



**SIGDO KOPPERS S.A.**

**POLITICA DE SEGURIDAD DE  
LA INFORMACIÓN**

Contraloría Corporativa

JUNIO 2025

	POLITICA CORPORATIVA	Código	IT_POL_HSK_SI_01_2025
	<b>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</b> Contraloría Corporativa	Versión	01
		Fecha Emisión	27-06-2025
		Estado	Aprobada

## CONTENIDO

1.	<b>INTRODUCCIÓN</b> .....	<b>2</b>
2.	<b>ALCANCE</b> .....	<b>2</b>
3.	<b>DEFINICIONES</b> .....	<b>3</b>
4.	<b>POLÍTICA GENERAL</b> .....	<b>3</b>
5.	<b>VIGENCIA</b> .....	<b>4</b>
6.	<b>CONTROL DE CAMBIOS</b> .....	<b>4</b>

### 1. INTRODUCCIÓN

El presente documento tiene como objetivo establecer los lineamientos principales de protección de la información y sistemas de información utilizados en Sigdo Koppers S.A. y sus filiales bajo el alcance de Ciberseguridad y Seguridad de la Información.

### 2. ALCANCE

La Política de Seguridad de la Información establece el marco común de acción de la compañía y todas sus empresas filiales, por tanto, todos los colaboradores y compañías del Grupo son responsables de garantizar el cumplimiento del documento establecido.

### 3. DOCUMENTOS RELACIONADOS

Los documentos referenciados a esta política son los siguientes:

- Política de Gestión de Seguridad Sigdo Koppers S.A.

	POLITICA CORPORATIVA	Código	IT_POL_HSK_SI_01_2025
	<b>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</b> Contraloría Corporativa	Versión	01
		Fecha Emisión	27-06-2025
		Estado	Aprobada

#### 4. DEFINICIONES

**Información:** La información es el conjunto de datos o hechos presentados, comunicados o registrados en distintos formatos y medios, como la comunicación oral, documentos escritos y medios electrónicos. Puede almacenarse y recuperarse en diversas formas, incluyendo datos digitales, informes generados por computadora, correos electrónicos, mensajes de voz, minutas de reuniones y documentos de trabajo entre otros.

**Sistema de Información:** Un sistema de información es un conjunto de componentes que facilitan el procesamiento de información. Incluye dispositivos como teléfonos móviles, tablets, computadoras y dispositivos de almacenamiento, así como hardware y software, servidores, sistemas operativos, activos virtuales, bases de datos, redes y aplicaciones.

**Ciberseguridad:** Es el conjunto de prácticas, herramientas y sistemas diseñados para proteger la información y los sistemas de información frente a accesos no autorizados, ataques, daños o interrupciones. Abarca la protección de distintos dispositivos tales como computadores, servidores, redes, aplicaciones y bases de datos, entre otros.

**Seguridad de la Información:** Conjunto de prácticas, políticas y controles destinados a proteger la información en todos sus formatos contra accesos no autorizados, alteraciones, divulgaciones y pérdidas.

**Amenaza:** Es cualquier evento o agente que pueda afectar la seguridad de la información, ya sea por intención maliciosa (como un ciberataque) o de manera accidental (como un desastre natural), poniendo en riesgo su confidencialidad, integridad y/o disponibilidad.

**Vulnerabilidad:** Debilidad de un sistema, proceso o control que puede ser aprovechada por una amenaza, poniendo en riesgo la seguridad de la información.

#### 5. POLÍTICA GENERAL

- 1) SK Converge es responsable de establecer la gobernanza y lineamientos estratégicos en materia de seguridad de la información y ciberseguridad, mientras que cada empresa del Grupo Sigdo Koppers es responsable de implementar este plan estratégico en el contexto de su propio negocio.
- 2) Se fomenta una cultura de ciberseguridad y seguridad de la información entre los colaboradores, proporcionando programas de formación, concientización y material informativo sobre buenas prácticas de seguridad, además de alertar sobre posibles ataques.
- 3) Se diseñan e implementan planes de respuesta a incidentes, estableciendo que todo colaborador que tenga conocimiento de un hecho que comprometa la seguridad de la información debe reportarlo a través de los canales de escalamiento definidos. De esta manera, se busca garantizar la continuidad del negocio, además de establecer protocolos claros de comunicación con los responsables internos y autoridades competentes.

	<b>POLITICA CORPORATIVA</b>  <b>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</b>  Contraloría Corporativa	Código	IT_POL_HSK_SI_01_2025
		Versión	01
		Fecha Emisión	27-06-2025
		Estado	Aprobada

- 4) La información y los sistemas de información utilizados en el Grupo Sigdo Koppers para almacenar y procesar esta información son protegidos bajo las herramientas disponibles, con el fin de preservar la confidencialidad, integridad y disponibilidad, ya sea de forma oral, escrita o digital.
- 5) Se evalúan amenazas y vulnerabilidades con el fin de prevenir y detectar cualquier evento no deseado, y en conjunto con las áreas dueñas del proceso, se implementará un conjunto de controles de seguridad para reducir su probabilidad de ocurrencia.
- 6) Tanto los colaboradores, como contratistas y cualquier otro organismo que trabaje con información y sistemas de información de la empresa, deben estar en conocimiento y cumplir con las políticas y procedimientos establecidos en el Grupo Sigdo Koppers.
- 7) Se velará por el cumplimiento de las normativas y legislaciones en materia de ciberseguridad y seguridad de la información, aplicables en cada país donde el Grupo Sigdo Koppers tenga presencia.

## 6. VIGENCIA

La presente política entrará en vigencia al momento de la aprobación por la Gerencia de Contraloría Corporativa, y será revisada en función de las necesidades.

Fecha	Versión	Descripción	Elaborado por:	Revisado por:	Aprobado por:
27-06-2025	1.0	Actualización	Emilio Mansilla Head of Cybersecurity	Carolina Montero M. Subgerente de Compliance SK S.A.	Alejandro Reyes Gerente Contralor  Ary Martínez CEO SK Converge

## 7. CONTROL DE CAMBIOS

Fecha	Versión	Descripción	Elaborado por:
27-06-2025	1.0	Actualización política.	Emilio Mansilla Head of Cybersecurity