1. Introducción

La presente Política de Prevención de Lavado de Activos, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) tiene como objetivo orientar a los colaboradores, administradores y socios comerciales de Sencinet sobre los lineamientos adoptados para identificar, evaluar, prevenir y mitigar los riesgos asociados con estos delitos, garantizando que los negocios se desarrollen con los más altos estándares de ética, integridad y transparencia.

Para efectos de esta política, se adoptan los siguientes conceptos:

Lavado de Activos (LA): Proceso mediante el cual una persona oculta o disimula la naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes, derechos o valores provenientes, directa o indirectamente, de actividades delictivas, integrándolos a la economía formal con apariencia de legalidad.

Financiamiento del Terrorismo (FT): Suministro, recolección o administración de fondos, bienes o servicios, de origen lícito o ilícito, con la intención o conocimiento de que serán utilizados, total o parcialmente, para cometer actos terroristas o para apoyar a individuos u organizaciones terroristas.

Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM): Acto de proporcionar fondos o servicios financieros para la fabricación, adquisición, posesión, desarrollo, exportación, transbordo, transporte, transferencia o utilización de armas nucleares, químicas o biológicas y sus vectores, en contravención de las leyes nacionales y las obligaciones internacionales.

2. Objetivos

2.1. Establecer las directrices, principios y responsabilidades corporativas que orienten las acciones destinadas a consolidar la cultura de prevención y combate al LA/FT/FPADM.

2.2. Alinear a Sencinet con las mejores prácticas de control interno y cumplimiento regulatorio en los sectores y países donde opera la Compañía.

2.3. Monitorear proactivamente los cambios en el entorno regulatorio local e internacional, asegurando la rápida adaptación de las áreas de negocio a las nuevas obligaciones legales y códigos de autorregulación aplicables.

Copia No controlada si está impresa o descargada.
Por consideraciones ambientales evite imprimir este documento.

3. Directrices

3.1. Alcance de Aplicación

Esta política aplica íntegramente a todos los colaboradores (internos o externos), miembros de la administración, proveedores, prestadores de servicios, distribuidores y socios comerciales que actúen en nombre o en beneficio de Sencinet.

3.2. Compromiso de la Alta Dirección

El Consejo de Administración reafirma el compromiso institucional de Sencinet con el cumplimiento irrestricto de las leyes contra el lavado de activos y adopta una política de tolerancia cero frente al uso de la infraestructura, activos o productos de la empresa para fines ilícitos.

3.3. Cultura de Integridad

Todos los destinatarios de esta política deben actuar con ética y transparencia, absteniéndose de facilitar, tolerar u omitir transacciones que puedan representar indicios de delitos financieros, independientemente de que involucren agentes públicos o privados.

3.4. Cultura de Identificación y Reporte

Cualquier persona dentro o fuera de Sencinet, pero principalmente quienes hacen parte de las áreas Comercial, Financiera, Procurement, Logistica, Recursos Humanos, deberá informar a las áreas de Compliance y Legal, de manera inmediata, en caso de detectar:

a. Una operación sospechosa o inusual de un cliente, proveedor, empleado, aliado de negocio

b. Cliente, proveedor, empleado, aliado de negocio (empresa o persona) reportada en listas vinculantes o de control (Ejemplo OFAC, OEA...)

c. Cliente, proveedor, aliado de negocio con una persona políticamente expuesta dentro de su personal, accionistas y/o beneficiarios finales.

Las áreas de Compliance y Legal mediante la consolidación de información deberán evaluar las alertas a partir de los cuales se pueda inferir o advertir la existencia de situaciones que no se ajusten a las pautas de normalidad de nuestro sector o que puedan afectar la reputación de Sencinet.

Copia No controlada si está impresa o descargada.
Por consideraciones ambientales evite imprimir este documento.

3.5. Gestión de Riesgos

El riesgo de LA/FT/FPADM forma parte de la Matriz de Riesgos Corporativos de Sencinet. Este riesgo es revisado periódicamente y actualizado obligatoriamente siempre que se lancen nuevos productos, servicios, modelos de negocio o exista expansión hacia nuevas jurisdicciones geográficas.

4. Mecanismos de Control y Due Diligence

Sencinet adopta el principio de Enfoque Basado en Riesgos (EBR) para monitorear y evaluar sus relaciones comerciales mediante los siguientes programas:

4.1 Conozca a su Cliente y Socio (KYC / KYP)

Sencinet realiza la identificación, verificación y clasificación de riesgos de sus clientes, proveedores y socios antes de la contratación (Onboarding). El proceso incluye la recopilación de información corporativa consistente, la identificación del beneficiario final y la verificación reputacional.

4.2 Personas Políticamente Expuestas (PEPs)

Los procesos de Due Diligence prestan especial atención a la identificación de Personas Políticamente Expuestas (PEPs), sus familiares y asociados cercanos. Las relaciones comerciales con PEPs de alto riesgo o con indicios de enriquecimiento injustificado requieren monitoreo reforzado y aprobación previa del área de Compliance.

4.3 Conozca a su Empleado (KYE)

Los procesos de reclutamiento y selección incorporan verificaciones de antecedentes compatibles con la criticidad del puesto a desempeñar, mitigando riesgos internos.

4.4 Restricciones de Relacionamiento

Sencinet tiene estrictamente prohibido iniciar o mantener relaciones comerciales con contrapartes que posean antecedentes confirmados de actividades ilegales no subsanadas o que se encuentren incluidas en listas restrictivas de sanciones internacionales (por ejemplo: OFAC, Naciones Unidas o sanciones locales).

4.5 Prohibición de Pagos en Efectivo

Las transacciones financieras realizadas en efectivo presentan un alto nivel de riesgo y deben evitarse. Cualquier excepción operativa extraordinaria deberá contar con aprobación previa de las áreas Financiera y de Compliance, respetar estrictamente los límites legales aplicables y registrarse íntegramente en los libros contables de la Compañía.

Copia No controlada si está impresa o descargada.
Por consideraciones ambientales evite imprimir este documento.

5. Monitoreo, Comunicación y Gobernanza

5.1 Rol de Compliance

El área de Compliance es responsable del diseño, monitoreo y actualización de los controles internos relacionados con LA/FT/FPADM, reportando periódicamente a la Alta Dirección sobre el desempeño de las áreas críticas con respecto a la política y los controles establecidos y/o cualquier señal de alerta u operación sospechosa identificada.

5.2 Identificación de Operaciones Sospechosas

Sencinet mantiene un monitoreo constante de sus transacciones financieras. Se consideran señales de alerta (*red flags*), entre otras, el fraccionamiento excesivo de pagos, la triangulación de cuentas sin justificación económica y la incongruencia entre la actividad económica de la contraparte y la operación realizada.

5.3 Reporte a las Autoridades

Las operaciones identificadas como sospechosas, luego de la debida investigación interna y validación por parte del Comité de Ética, serán reportadas a las Unidades de Inteligencia Financiera competentes de cada país (por ejemplo: COAF en Brasil, UIAF en Colombia), dentro de los plazos legales aplicables.

5.4 Deber de Confidencialidad (Anti-Tipping Off)

Los análisis y comunicaciones de operaciones sospechosas a las autoridades gubernamentales tienen carácter estrictamente confidencial. Está prohibido informar a terceros o a las personas involucradas sobre investigaciones o reportes realizados.

5.5 Auditoría

Los procedimientos y controles de LA/FT/FPADM son auditados periódicamente de forma independiente por Auditoría Interna y por auditores externos independientes.

5.6 Capacitación Continua

Todos los colaboradores que desempeñen funciones en áreas críticas orientadas a garantizar el cumplimiento de los controles internos (Finanzas, Comercial, Procurement, Logistica, Recursos Humanos) deberán participar periódicamente en capacitaciones obligatorias liberadas por el área de Compliance, sobre identificación de riesgos de lavado de activos y utilización de los canales de denuncia.

6. Canales de Reporte y Consecuencias

Copia No controlada si está impresa o descargada.
Por consideraciones ambientales evite imprimir este documento.

6.1 Canal de Denuncias

Las sospechas fundamentadas, desviaciones o incumplimientos de esta política deben ser reportadas inmediatamente a través del Canal Oficial de Denuncias de Sencinet:

Correo electrónico: yourvoice@sencinet.com

Sencinet garantiza la absoluta confidencialidad, el anonimato (cuando sea solicitado) y la no represalia contra cualquier denunciante que actúe de buena fe.

6.2 Consultas de Compliance

Las consultas relacionadas con la interpretación o aplicación práctica de esta política deben dirigirse al correo electrónico: **askcompliance@sencinet.com**

6.3 Régimen Disciplinario y Sanciones

El incumplimiento de las disposiciones de esta política sujetará al infractor a medidas disciplinarias que podrán variar desde advertencias hasta el despido con justa causa, de conformidad con la legislación laboral local aplicable. En el caso de terceros y socios comerciales, podrá dar lugar a la terminación inmediata del contrato por incumplimiento de obligaciones de Compliance, sin perjuicio de la reclamación por daños y perjuicios y de las comunicaciones penales o civiles pertinentes ante las autoridades competentes.

7. Historial de revisiones

Versión	Fecha	Autor(es)	Contenido revisado
1	11/05/2022	Patricia Gazzineo	Creación del documento. Esta Política reemplaza la Política de Lavado de Activos.
2	28/05/2024	Angela Luque/Julia Limas	Cambio de autor y aprobador. Revisión y ajuste de áreas responsables
3	05/08/2026	Julia Limas/Alessandra Tsai	**Actualización general de cumplimiento:** estandarización de las siglas PEPs; eliminación de redundancias textuales y estructuración de rutinas KYC/KYP/KYE; inclusión de la norma de confidencialidad; fortalecimiento de sanciones y monitorización basada en riesgos.