.2. Identidad / calificaciones del evaluador

El evaluador debe actuar con rigor para garantizar que las políticas, declaraciones y servicios se implementen correctamente y para detectar los elementos de incumplimiento que puedan poner en peligro la seguridad del servicio.

La TSA se compromete a contratar asesores con un alto nivel de experiencia en seguridad de sistemas, particularmente en el campo de la parte auditada.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

8.3. Relación del asesor con la entidad evaluada

El evaluador es designado por SOFTNET y aprobado por CAMERFIRMA, y se le permite auditar las prácticas que rigen el componente objetivo de la auditoría. El evaluador puede ser parte de SOFTNET pero es independiente de las operaciones de la TSA.

8.4. Temas cubiertos por la evaluación

El evaluador realiza auditorías de cumplimiento del componente especificado, cubriendo total o parcialmente la implementación de:

- La PST y DPST;
- el SST.

Antes de cada auditoría, el evaluador proporcionará al Responsable de la TSA una lista de componentes y procedimientos que desean auditar, y posteriormente preparará el programa de auditoría detallado.

8.5. Acciones tomadas como resultado de deficiencia

Después de la auditoría de cumplimiento, el equipo de evaluación le da a la TSA el resultado que puede ser "éxito", "fracaso" o "por confirmar".

En caso de falla, el equipo de evaluación entrega recomendaciones a la TSA. La TSA luego decide qué acciones realizar.

En caso de que el resultado "se confirme", el equipo de evaluación identifica los incumplimientos y los prioriza. Luego, la TSA programa la corrección de estos incumplimientos. Una auditoría de validación luego verifica sus correcciones efectivas.

En caso de éxito, la TSA confirma que la parte auditada cumple con los requisitos del PST y DPST.

8.6. Comunicación de resultados.

Los resultados de la auditoría se ponen a disposición del Responsable de la TSA de SOFTNET y de cualquier otra organización externa para la calificación necesaria u otros fines (Ejemplo: Regulador, Proveedor de aplicaciones, Proveedor de Trust Store, etc.).

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. Responsabilidades.

Respecto a las responsabilidades financieras estas están amparadas bajo los términos y alcances de la póliza de seguros que para esos fines debe estar vigente en tanto el servicio este vigente.

La TSA dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente en Perú.

La TSA actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de sus clientes.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

GERENCIA GENERAL SOFT&NET SOLUTIONS S.A.C.

Las responsabilidades incluyen las establecidas por la presente CPS, así como las que resulten de aplicación como consecuencia de la normativa peruana.

9.2. Política de Reembolso.

SoftNet proporcionará un reembolso a los suscriptores bajo ciertas circunstancias y sujeto a ciertas condiciones. Los detalles de estos estarán contenidos en el documento contractual correspondiente

9.3. Cobertura del Seguro.

Para la EC Raíz, ECs emisoras y los servicios de certificación prestados directamente por emSign, se mantiene un contrato de seguro que cubra la responsabilidad expresada en la sección Obligaciones.

Para los afiliados y clientes corporativos que actúan como ECs o ERs, las condiciones contractuales acordadas entre las partes garantizan las responsabilidades asumidas por cada parte y transfieren los requisitos a favor del correspondiente seguro para las obligaciones transferidas

9.4. Avisos Individuales y Comunicaciones con los Participantes.

SoftNet acepta avisos relacionados con esta CP y DPC, en papel o en forma electrónica, en la ubicación y / o dirección de correo electrónico especificada en este documento. Los avisos se consideran efectivos después de que el remitente recibe un acuse de recibo válido y firmado de SoftNet. Si el remitente no recibe un acuse de recibo dentro de los siete días, el remitente debe reenviar el aviso en papel a la dirección especificada en este PC y DPC utilizando un servicio de mensajería que confirma la entrega.

SoftNet proporcionará cualquier aviso requerido bajo esta PC y DPC por medios físicos o electrónicos, a menos que se acuerde específicamente lo contrario.

10. CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la TSA de SOFTNET, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción	Autor
12.05.2023	1.0	Documento Inicial	Responsable de Seguridad
12.05.2023	1.0	Documento Revisado	Administrador de la TSA
12.05.2023	1.0	Documento Aprobado	Responsable de la TSA
24/06/2023	1.1	Se agrego el Apartado 9, Otros Asuntos Legales y Comerciales, como información necesaria para el desarrollo de las Políticas y Declaración de Practicas	Responsable de Seguridad
24/06/2023	1.1	Documento Revisado	Administrador de la TSA
24/06/2023	1.1	Documento Aprobado	Responsable de la TSA

Elaborado por: **Pedro Rivera**	**Revisado y Aprobado por:** **Christian Gutierrez**	**Revisado y Aprobado por:** **Carlos Dextre**
 V°B°	 V°B°	 V°B°
Cargo: OFICIAL DE SEGURIDAD	Cargo: Administrador del STA	Cargo: Responsable de la TSA

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA