1. OBJETIVO

Establecer los lineamientos de la **Gestión de la Seguridad** en la cadena de suministro de la empresa, asegurando la **prevención, control y mitigación de riesgos** relacionados con las operaciones de seguridad física y electrónica, garantizando la **confianza de clientes, colaboradores, proveedores y autoridades** en cumplimiento con la normativa legal vigente en Panamá y con los requisitos de la Norma **ISO 28000:2022**.

2. ALCANCE

La presente política aplica a todas las **operaciones, procesos, instalaciones, personal, contratistas y proveedores** vinculados con la prestación de servicios de:

- Seguridad física en instalaciones, patrullajes y custodia de activos.
- Seguridad electrónica (CCTV, alarmas, sistemas de acceso y monitoreo).
- Transporte, almacenamiento e instalación de equipos de seguridad.
- Procesos administrativos y de soporte relacionados.

3. RESPONSABILIDAD Y AUTORIDAD

- **Gerencia General:** Aprobar, difundir y garantizar la aplicación de esta política.
- **Responsable del Sistema de Gestión de Seguridad (SGS):** Asegurar la implementación, seguimiento y mejora continua del sistema conforme a ISO 28000.
- **Mandos Operativos (supervisores y jefes de área):** Aplicar los procedimientos de seguridad y controlar su cumplimiento en campo.
- **Colaboradores:** Cumplir con las políticas, procedimientos y capacitaciones recibidas, reportando cualquier incidente, amenaza o vulnerabilidad.
- **Proveedores y contratistas:** Cumplir con los requisitos de seguridad establecidos por la empresa y la legislación nacional.

4. DESCRIPCION DE ACTIVIDADES

1. Identificación y evaluación de riesgos en la cadena de suministro

- Realizar un **análisis de riesgos** en todas las etapas de la cadena (adquisición, transporte, almacenamiento, instalación y operación).
- Utilizar **metodologías de evaluación** (matriz de probabilidad e impacto, análisis de escenarios).
- Identificar amenazas como: robo, vandalismo, fallas tecnológicas, ciberataques, desastres naturales, corrupción, entre otros.
- Priorizar los riesgos con base en su nivel de criticidad.

- Documentar los resultados en una **Matriz de Riesgos y Oportunidades** y definir controles.

2. Cumplimiento normativo en materia de seguridad privada, laboral, ambiental y de protección de datos

- Asegurar que la empresa cuenta con **licencias vigentes** de seguridad privada (emitidas por el Ministerio de Seguridad Pública de Panamá).
- Cumplir con la **legislación laboral** (salarios, jornadas, EPP, salud ocupacional).
- Implementar prácticas de **gestión ambiental** (manejo de residuos electrónicos, baterías, cables, combustible).
- Cumplir con la **Ley 81 de 2019 de Protección de Datos Personales en Panamá**.
- Mantener un **registro de requisitos legales aplicables** y verificar periódicamente su cumplimiento.

3. Capacitación y concienciación del personal en seguridad física, cibernética y ambiental

- Diseñar un **plan anual de capacitación** que incluya:
  - Seguridad física (protocolos, reacción ante incidentes, autoprotección).
  - Seguridad cibernética (uso responsable de sistemas, manejo de contraseñas, prevención de phishing).
  - Gestión ambiental (reciclaje, reducción de residuos, control de emisiones).
- Realizar **simulacros periódicos** de emergencias y amenazas.
- Evaluar la eficacia de las capacitaciones mediante encuestas, exámenes o auditorías internas.

4. Control de accesos físicos y electrónicos en instalaciones y equipos

- Implementar **sistemas de control de acceso** en oficinas, bodegas y centros de monitoreo (tarjetas, biometría, CCTV).
- Establecer un **registro de visitas** y personal autorizado.
- Monitorear en tiempo real las instalaciones con cámaras y alarmas.
- Proteger equipos y vehículos con dispositivos electrónicos (rastreo GPS, sensores de apertura).
- Revisar y actualizar periódicamente los **perfiles de acceso** de los empleados.

5. Protección de la información sensible de clientes y operaciones

- Clasificar la información como **confidencial, restringida y pública**.
- Implementar **protocolos de seguridad digital**: firewalls, antivirus, sistemas de respaldo, cifrado de datos.
- Establecer **políticas de uso de correo corporativo y dispositivos móviles**.
- Controlar el acceso a la información mediante **roles y permisos**.
- Realizar auditorías de seguridad informática y pruebas de vulnerabilidad.

6. Gestión de incidentes y emergencias, incluyendo planes de contingencia

- Elaborar un **Plan de Respuesta a Emergencias** que contemple: asaltos, incendios, desastres naturales, sabotajes, fallas tecnológicas.
- Definir una **cadena de mando** para la atención de incidentes.
- Contar con **protocolos de comunicación interna y externa** en caso de crisis.
- Realizar **simulacros periódicos** (al menos semestrales).
- Evaluar y documentar cada incidente para generar **acciones correctivas**.

7. Monitoreo y auditoría interna del sistema de gestión

- Definir **indicadores de desempeño en seguridad** (ej.: % de incidentes atendidos, tiempo de respuesta, cumplimiento de capacitación).
- Realizar **auditorías internas** al menos una vez al año para verificar el cumplimiento de procedimientos y controles.
- Utilizar **sistemas de monitoreo en tiempo real** para operaciones críticas (vehículos, instalaciones, clientes).
- Documentar hallazgos y generar **planes de acción correctiva**.

8. Relación y cooperación con autoridades competentes en materia de seguridad y cumplimiento legal

- Mantener comunicación activa con: Ministerio de Seguridad, Policía Nacional, SINAPROC, Ministerio de Ambiente, Autoridad de Innovación Gubernamental (para temas digitales).
- Participar en **programas de cooperación público-privada** de seguridad.
- Reportar incidentes que involucren delitos o riesgos graves.
- Establecer **protocolos de coordinación** con autoridades en caso de crisis.

9. Mejora continua del desempeño en seguridad mediante indicadores, auditorías y revisión por la dirección

- Aplicar el **ciclo PHVA (Planificar – Hacer – Verificar – Actuar)** en todas las operaciones.
- Establecer **indicadores clave de seguridad** (ej.: reducción de robos, tiempos de respuesta, cumplimiento normativo, satisfacción del cliente).
- Realizar **revisión por la dirección** al menos una vez al año para evaluar la eficacia del sistema.
- Promover la innovación tecnológica (IA en monitoreo, sistemas verdes, ciberseguridad avanzada).
- Documentar las lecciones aprendidas y difundirlas en la organización.

4.1 Indicadores de Gestión:

A. Indicadores Operacionales

Objetivo: Promover prácticas de gestión de operaciones que reduzcan los tiempos de respuesta optimizando las labores diarias y prestando un servicio de calidad a los clientes.

Estrategias y Actividades

1. **Control de Número de Incidentes**

- **Actividad:** Llevar la estadística del número de incidentes que puedan ocasionar la interrupción del servicio
- **Medible:** Cantidad de incidentes reportados vs puestos de trabajo.
- **Indicador:** Cantidad de Incidentes vs puestos de trabajo en porcentaje **(meta: 30%) .**

2. **Control de tiempo de Respuesta a Incidentes Reportados**

- **Actividad:** Llevar la estadística del tiempo de respuesta ante un incidente de Base Control que puedan ocasionar la interrupción del servicio
- **Medible:** Cantidad de minutos empleados en la reacción de Base Control entre el número de incidentes.
- **Indicador:** Cantidad de minutos vs eventos en porcentaje **(meta: 5 minutos por evento) .**

3. **Control de tiempo de Respuesta para resolver los Incidentes Reportados**

- **Actividad:** Llevar la estadística del tiempo de respuesta desde su inicio hasta la resolución del evento disruptivo que puedan ocasionar la interrupción del servicio
- **Medible:** Cantidad de minutos empleados en la resolución por el operador de Base Control entre el número de incidentes.
- **Indicador:** Cantidad de minutos vs eventos en porcentaje **(meta: 30 minutos por evento) .**

5. DEFINICIONES

- **SGS (Sistema de Gestión de Seguridad):** Conjunto de políticas, procesos y controles implementados para cumplir con la norma ISO 28000.
- **Cadena de suministro:** Conjunto de actividades relacionadas con la adquisición, transporte, almacenamiento, instalación y operación de bienes y servicios de seguridad.
- **Riesgo de seguridad:** Posibilidad de que un evento afecte negativamente la continuidad de las operaciones, la integridad de las personas, la información o los activos.
- **Incidente de seguridad:** Evento no planificado que interrumpe o puede interrumpir la operación normal del servicio.
- **Mejora continua:** Proceso de optimización permanente del sistema de gestión mediante la revisión y actualización de sus controles.

6. REFERENCIAS

- Norma ISO 28000-2022

7. REGISTROS.

- USG-CA-F-002 Lista Maestra de Documentos
- USG-CA-F-003 Lista Maestra de Documentos Externos

8. ANEXOS

- USG-CA-F-002 Lista Maestra de Documentos
- USG-CA-F-003 Lista Maestra de Documentos Externos

9- CONTROL DE REVISIONES

N° de Rev.	Fecha	Descripción del Cambio	# Pag.	Elaborado Por: Fecha:	Revisado Por: Fecha:	Aprobado Por: Fecha:
00	27-jul-25	Emisión Original		Jorge Castillo 27-jul-25	Alexis Aldazoro 27-jul-25	Antonio Quintero 27-jul-25