Política de seguridad para el SVA Sistema de Intermediación Digital

Política

	Nombres y Apellidos	Firma
Elaborado por:	Pablo Chacón **Oficial de Seguridad de la Información**	
Revisado y Aprobado por:	Alexander De Feudis **Líder del Comité de Riesgos**	

Identificación del Documento

Código del documento	POL-16
Nombre del documento	Política de seguridad del SVA Sistema de Intermediación Digital
Versión vigente	1.1
Clasificación	Pública
Responsable de aprobación	Líder del Comité de Riesgos

1. Alcance

La presente política es de cumplimiento obligatorio para el personal de TOC PERU que participa de las operaciones de los servicios relacionados con el Sistema de Intermediación Digital IdentiaSign en todas sus versiones.

2. Objetivo

Establecer los lineamientos para garantizar la autenticidad e integridad de la información crítica mediante la gestión de riesgos de seguridad y la aplicación de políticas y controles que regulen las actividades críticas de las operaciones del Servicio de Intermediación Digital Identia Sign de TOC PERU SAC, de sus servicios por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones en los ámbitos legales, regulatorios y contractuales y los propios procedimientos y políticas de la empresa.

3. Base Legal

- ISO/IEC 27001:2022 – Anexo A - Controles A.5.17 a A.5.23 / Control A.7.4
- POL-05 Política General de Seguridad de la Información v1.0 del SGSI de TOC PERU SAC
- MAN-33 Manual de políticas de Seguridad de la Información v1.0 del SGSI de TOC PERU SAC
- POL-12 Política de Control de Acceso del SGSI de TOC PERU SAC
- PLA-04 Plan de continuidad de negocio con enfoque en DRP de TOC PERU SAC
- Reglamento de la Ley de Firmas y Certificados Digitales (Ley N.° 27269, modificada por la Ley N.° 27310)

4. Definiciones

- **SVA**: Servicio de Valor Añadido
- **PSVA**: Prestador del Servicio de Valor Añadido
- **SID**: Sistema de Intermediación Digital.

- **Tercero que confía**: Persona que recibe un documento, log o notificación firmada digitalmente, y que confía en la validez de las transacciones realizadas
- **Identificador único**: Código o nombre que permite distinguir a cada usuario.
- **Credenciales**: Elementos de autenticación (contraseña, token, biometría, etc.).
- **Gestión de usuarios**: Conjunto de actividades para controlar el ciclo de vida de los accesos.
- **IdentiaSign**: Plataforma de intermediación digital de TOC PERU SAC que opera como SaaS y que permite la realización de procesos de firma electrónica de documentos con validación de identidad.

.

5. Sobre la seguridad física

- Las instalaciones en las que opere TOC PERU y/o los centros de datos utilizados por sus sistemas de información deben prever el daño por desastres naturales, así como desastres creados por el hombre, como incendios, disturbios civiles y otras siniestros, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil, si se encuentran en el Perú. De encontrarse fuera del país, deben mantener las acreditaciones que demuestren el cumplimiento de las medidas de seguridad física propias de su naturaleza.
- **Seguridad física del personal y el equipamiento:** A fin de proteger al personal y el equipamiento en las instalaciones en las que se realicen las operaciones de TOC PERU, se deben implementar los siguientes controles:
    - Señalización de zonas seguras
    - Provisión de extinguidores contra incendios
    - No debe existir cableado eléctrico expuesto
    - Uso de estabilizadores y reguladores de electricidad
- **Perímetros de seguridad y control de acceso físico:** Acorde al control A.7.4 de la norma ISO 27001:2022, se definen las reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad; en el Sistema de Gestión de Seguridad de la Información (SGSI) de TOC PERU SAC. Detalles del anterior propósito y finalidad, se encuentran en el documento POL-12 Política de Control de Acceso, donde se hace referencia a la gestión de privilegios, equipos, software, entre otros.
- **Con respecto a las áreas de archivo** de documentos en papel y archivos electrónicos, estas deben estar protegidas constantemente contra acceso no autorizado:
    - Deben estar en ambientes separados de las áreas públicas
    - Solo debe ingresar personal autorizado
    - El ingreso y salida del personal debe ser registrado
    - Los terceros y el personal de limpieza pueden ingresar con autorización del Responsable de
    - Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área
    - El ingreso y salida de documentos debe ser registrada

- Debe estar cerrada bajo llave cuando no esté siendo usada
- Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

6. Control de acceso a la red

- Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos. Las reglas de acceso a la red a través de los puertos estarán basadas en la premisa " todo está restringido, a menos que esté expresamente permitido".
- **Utilización de los servicios de red:** Para la activación y desactivación de derechos de acceso a las redes, se debe:
  - Controlar el acceso a los servicios de red tanto internos como externos.
  - Identificar las redes y servicios de red a los cuales se permite el acceso.
  - Realizar procedimientos de autorización de acceso entre redes.
  - Establecer controles y procedimientos de administración para proteger el acceso y servicios de red
- **Autenticación de usuarios para conexiones externas**: La empresa contempla servicios de conexiones seguras para usuarios que requieran conexión remota a la red de datos.
- **Identificación de equipos en la red:** La empresa controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.
- **Protección de los puertos de configuración y diagnóstico remoto**: Se debe considerar los siguientes aspectos:
  - Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estará restringido a los administradores de red o servidores.
  - Los usuarios finales deberán permitir tomar el control remoto de sus equipos para el Área de Soporte, teniendo en cuenta no tener archivos con información sensible a la vista, no desatender el equipo mientras que se tenga el control del equipo por un tercero.
  - Se deben implementar controles de acceso a nivel de puertos según los estándares tanto en las oficinas centralizadas, como en los sitios de teletrabajo.
- **Separación de redes**: Se deben considerar los siguientes aspectos:
  - La empresa utilizará dispositivos de seguridad "firewalls", para controlar el acceso de una red a otra.
  - La segmentación se realizará en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLANs en los equipos de comunicaciones.
  - Las redes inalámbricas no podrán conectarse a redes alámbricas.

- **Control de conexión de las redes**: Se deben considerar los siguientes aspectos:
    - Acotar la capacidad de descarga de los usuarios finales según las recomendaciones de los estándares vigentes
    - Implementar medidas de seguridad adecuadas para las conexiones WiFi.
    - Restringir el acceso a mensajería instantánea, telefonía a través de internet, correo electrónico comercial no autorizado, descarga de archivos de sitio peer to peer, conexiones a sitios de streaming no autorizado, acceso a sitios de pornografía, servicios de escritorio remoto a través de internet, cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de esta.
- **Control de enrutamiento de red:** El servicio de internet institucional será supervisado por el Oficial de Seguridad de Información y será el único servicio de internet autorizado.

7. Medidas de protección para activos de información

Los activos de información de la empresa deben contar con las medidas de protección adecuadas.

- **Protección contra agua y fuego:** Se deben considerar los siguientes aspectos:
    - Las instalaciones deben estar protegidas contra exposición al agua, en particular, las áreas de archivo deben estar distantes de zonas de filtración de agua o humedad.
    - Está prohibido generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones.
    - Se debe contar con extinguidores visibles y calibrados
    - Se debe preveer la copia de documentos y archivos electrónicos disponibles en ubicaciones seguras.
- **Protección de los archivos:** Se deben considerar los siguientes aspectos:
    - Los archivos físicos deben estar protegidos en áreas de archivo ad hoc, en contenedores de protección contra siniestros y agentes destructores y deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación.
    - Los archivos virtuales deben estar almacenados con copias de seguridad y medidas de protección adecuadas a su naturaleza y criticidad
    - Los archivos que requieran ser eliminados en su soporte físico o electrónico deberán ser borrados o destruidos de manera irrecuperable.
    - Una copia de los documentos y archivos electrónicos deben ser guardada en un lugar de contingencia protegida contra acceso no autorizado.

8. Gestión de roles

- **Roles de confianza:** Los roles de confianza deben ser definidos y asignados formalmente por la empresa.
- La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones.
- Los cambios en los documentos normativos requieren de la autorización de los responsables de TOC PERU SAC; los roles del Responsable de Seguridad y el Responsable de Privacidad, no son incompatibles y pueden ser asumidos por un mismo personal.
- Los roles de confianza deben emplear controles de acceso físico para el acceso a las áreas de archivo, así como lógicos. Los controles de acceso dependen de la configuración de los sistemas de TOC PERU.
- El auditor asignado por el INDECOPI deberá ser siempre una persona independiente de las operaciones de TOC PERU SAC.
- Los registros archivados y los registros de auditoría se mantienen durante el tiempo de validez de los certificados involucrados y se retienen por un período no inferior a 10 años.
- Las evaluaciones técnicas y de archivos del INDECOPI deberán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

9. Registro de auditorías al SID

- Las auditorías internas se llevarán a cabo al menos una vez al año.
- Las evaluaciones técnicas de INDECOPI se llevarán a cabo una vez al año y cada vez que INDECOPI lo requiera.
- Cualificación del Auditor: Para las actividades propias de las auditorías al Sistema de Intermediación Digital, el auditor debe estar autorizado por el INDECOPI para realizar sus funciones. Debe ser independiente de la empresa y no haber realizado trabajos relacionados con la actividad a auditar dentro de los dos años anteriores a la ejecución de la auditoría. Además, debe contar con experiencia en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas
- El registro de auditoría de eventos debe registrar la hora, fecha e identificadores software/hardware.
- Periodo de conservación del registro de auditorías: 10 años
- **Protección de los registros de auditoría:** Los registros estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.
- **Destrucción de un archivo de auditoría:** solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

10. Recuperación frente al compromiso y desastre

- TOC PERU mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones de intermediación digital, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade sus recursos y servicios.
- El plan asegura que los servicios de intermediación digital puedan ser reasumidos dentro de un plazo máximo de veinticuatro (24) horas.
- Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, juntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.
- La recuperación de los sistemas administrados por TOC PERU, incluyendo la disponibilidad de la plataforma de intermediación digital, será notificada por la empresa a sus usuarios mediante un mensaje de correo electrónico.
- Los registros archivados y los registros de auditoría se mantienen durante el tiempo de validez de los certificados involucrados y se retienen por un período no inferior a 10 años. TOC Perú SAC registra y guarda todos los logs de los eventos, incluyendo, al menos, los aspectos siguientes.
    - Registro de eventos de sistemas:
    - Encendido del sistema.
    - Apagado del sistema.
    - Registro de inicio y fin de sesión.
    - Registro de Intentos de accesos no autorizados
    - Registro de intentos de creación, modificación, borrado, establecimiento de contraseñas o cambio de privilegios.
    - Registro de generación de claves propias.
    - Registros de las aplicaciones
    - Encendido y apagado de las aplicaciones
    - Cambios en la configuración y mantenimiento del sistema.
    - Eventos del ciclo de vida de los certificados.
    - Registros de la destrucción de los medios que contienen las claves, datos de activación.
    - Registro de eventos tecnológicos:
    - Modificación y actualización en la política de seguridad de la información. Fallas e intermitencias del sistema.
    - Fallas del funcionamiento del hardware.
    - Registro de actividades en firewall, enrutadores y otros equipos de comunicaciones..
    - Mantenimiento, actualización y modificaciones en la configuración del sistema.
    - Informes de compromisos y discrepancias.
    - Registros de la destrucción de información de claves, datos de activación.

11. Confidencialidad de la información

La empresa mantiene de manera confidencial la siguiente información:

- Material comercial: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares y terceros en quien confían.
- Documentos propios de sus procedimientos internos
- Los datos personales de su personal, de sus clientes y de todo aquel tercero que confíe en sus servicios, incluyendo a los usuarios del Sitema de Intermediación Digital.

12. Control de versiones

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
1.0	Versión Inicial	Gerente General	Jefe de Operaciones	Líder del Comité de Riesgos	24/10/2025	24/10/2025
1.1	Actualización por versión 3 de IdentiaSign	Gerente General	Jefe de Operaciones	Líder del Comité de Riesgos	26/12/2025	26/12/2025