SERVICIO DE VALOR AÑADIDO
AUTORIDAD DE SELLADO DE TIEMPO

POLÍTICA DE SEGURIDAD

PS
SGTSA-PO-02

Versión 1.0

CONTENIDO

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 2020 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 para cumplir la certificación ISO 27001.

2. OBJETIVO

Establecer el marco general y los lineamientos referidos a la seguridad de la información en los procesos relacionados a su papel de Autoridad de Sellado de Tiempo.

3. ALCANCE

El contenido de la presente política, así como los procedimientos que se deriven de ella, serán de cumplimiento obligatorio para el personal involucrado en la Prestación de Servicio de Valor Añadido de la TSA de SoftNet. También será de cumplimiento obligatorio de los proveedores de servicios o terceros que proporcionen sus servicios a la TSA de SoftNet.
El servicio prestado por la TSA de SoftNet es la emisión de sellos de tiempo, los cuales corresponden con una prueba confiable que un documento electrónico existió en un determinado momento en el tiempo, cuando el sello de tiempo es emitido, y que desde ese momento no fue alterado.

4. RESPONSABILIDADES

SoftNet asume las responsabilidades de representación de los servicios de sello de tiempo que brinda, a fin de ejecutar las garantías y cláusulas contractuales con los clientes. En tal sentido establece y garantiza el cumplimiento de los niveles de servicio y requerimientos contractuales acordados con cada cliente.

5. DEFINICIONES Y ABREVIACIONES

5.1. DEFINICIONES

Tercero que confía	Persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez de dicho sello
Suscriptor	Persona natural o jurídica que requiere los servicios provistos por una Autoridad de sellado de tiempo – TSA y que está de acuerdo con los acuerdos y obligaciones descritos en la Declaración de Prácticas y la Política de Sellado de Tiempo.

Política de sellado de tiempo	Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.
Sello de tiempo	Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. El sello de tiempo incluye: • La firma digital de la entidad de sellado de tiempo. • Identificador electrónico único del documento (HASH o resumen). • Fecha y hora recogida de una fuente fiable de tiempo.
Autoridad de Sellado de tiempo	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas	Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.
Sistemas de la TSA	Sistemas de tecnologías de la información qu soportan la provisión de servicios de sellado de tiempo.
Unidad de Sellado de tiempo	Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

5.2. ABREVIACIONES

BIPM International Bureau of Weights and Measures (Bureau International des Poids et Mesures)
GMT Greenwich Mean Time
IERS International Earth Rotation Service
TAI International Atomic Time (Temps Atomique International)
TSA Time-Stamping Authority
TSU Time-Stamping Unit
UTC Coordinated Universal Time

6. EVALUACIÓN DE RIESGOS

Para cada subproceso vital o crítico que se desarrolla en el ámbito del proceso de emisión de sellos de tiempo, se deberá efectuar el análisis y evaluación de riesgos, teniéndose en consideración tanto las amenazas internas como externas; asimismo, se identificarán, evaluarán e implementarán las opciones de tratamiento del riesgo que permitan mitigar el impacto de los activos de información.
La evaluación y tratamiento del riesgo se realizará de acuerdo a la Metodología de Análisis y Tratamiento del Riesgo definida por SoftNet en su Plan de Contingencia.

7. CONTROL DE ACCESOS

Se controlará el acceso a la información confidencial generada durante el proceso de emisión de sellos de tiempo, en concordancia con lo establecido en el Plan de Privacidad, la clasificación de información y los resultados de la evaluación de riesgos.
La administración del acceso a los usuarios debe considerar que:

- Toda solicitud de acceso físico y lógico, así como la administración de las cuentas de usuario a los activos de información deberá ser realizada conforme a los procedimientos establecidos.
- Sólo se asignarán cuentas de acceso individuales.

El personal que reciba una cuenta de usuario para el acceso a los activos de información deberá hacer uso adecuado de sus contraseñas de acceso, manteniendo la confidencialidad de la misma, no dejando sus estaciones de trabajo desatendidas, solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad y seleccionando una contraseña que tenga un nivel adecuado de complejidad.
Es responsabilidad de los propietarios de los activos de información el clasificar la información (física o digital) de acuerdo con lo indicado en los lineamientos definidos para la clasificación de la información. Asimismo, identificar y agrupar a los usuarios, considerando su necesidad de información para el desarrollo de sus funciones o labores que realicen, con la finalidad de establecer los niveles de acceso a la base de datos, sistemas y/o aplicativos, centro de datos, infraestructura de procesamiento de información, archivos físicos y electrónicos, de acuerdo con el resultado de la evaluación de riesgos y los requerimientos de la organización.
Corresponde a los órganos que conforman el proceso de emisión de sellos de tiempo establecer un proceso periódico de revisiones de los derechos de acceso de su personal, así mismo, programar revisiones periódicas de las políticas configuradas en su red de datos.
Es responsabilidad del encargado o supervisor solicitar, en el menor tiempo posible, la inactivación de las cuentas de usuario cuando éstos ya no presten sus servicios, o cuando el usuario ya no requiera el acceso a la información de SoftNet.

8. SEGURIDAD DE PERSONAL

Se debe asegurar que el personal, contratista y terceros reciban y comprendan sus responsabilidades respecto al uso y tratamiento de los activos de información, con la finalidad de reducir el riesgo de hurto, fraude o mal uso de la información. Así mismo, se deberá asegurar la implementación de controles de seguridad relacionados al personal, antes, durante y finalizado el empleo o servicio brindado dentro del proceso de emisión de sellos de tiempo.
<u>Antes del empleo:</u>

- Los perfiles de los puestos deberán ser definidos en base a las funciones que se van a desarrollar y las responsabilidades que les competan.
- Se deben implementar controles para la selección y contratación del personal, a fin de verificar la veracidad de los datos proporcionados por los postulantes, así como sus antecedentes penales y policiales. Para el caso de quienes vayan a desarrollar roles de confianza, se podría incluir la verificación de sus antecedentes crediticios.
- Para los servicios efectuados por terceros, la verificación de los datos del personal la efectuará el proveedor del servicio. SoftNet se reserva el derecho de verificar dicha documentación.
- Cada una de las personas que presta servicios en el proceso de emisión de sellos de tiempo debe firmar un acuerdo de confidencialidad o un documento de compromiso de aceptación o

cumplimiento, según corresponda, para salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

Durante el empleo:

- Toda persona que preste servicios en el proceso de emisión de sellos de tiempo debe recibir charlas de inducción en materia de Seguridad de la Información.
- Se deben desarrollar actividades de capacitación continua, dirigidas a mantener actualizados los conocimientos del personal respecto al uso y reserva de la información, así como a las políticas y procedimientos relevantes para sus funciones.
- Para los casos de tercerización de servicios se informará al prestador del servicio cuáles son los criterios que deberá considerar para la seguridad de la información, así como también, se monitoreará y revisará su cumplimiento.
- Todo incumplimiento de la Política de Seguridad de parte del personal o proveedores deberá ser informado al Oficial de Seguridad para su análisis, evaluación y comunicación al órgano correspondiente, a fin de que éste proceda a la sanción que corresponda en concordancia con su normativa correspondiente, o en el caso de proveedores, para su comunicación a la Gerencia para la sanción que corresponda de acuerdo a los términos contractuales existentes.

Finalización del empleo:

- Todo cambio o finalización de funciones deberá realizarse de acuerdo a los procedimientos de SoftNet, incluyendo le entrega de los bienes asignados al personal. De igual modo, se deberá solicitar al retiro de los accesos de su personal a la información o servicios.

9. SEGURIDAD FÍSICA

Se deben implementar controles de seguridad física con la finalidad de prevenir accesos no autorizados a los ambientes en que se procesa o resguarda información confidencial, y de esta manera, evitar el daño o pérdida de los archivos de información críticos.

Se deben delimitar los perímetros del ambiente en que se procesa o resguarda la información sensible, así como, establecer controles físicos de entrada y salida. Se deben instalar controles de seguridad contra incendios, aniegos y otros, que permitan alertar en casos de emergencia.

Los ambientes serán diseñados e implementados adecuadamente para la seguridad del personal y de los recursos que albergan. Se deberá, así mismo, establecer controles de acceso a los ambientes, al uso de las llaves de los mismos, y asignar a los responsables respectivos. También se debe definir e implementar un plan de evacuación en caso de desastre.

Estas políticas de seguridad física se deben considerar también para los ambientes de contingencia.

10. SEGURIDAD DE COMUNICACIONES Y REDES

Se deben establecer responsabilidades y procedimientos documentados de operación asociado al procesamiento de información y recursos de comunicaciones, con el objetivo de evitar daños, accesos no autorizados, mal uso de los activos de información, garantizar la seguridad de los datos y la disponibilidad de los servicios utilizados a través de la red de SoftNet y del internet.

En lo posible se segregarán las tareas y se implementará un procedimiento de gestión de cambios, con la finalidad de prevenir modificaciones no autorizadas en los equipos de comunicaciones y redes.

11. MANTENIMIENTO DE EQUIPOS Y SU DESECHO

Se debe asegurar la disponibilidad e integridad de los equipos a través de un adecuado plan de mantenimiento preventivo especialmente para los equipos críticos, el cual se realizará según el procedimiento establecido por SoftNet, documentándose los incidentes que ocurren antes, durante y después del mantenimiento.
Antes del desecho o reúso de los equipos se revisará que toda información sensible haya sido removida o sobre escrita, con la finalidad de prevenir el acceso no autorizado a información sensible.
El reemplazo, decomiso, manipulación y desecho, tanto del hardware como del software, se realizará de acuerdo a los criterios establecidos por SoftNet para el correcto uso de los equipos.

12. CONTROL DE CAMBIOS Y CONFIGURACIÓN

Se debe asegurar un control satisfactorio de todos los cambios realizados a los equipos, software y procedimientos, en lo posible se deberá garantizar la posibilidad de revertir los cambios efectuados sin éxito.
Se deberá realizar y aprobar los cambios en los sistemas y recursos de tratamiento de información; así mismo, previo al cambio se efectuará un análisis de impacto a los sistemas y proceso, comunicando el cambio a todos los involucrados. Se ha dispuesto que todo cambio o modificación que se realice al sistema sea debidamente documentado, y además que dichas modificaciones se efectúen, de preferencia, fuera del horario de atención a los clientes o en horas de menor demanda.

13. PLANIFICACIÓN DE CONTINGENCIA

Los áreas que tienen la responsabilidad de desarrollar y proporcionar los servicios de emisión de sellos de tiempo que se brindan a los usuarios, implementarán un Plan de Contingencia a nivel de servicios, que les permita reaccionar ante una posible interrupción en las actividades críticas del proceso y en el tiempo requerido por SoftNet.
Para establecer el Plan de Contingencias se identificarán procesos críticos para el servicio prestado, los eventos que puedan ocasionar interrupciones en estos procesos, y los planes o acciones que se deberán efectuar para mantener y recuperar las operaciones, así como el período en que estos deberán recuperarse.
Se deberá establecer pruebas periódicas del Plan de Contingencias, que permitan evaluar su eficacia y efectuar su actualización, de ser el caso.

14. RESPUESTA A INCIDENTES

Se deberá clasificar, comunicar y atender los incidentes de manera rápida, eficaz y sistemática, a fin de garantizar el restablecimiento del servicio afectado en el menor tiempo posible.
Para el caso de los incidentes que afecten la seguridad de la información, se deberá establecer que toda persona (personal o proveedor) que presta servicios en el proceso de emisión de sellos de tiempo deberá comunicar oportunamente al Oficial de Seguridad o persona designada, cuando se haya detectado o tomado conocimiento del incidente, para que puedan ser atendidos conforme al procedimiento establecido. Adicionalmente, los encargados de supervisar la seguridad de la información y privacidad de datos, deberán llevar un registro de los incidentes de seguridad ocurridos en su ámbito de alcance, monitoreando la implementación de las acciones correctivas o preventivas que ameriten.

15. AUDITORÍAS Y DETECCIÓN DE INTRUSIONES

Se programarán como mínimo una auditoría al año. Al término de la auditoría el área o persona auditada deberán implementar en el menor tiempo posible las acciones correctivas y preventivas identificadas.
Se deberán ejecutar pruebas periódicas de detección de intrusiones, así como, implementar controles que permitan alertar los intentos de acceso no autorizados.
Los sistemas y procesos (manuales o automáticos) deberán contar con registros de auditoría actualizados, los mismos que deben brindar información de la acción ejecutada, la hora, fecha, identificación del personal, software y hardware utilizado, según corresponda.

16. MEDIOS DE ALMACENAMIENTO

Se debe asegurar la protección de los documentos, medios informáticos, datos de entrada y salida y documentación del proceso de emisión de sellos de tiempo de las ocurrencias como daño, modificación, robo o acceso no autorizado.
Se debe establecer un procedimiento para la administración de los medios de almacenamiento de información, y los controles de seguridad requeridos para el almacenamiento, uso y protección de la información, considerándose también el uso de los medios de almacenamiento removibles, el proceso de eliminación segura de información, la planificación y ejecución de copias de seguridad, así como su proceso de restauración.

17. ADMINISTRACIÓN DE CLAVES

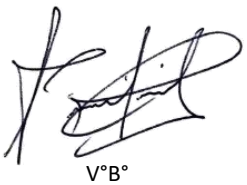
Se deben asegurar la confidencialidad de las claves criptográficas y se implementarán los controles requeridos de acuerdo al nivel de seguridad acreditado.

18. 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.

HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción	Autor
15.05.2020	V 1.0	Documento Inicial	Oficial de seguridad
01.06.2020	V 1.0	Documento Revisado y Aprobado	Responsable de la TSA

Elaborado por: PEDRO RIVERA	Revisado y Aprobado por: MIGUEL TITO	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
Fecha: 15 / 05 / 2020	Fecha: 22 / 05 / 2020	Fecha: 01 / 06 / 2020