Servicios de Valor Añadido

THOMAS SIGNE
Soluciones Tecnológicas Globales

Política de Seguridad de los Servicios de Valor Añadido

Sistema de Intermediación Digital

Información del documento

Nombre	Política de Seguridad de los Servicos de Valor Añadido – Sistema de Intermediaci
Realizado por	Thomas Signe Perú
País	Perú
Versión	1.3
Fecha	Septiembre 2021
Tipo de documento	Confidencial
Código	THS-PE-AC-POL-03

Historial de versiones

Versión	Fecha	Descripción
1.0	02/10/2017	Elaboración de documento inicial.
1.1	01/04/2019	Integración con el sistema de gestión del Grupo. Cambio de código del documento de THS-PE-POL-SI-SID-01 a THS-PE-POL-SVA-AC-00 Se modifica el alcance el cual abarca todos los Sistemas de Intermediación Digital de Thomas Signe. Se modifica los controles de seguridad debido a la migración del centro de datos gestionado. Se modifica la estructura del documento. Se agrega el apartado seguridad en las redes.
1.2	30/12/2020	Ajuste d ela codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.5

1.3	16/09/2021	Cambio de imagen THS

ÍNDICE

1 INTRODUCCIÓN

Signe S.A. (en adelante 'Signe') es una empresa con domicilio en España que brinda principalmente servicios consistentes en la edición e impresión de documentos de seguridad para empresas públicas y privadas. A partir del año 2010, Signe inicia su actividad como Prestador de Servicios de Certificación (PSC) que emite certificados reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica en España.

Desde hace más de 30 años, Signe se ha especializado en el diseño y desarrollo de soluciones de seguridad documental, produciendo y editando documentos -tanto en soporte papel como digital- protegidos contra posibles falsificaciones y modificaciones fraudulentas.

Hoy en día, gracias a una constante inversión en tecnología punta y la aplicación de estrictos controles de calidad, Signe se posiciona como un referente dentro del sector a nivel europeo y, cada vez más, también a nivel mundial.

En el año 2018, en una alianza comercial con la empresa Thomas&Greg Perú, se ha creado la empresa Thomas Signe de Perú S.A. (en adelante Thomas Signe), para actuar como Entidad de Certificación, Entidad de Registro, Software de Firma Digital y Servicios de Valor Añadido como Sistema de Intermediación Digital y Autoridad de Sellado de Tiempo (Timestamp); y así brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

En calidad de Prestador de Servicios de Valor añadido - SVA, Thomas Signe provee servicios por medio de la infraestructura de Signe en España, a través de la implementación de soluciones que utilizan los certificados digitales con el propósito de asegurar las transacciones documentarias. En este sentido, Thomas Signe provee las soluciones de software y el sistema de gestión necesarios para en conjunto regular y controlar la gestión de usuarios y el intercambio seguro de información, así como la generación y protección de registros auditables de las transacciones realizadas.

La infraestructura tecnológica y operativa del Sistema de Intermediación Digital son provistas por Signe. Dicha infraestructura ha obtenido la cualificación eIDAS que es verificada anualmente por auditores autorizados y comercializadas en Perú a través de Thomas Signe.

2 OBJETIVO

El presente documento establece directrices para garantizar la autenticidad e integridad de los Servicios de Valor Añadido de Thomas Signe en base a los Sistemas de Intermediación Digital, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación de Thomas Signe cubre los sistemas de aplicaciones de software de trámite administrativo, el cual utiliza procesos de firma digital y autenticación para resguardar la autenticidad, integridad y confidencialidad de las transacciones o trámites administrados. Asimismo, la acreditación cubre las políticas y procedimientos necesarios para gestionar y proteger los servicios y sistemas de certificación digital.

Signe como proveedor de infraestructura tecnológica y operativa del Sistema de Intermediación Digital, asume todos los aspectos de seguridad y calidad de los Servicios de Valor Añadido – Sistema de intermediación digital, provistos por Thomas Signe.

4 DEFINICIONES Y ABREVIACIONES

Prestador de Servicios de Valor Añadido:	PSVA: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE.
Servicios de valor añadido:	SVA: Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
Política de servicios de valor añadido:	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Suscriptor:	Entidad que requiere los servicios provistos por la SVA de Thomas Signe y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía:	Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas.
Declaración de Prácticas de Servicios de Valor Añadido:	DPSVA: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo con lo establecido por INDECOPI.

5 ALCANCE

La presente política es de cumplimiento obligatorio para el personal y terceros subcontratados por Thomas Signe, quienes participan de las operaciones críticas de los Servicios de Valor Añadido coforme a las responsabilidades específicas en las siguientes secciones.

6 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Como proveedor de servicios de los Sistemas de Intermediación Digital, Signe cuenta con controles de seguridad física y del entorno. Para ello subcontrata la infraestructura del Centro de Datos de TELEFÓNICA, el cual cuenta con la certificación TIER IV GOLD.

Los controles de seguridad abarcan el ambiente físico, las redes, los sistemas, entre otros; los cuales se especifican a continuación.

6.1 CONTROLES FÍSICOS

Se tienen establecidcos controles de seguridad física y del entorno para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y del entorno ofrece protección frente:

-Accesos físicos no autorizados.

-Desastres naturales.

-Incendios.

-Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)

-Derrumbamiento de la estructura.

-Inundaciones.

-Robo.

-Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los Servicios de Valor Añadido de los Sistemas de Intermediación Digital.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año.

6.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

La infraestructura del centro de datos de Telefónica, en el cual se encuentran los equipos de Signe, como proveedor de servicios de Thomas Signe, está construida con materiales que garantizan la protección contra acceso no autorizado, ubicado en una zona de bajo riesgo de desastres naturales.

En concreto, la sala donde se realizan las operaciones criptográficas es una jaula de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti – humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

6.1.2 ACCESO FÍSICO

El acceso físico al centro de datos está limitado y protegido mediante una combinación de medidas físicas y procedimientales.

Está limitado a personal expresamente autorizado, con identificación en el momento de acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

Los visitantes son acompañados por personal autorizado, habiendo sido previamente identificados mediante su documento oficial de identidad y registrados.

6.1.3 SEGURIDAD EN LAS REDES

La seguridad en las redes que dan soporte a las actividades están aseguradas mediante las siguientes medidas:

Signe como proveedor de infraestructura dispone de un firewall sobre el que se han implementado las medidas de seguridad necesarias para la correcta actividad de la empresa. Además dispone de un proxy que permite realizar funciones de control de navegación y de aplicaciones.

La red se encuentra protegida por VPN y existen reglas en el mismo firewall para poder acceder.

6.1.4 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El centro de datos dispone de equipos estabilizadores de corriente y un sistema de alimentación eléctrica mediante grupos electrógenos preparados para funcionar de forma continua.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

6.1.5 EXPOSICIÓN AL AGUA

El centro de datos dispone de un sistema de detección de humedad.

6.1.6 PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

6.1.7 SISTEMA DE ALMACENAMIENTO

Cada medio de almacenamiento desmontable que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información y permance solamente al alcance de personal autorizado.

6.1.8 ELIMINACIÓN DE LOS SOPORTES DE INFORMACIÓN

Cuando haya dejado de ser útil, los medios de almacenamiento, antes de ser desechados o reutilizados, deben ser procesados para su borrado, físicamente destruidos o hacer ilegible la información contenida.

6.1.9 COPIAS DE SEGURIDAD FUERA DE LAS INSTALACIONES

Signe, como proveedor de servicios de Thomas Signe, mantiene un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos independiente del centro operacional.

6.2 CONTROLES DE PROCEDIMIENTO

6.2.1 ROLES DE CONFIANZA

Los roles de confianza de Thomas Signe son los que se describen en el documento "Diagrama Organizacional". De esta forma, se garantiza una segregación de funciones que disemina el control y limita el fraude interno.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

Los roles establecidos son:

-Responsables del Sistema de Intermediación Digital: Responsable de la dirección de las operaciones del SID conforme a la normatividad vigente, para aprobar y revisar la implementación y cumplimiento de todos los documentos normativos.

-Responsable de Seguridad de la Información y privacidad de datos personales: Responsable general para aprobar, administrar y velar por el cupmplimiento de las políticas de seguridad y la privacidad de datos personales de los clientes.

-Proveedor de Servicios: Servicios tercerizados que administra la infraestructura tércnica de servicios del SVA, bajo el cumplimiento de estándares internacionales y las prácticas de Thomas Signe.

-Equipo de soportes y atención de incidentes: Atienden a las organizaciones clientes en casp de incidentes de acuerdo a las responsabilidades contractuales.

-Auditor: Servicio tercerizado para los trabajos de auditoría.

6.2.2 IDENTIFICACIÓN Y AUTENTICACIÓN POR ROL

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

6.2.3 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Las tareas de Auditor son independientes de las actividades de operación de los servicios de la SVA.

6.3 CONTROLES DE PERSONAL

6.3.1 REQUISITOS RELATIVOS A LA CALIFICACIÓN, CONOCIMIENTO Y EXPERIENCIA PROFESIONAL

Todo el personal que realiza funciones criticas en la entrega de servicios del SVA está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

Thomas Signe retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

6.3.2 PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

Antes de contratar al personal, Thomas Signe realiza las investigaciones pertinentes respecto de sus antecedentes.

6.3.3 REQUERIMIENTOS DE FORMACIÓN

Se llevan a cabo cursos necesarios para asegurarse de la correcta realización de las tareas de los SVAs, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada trabajador.

6.3.4 REQUERIMIENTOS Y FRECUENCIA DE ACTUALIZACIÓN DE LA FORMACIÓN

Se realizarán actualizaciones de formación de manera anual.

6.3.5 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Se dispone de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

6.3.6 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los terceros contratados, que tengan acceso a información sensible deberán firmar previamente las cláusulas de confidencialidad y los requerimientos operacionales y seguridad establecidos en la política de privacidad y seguridad de Thomas Signe.

Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato de servicios de terceros.

6.3.7 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Thomas Signe pondrá a disposición de todo el personal que participa de los servicios de la SVA, la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad:

- Declaración de prácticas
- Política de privacidad
- Política de seguridad

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

6.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

6.4.1 TIPOS DE EVENTOS REGISTRADOS

Thomas Signe registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la SVA. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de
- privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la SVA a través de la red.
- Intentos de accesos no autorizados a la red interna de la SVA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la SVA
- Encendido y apagado de la aplicación de la SVA.
- Cambios en los detalles de la SVA y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de la SVA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Thomas Signe conserva, ya sea manual o electrónicamente, la siguiente información:

- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en la SVA.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las SVA.

6.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA

Se revisarán los logs de auditoría periodicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

6.4.3 PERIODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría el tiempo que se considere necesario para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

6.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Los dispositivos son manejados en todo momento por personal autorizado.

6.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Thomas Signe dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

6.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo.

6.4.7 ANÁLISIS DE VULNERABILIDADES

Thomas Signe realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

6.5 ARCHIVO DE REGISTROS

6.5.1 TIPOS DE EVENTOS ARCHIVADOS

Se conservarán los eventos relevantes que tengan lugar durante el ciclo de vida de los servicios de las SVAs.

6.5.2 PERIODO DE CONSERVACIÓN DE REGISTROS

Todos los datos del sistema relativos a los SVAs se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable.

6.5.3 PROTECCIÓN DEL ARCHIVO

Thomas Signe asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

6.5.4 PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO

Thomas Signe dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

6.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los documentos relevantes con firma digital generados por los SVAs, incluirán sellos de tiempo acreditados por la IOFE.

6.5.6 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Durante la auditoría requerida por el INDECOPI, el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realiza solo por personal autorizado.

Thomas Signe proporcionará la información y los medios al auditor para poder verificar la información archivada.

6.6 PLAN DE RESUPERACIÓN DE DESASTRES

6.6.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Como proveedor de servicios de los Sistemas de Intermediación Digital, Signe ha desarrollado un plan de contingencia para recuperar todos los sistemas detallado en el documento “Aspectos de Seguridad de la Información para la GCN”

Cualquier fallo en la consecución de las metas marcadas por este procedimiento, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la SVA para implementar dichos procesos.

6.6.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

En el caso de que tuviera lugar un incidente que alterara o corrompiera tanto recursos hardware, software como datos, Thomas Signe procederá según lo estipulado en el documento “Aspectos de Seguridad de la Información para la GCN”.

6.6.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA ENTIDAD DE CERTIFICACIÓN

El plan de contingencias de la jerarquía de Thomas Signe trata el compromiso de la clave privada de la EC como un desastre. En caso de compromiso de la clave privada, Thomas Signe procederá a:

- Informar a todos los Suscriptores, usuarios y otras ECs con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la EC.

- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

6.6.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Thomas Signe restablecerá los servicios críticos de los Servicios de Valor Añadido de acuerdo con la DPSVA de Thomas Signe dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el documento "Aspectos de Seguridad de la Información para la GCN".

7 RESPONSABLE DE SEGURIDAD Y PRIVACIDAD

El Responsable de Seguridad y Privacidad de Datos Personales de Thomas Signe se encarga de velar por el cumplimiento de la presente política, así como de su revisión periódica, difusión, concientización y capacitación al personal y terceros para su adecuado cumplimiento.

8 CONFORMIDAD

Este documento ha sido aprobado por el Responsable del Prestador de Servicios de Valor Añadido de Thomas Signe, y tiene carácter normativo sobre todos los servicios de valor añadido, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.