



ISVI LTDA., como empresa de vigilancia y seguridad privada, establece esta política para planificar, ejecutar, controlar, evaluar y mejorar sus operaciones de seguridad; proteger la vida, la dignidad, los derechos humanos, los activos, la información y la infraestructura; asegurar la resiliencia de la cadena de suministro; y prevenir, detectar y responder frente al soborno, el fraude, la corrupción y demás conductas contrarias a la integridad.

La Alta Dirección adopta una postura de cero tolerancia frente al soborno y respalda visiblemente esta política, asignando los recursos, las competencias, la autoridad y la independencia requeridos para su implementación y mantenimiento.

Esta política aplica a todas las actividades, procesos, sedes, proyectos y servicios incluidos en el alcance del Sistema Integrado de Gestión de ISVI LTDA., así como a las operaciones desarrolladas para clientes públicos y privados de los diferentes sectores económicos atendidos por la organización.

Es obligatoria para socios, órgano de gobierno, Alta Dirección, directores, supervisores, inspectores, vigilantes, escoltas y demás colaboradores; y, según corresponda al riesgo y a la relación contractual, para clientes, proveedores, contratistas, subcontratistas, aliados estratégicos, socios comerciales, visitantes y terceros que actúen en nombre, representación o beneficio de ISVI LTDA., o que administren, custodien o utilicen activos propios o de clientes.

Principios y compromisos integrales

- **Legalidad y requisitos aplicables.** Cumplir la legislación y regulación aplicable, las obligaciones contractuales, los compromisos voluntarios asumidos y los demás requisitos relacionados con operaciones de seguridad, cadena de suministro, derechos humanos, control de activos y prevención del soborno.
- **Gestión basada en riesgos.** Identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos y oportunidades de las operaciones de seguridad, la cadena de suministro y el soborno; mantener análisis vigentes por puesto, proceso, sede, proyecto, socio comercial y actividad, conforme al nivel de riesgo.
- **Derechos humanos.** Respetar la dignidad, la vida y los derechos humanos; evitar, prevenir y reducir la probabilidad y las consecuencias de eventos no deseables o perturbadores; y disponer mecanismos accesibles, confidenciales y sin represalias para quejas y reclamaciones.
- **Uso de la fuerza.** Aplicar los principios de legalidad, necesidad, proporcionalidad, precaución y rendición de cuentas, privilegiando la prevención, el diálogo y el desescalamiento. Todo evento será reportado, revisado e investigado según corresponda.
- **Continuidad y resiliencia.** Mantener capacidades, planes, recursos, ejercicios y pruebas para prevenir, responder, recuperar y aprender de incidentes que afecten los servicios, activos o la cadena de suministro.
- **Protección y custodia de activos:** Proteger y custodiar los activos propios, de clientes o de terceros que sean formalmente entregados o puestos bajo la responsabilidad de ISVI LTDA., aplicando los controles de seguridad establecidos para prevenir su pérdida, daño, alteración, uso indebido o acceso no autorizado y preservar su integridad durante el tiempo que permanezcan bajo su custodia.



- **Seguridad de la cadena de suministro:** Prevenir y tratar amenazas como hurto, fraude, soborno, corrupción, extorsión, terrorismo, sabotaje, crimen organizado, narcotráfico, contrabando, contaminación de carga, ciberataques y accesos no autorizados. Los proveedores críticos serán evaluados y sujetos a acuerdos y controles de seguridad proporcionales al riesgo.
- **Evaluación de impactos.** Considerar los posibles impactos adversos que la política, los objetivos, las metas, los controles y los programas de seguridad puedan generar sobre las personas, los clientes, los requisitos legales y contractuales, los derechos humanos, el ambiente, la seguridad y salud en el trabajo, la continuidad del negocio, la cadena de suministro, las finanzas, la integridad y la reputación de ISVI LTDA.
- **Seguridad de la información.** Controlar el acceso físico y lógico y proteger el intercambio de información con clientes, proveedores, autoridades y demás partes autorizadas, de acuerdo con requisitos legales, contractuales y de protección de datos.
- **Prevención del soborno y fraude.** Prohibir el soborno directo o indirecto, en cualquier forma y cuantía, incluido ofrecer, prometer, entregar, solicitar o aceptar ventajas indebidas. También se prohíben fraude, apropiación indebida, pagos de facilitación, comisiones ilícitas, extorsión, colusión, registros falsos, ocultamiento y conflictos de interés no declarados.
- **Controles antisoborno.** Aplicar debida diligencia basada en riesgo y controles financieros y no financieros sobre transacciones, compras, pagos, donaciones, patrocinios, regalos, hospitalidad, contratación, socios comerciales y decisiones con exposición a soborno. Ninguna meta comercial justifica incumplir esta política.
- **Planteamiento de inquietudes.** Promover reportes de buena fe o basados en una creencia razonable, confidenciales o anónimos cuando esté permitido, sin temor a represalias. Toda denuncia será recibida, protegida, analizada e investigada de manera oportuna, independiente, imparcial y trazable.
- **Competencia y cultura.** Seleccionar personal competente y proporcionar inducción, formación, sensibilización y reentrenamiento según riesgos, incluidos uso de la fuerza, derechos humanos, seguridad de la cadena, custodia de activos, integridad y antisoborno.
- **Gestión de incidentes.** Reportar, contener, documentar, investigar y tratar incidentes operacionales, de cadena, de activos, derechos humanos, fraude o soborno; determinar causas y establecer correcciones, acciones correctivas y verificación de eficacia.
- **Ambiente y SST.** Mantener activos y equipos seguros, promover su uso responsable y gestionar los residuos derivados del mantenimiento, reposición o disposición final, previniendo lesiones, enfermedades e impactos ambientales.
- **Mejora continua.** Medir el desempeño, verificar controles, realizar auditorías, revisar esta política y mejorar continuamente los sistemas de gestión de operaciones de seguridad, seguridad de la cadena de suministro y antisoborno.

Armamento, dotación y medios tecnológicos

Los servicios se prestarán con o sin armas de fuego y con los elementos de protección, defensa, comunicación y medios tecnológicos autorizados, definidos según la evaluación de riesgos, los requisitos contractuales y la normativa aplicable. El armamento y las municiones deberán estar legalmente autorizados, registrados, asignados, almacenados, transportados y controlados. Se prohíbe el uso de armas personales, no autorizadas o modificadas.



El personal autorizado recibirá capacitación y reentrenamiento periódico en manejo seguro, prevención, desescalamiento y uso proporcional de la fuerza. Los servicios sin armas dispondrán de la dotación y los medios autorizados establecidos para cada operación.

Roles, responsabilidades y autoridades

Órgano de gobierno y Alta Dirección: Asumir la responsabilidad general por la implementación y el cumplimiento; aprobar y respaldar la política; asegurar su integración en los procesos; asignar recursos; revisar el desempeño; exigir su aplicación en todos los niveles y respaldar a quien rechace participar en soborno, aun si ello ocasiona la pérdida de una oportunidad de negocio.

Directores y líderes de proceso: Implementar los requisitos y controles en su proceso; asignar y comunicar responsabilidades; gestionar riesgos; asegurar competencias y recursos; verificar la eficacia; reportar desempeño, incidentes, incumplimientos y oportunidades de mejora; y gestionar conflictos de interés.

Responsable del SGOS / Dirección SIG: Asegurar que el sistema de gestión de operaciones de seguridad se establezca, implemente, mantenga y mejore; monitorear necesidades y expectativas de partes interesadas; promover conciencia; informar su desempeño a la Alta Dirección y coordinar acciones sin desplazar la responsabilidad operativa de los líderes.

Oficial de Cumplimiento / función antisoborno: Supervisar el diseño, implementación, cumplimiento y mejora del sistema antisoborno; asesorar; vigilar riesgos y debida diligencia; gestionar o supervisar denuncias e investigaciones; e informar directamente al órgano de gobierno y a la Alta Dirección. Actuará con competencia, autoridad, independencia, recursos y acceso directo, sin interferencias ni represalias.

Operaciones, supervisores, inspectores, vigilantes y escoltas: Cumplir consignas y controles; proteger personas y activos; aplicar los principios de uso de la fuerza; mantener registros; reportar novedades, incidentes y riesgos; preservar evidencias y participar en entrenamientos, ejercicios e investigaciones.

Gestión administrativa y financiera: Solicitar al proceso competente la realización de la debida diligencia de proveedores, contratistas y demás terceros, según su nivel de riesgo; implementar la segregación de funciones, los niveles de autorización, los registros contables exactos, las conciliaciones y los controles financieros y no financieros; y prevenir el fraccionamiento de compras, los pagos, transacciones o disposiciones de activos no autorizados.

Todo el personal y terceros pertinentes: Conocer, cumplir y aplicar esta política en lo relativo a su rol; proteger activos e información; declarar conflictos de interés; cooperar con verificaciones e investigaciones; y reportar de buena fe riesgos, incidentes, sospechas o incumplimientos.

Los objetivos se despliegan en la planificación del Sistema Integrado de Gestión.

Esta política se mantendrá disponible como información documentada, será comunicada, explicada y entendida dentro de la organización y por las personas que trabajen para ella o en su nombre, y estará disponible para las partes interesadas pertinentes, según corresponda.



**POLÍTICA INTEGRAL DE OPERACIONES DE
SEGURIDAD, CADENA DE SUMINISTRO,
CUSTODIA DE ACTIVOS Y ANTISOBORNO**

CÓDIGO: DI-SIG-16

FECHA: 21-JUL-2026

VERSIÓN: 01

Página 4 de 4

La política será comunicada a los socios comerciales que presenten un nivel de riesgo de soborno superior a bajo y, cuando corresponda, a aquellos cuya relación contractual, actividad o controles establecidos requieran su conocimiento, aceptación y cumplimiento. La organización promoverá la consulta, participación y retroalimentación mediante los canales definidos.

Se prohíbe cualquier represalia, amenaza, discriminación o perjuicio contra quien se niegue a participar en soborno o reporte de buena fe una inquietud, incluso si no se confirma posteriormente, siempre que no haya actuado de mala fe. La confidencialidad, la presunción de inocencia, el debido proceso y la protección de datos se preservarán durante el tratamiento de reportes e investigaciones.

El incumplimiento podrá generar medidas disciplinarias, administrativas y contractuales, terminación de vínculos, reclamación de daños y denuncias ante autoridades, según la gravedad, el debido proceso y la legislación aplicable, sin perjuicio de las responsabilidades civiles o penales correspondientes.

La política será revisada como mínimo una vez al año y cuando existan cambios significativos legales, normativos, contractuales, organizacionales, tecnológicos, operativos, de contexto, de riesgos, adquisiciones o fusiones que puedan afectar la continuidad, relevancia o eficacia de los sistemas de gestión. La revisión considerará resultados de indicadores, incidentes, quejas, denuncias, auditorías, ejercicios, evaluación de controles y revisión por la dirección.

La presente Política se firma el 21 de julio de 2026 y entra en vigor a partir de su aprobación. Se mantendrá disponible como información documentada, será comunicada y entendida en todos los niveles de la organización y estará disponible para las partes interesadas pertinentes



JOSÉ AMORTEQUI
Presidente Ejecutivo