

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

PL - GTI - 10 - POLÍTICA GENERAL SEGURIDAD DE LA INFORMACIÓN

Versión 4

20/11/2025

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

1. OBJETIVO

Documentar la importancia para la Alta Dirección de identificar y proteger los activos de información de Sofka, por lo cual se compromete a desarrollar, implementar, mantener, mejorar de forma continua un Sistema de Gestión de Seguridad de la Información - SGSI y asegurar el cumplimiento de los requisitos de la norma internacional **ISO/IEC 27001:2022**, así como la legislación y regulaciones aplicables, incluyendo aquellas relativas a la privacidad de datos.

2. ALCANCE

Inicia con la necesidad de establecer una política general de Seguridad de la Información para el SGSI de Sofka, es de obligatorio cumplimiento en todos los procesos, por los trabajadores, terceros y cualquier persona que preste servicios y/o tenga acceso a los activos de información.

3. RESPONSABLES

Alta Dirección, Oficial de Seguridad

4. DEFINICIONES

- **Confidencialidad:** Indica que la información o el activo de información solo debe ser accedida por quien está autorizado, ocultando o manteniendo su condición de ser secreta o sensible.
- **Disponibilidad:** La información o el activo de información debe estar disponible cuando y donde sea necesario, no se debe degradar el acceso.
- **Integridad:** La información o el activo de información debe permanecer inalterada ante accidentes o intentos maliciosos y solo las personas autorizadas la pueden modificar.
- **RIT:** Reglamento Interno de Trabajo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

5. CONTENIDO

5.1. Política

Sofka S.A.S es una compañía dedicada a transformar la vida de las personas siendo el aliado tecnológico más confiable, reconoce la información como activo fundamental para la operación de los servicios con cliente, a nivel interno y la toma de decisiones.

Para esto se soporta en la definición de procesos y la seguridad de la información, con la definición e implementación de un conjunto de controles, tales como **políticas, procedimientos, estructuras, software e infraestructura**, para la preservación de la confidencialidad, integridad y disponibilidad de la información.

La Alta dirección de sofka aprueba esta política como parte de su compromiso para el cumplimiento de los requisitos para el Sistema de Gestión de Seguridad de la Información, junto a la adopción de buenas prácticas para garantizar las confidencialidad, integridad y disponibilidad de la información de la organización, Sofkian@s, clientes y terceros involucrados en el desarrollo de las labores.

5.2. Compromiso de la Alta Dirección

La Alta Dirección de sofka, evidencia su continuo compromiso con el SGSI de la siguiente manera:

- Asignando recursos para el desarrollo de las iniciativas orientadas a la implementación de Seguridad de la información y Ciberseguridad.
- Definiendo y asignando la responsabilidad para la gestión de la seguridad de la información en la organización.
- Apoyando y promoviendo una cultura de seguridad de la información y ciberseguridad, con la divulgación y recordación de las políticas y lineamientos de seguridad de la información y ciberseguridad.
- Promoviendo el cumplimiento de los objetivos de seguridad de la información, buenas prácticas de seguridad y ciberseguridad en la entrega de los servicios al cliente, como parte de la mejora continua del SGSI.

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

- Participando de los espacios definidos para el monitoreo del desempeño del SGSI.
- Definiendo y revisando periódicamente la metodología, el apetito al riesgo y los criterios de aceptación del riesgo para la evaluación y el tratamiento de riesgos de seguridad, implementando las acciones necesarias para su mitigación y mejora continua.

5.3. Lineamientos Generales

- Se deben definir objetivos de seguridad de la información en funciones y niveles pertinentes
- Todos los sof kian@s deben proteger y asegurar la información dando cumplimiento a las políticas definidas para la seguridad de la información y ciberseguridad.
- Se deberá realizar la clasificación, el etiquetado y el manejo seguro de los activos y/o información, de acuerdo a los criterios de valoración de la Confidencialidad, Integridad y Disponibilidad (CID). Estos criterios y sus niveles se encuentran definidos en el *PD_GT104 Procedimiento Etiquetado y Manejo de Información*.
- Los Sofkian@s y terceros con acceso a los activos de información, somos responsables de reportar eventos o incidentes materializados que afecten la confidencialidad, integridad y/o disponibilidad de la información, a través de los canales definidos por Sofka.
- Se deben desarrollar programas de concienciación y formación sobre las políticas y procedimientos en materia de seguridad de la información y ciberseguridad, al personal interno y externo con acceso a información de la organización.
- Todos los Sofkian@s deben participar de las actividades de concienciación y desarrollar el curso del SGSI a su ingreso y renovar la ejecución del mismo cada vez que se cumple un año.

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

- El incumplimiento de la presente política o políticas complementarias del SGSI será tramitado como una falta de acuerdo a las definiciones del RIT de Sofka.
- Esta política debe ser revisada o actualizada por lo menos una vez al año.

5.4. Ciberseguridad y Adopción de Inteligencia Artificial (IA)

Sofka reconoce que la IA es un pilar estratégico, por lo que su adopción debe ser segura. Los siguientes lineamientos aplican al uso y desarrollo de sistemas de IA/ML:

- Como buena práctica todo *dataset* utilizado para el entrenamiento, prueba o validación de modelos de IA deberá ser evaluado bajo los criterios de Confidencialidad, Integridad y Disponibilidad (CID). Si el *dataset* contiene información clasificada como Confidencial o Restringida, el Propietario del Dato debe aplicar un proceso de anonimización o tokenización, o bien obtener la aprobación explícita antes de su uso en el modelo, para mitigar el riesgo de fuga de información.
- El Modelo de IA y sus resultados generados deben heredar por defecto la clasificación de Confidencialidad más alta de los datos de entrada, salvo que el Propietario del Modelo apruebe formalmente una reclasificación inferior tras una Evaluación de Riesgos de Reidentificación.
- Se priorizará el uso de herramientas basadas en IA/ML para la detección de anomalías, el análisis predictivo de amenazas y la automatización de la respuesta a incidentes, como parte de la mejora continua del SGSI.

	Política General Seguridad de la Información	Código:	PL_GT110
		Versión:	4
		Fecha:	20/11/2025
		Acceso:	Público

6. CONTROL DE CAMBIOS

Versión	Descripción del Cambio	Realizado por	Fecha
1	Creación del documento	Gerente de Seguridad de la Información	27/02/2024
2	- Se realizan ajustes de acuerdo a lineamientos de nueva marca. - Se modifica el nivel de acceso, cambiando de interno a público.	Analista de procesos	30/10/2024
3	Se actualiza política de acuerdo a las observaciones recibidas durante la Etapa 1 de auditoria de otorgamiento	Líder de Seguridad de la Información	20/11/2024
4	Se actualiza la política y se incorpora el numeral 5.4 'Ciberseguridad y Adopción de Inteligencia Artificial (IA)'.	Líder de Seguridad de la Información	20/11/2025

7. ANEXOS

[Site de Seguridad de la Información](#)

CONFIDENCIALIDAD: La información contenida en este documento es confidencial y de propiedad exclusiva de SOFKA. Se comparte únicamente con el destinatario autorizado y no puede ser divulgada, reproducida ni utilizada para ningún propósito distinto al autorizado sin el consentimiento previo y por escrito de SOFKA. Cualquier acceso, uso, distribución o divulgación no autorizada de este documento podrá estar sujeta a acciones legales conforme con las Leyes legales aplicables en la República de Colombia.

Si ha recibido este documento por error, le solicitamos que lo notifique de inmediato a SGSI@sofka.com.co y proceda a su eliminación definitiva.