# POLÍTICA MARCO DE SEGURIDAD DE LA INFORMACIÓN

26/05/2026

DOCUMENTO INTERNO

Contenido


OBJETIVOS 2
ALCANCE 2
RESPONSABILIDADES 2
INTRODUCCIÓN 3
POLÍTICA MARCO DE SEGURIDAD DE LA INFORMACIÓN 4
CONTROL DEL DOCUMENTO 5

## OBJETIVOS

Definir las política marco de gestión de seguridad de seguridad de la información aplicables a toda la organización.

## ALCANCE

Toda la organización.

## RESPONSABILIDADES

- Usuario/colaborador: cumplir con la política descrita en el presente documento. Informar cualquier desvío que detecte respecto de las políticas.
- Líder: monitorear que el personal a su cargo tenga conocimiento de la presente política.
- RRHH (Recursos Humanos): documentar el procedimiento de sanciones disciplinarias ante el incumplimiento de la presente política. Comunicar la presente política a todo el personal de la organización
- Responsable de Seguridad de la Información: gestionar las incidencias de seguridad de la información relacionados con el incumplimiento de la presente política.
- Comité de Seguridad de la Información: definir las políticas particulares de seguridad de la información. Velar por el cumplimiento de la presente política.

# INTRODUCCIÓN

Este documento establece la política marco de seguridad de la información a ser cumplimentada por toda la organización a fin de garantizar la seguridad de la información tanto de la organización como de sus partes interesadas.

La seguridad de la información es fundamental para el éxito continuo y la reputación de la organización. Proteger la información confidencial, mantener la integridad de los datos y garantizar la disponibilidad de los recursos es esencial para cumplir con nuestras obligaciones con los clientes, socios y regulaciones.

# POLÍTICA MARCO DE SEGURIDAD DE LA INFORMACIÓN

InsideOne es una empresa especializada en soluciones de transformación digital con inteligencia artificial, que ofrece a través de su plataforma SaaS propia —desarrollada y administrada internamente— capacidades de automatización, omnicanalidad y gestión de procesos financieros. Con más de 20 años de trayectoria acompañando a organizaciones de América Latina, InsideOne opera actualmente con presencia en México y Colombia, brindando servicios a sectores como Banca, Seguros, Retail y Telecomunicaciones.

La misión de InsideOne es ofrecer a las empresas un servicio seguro, confiable y eficiente para optimizar la gestión financiera y la experiencia de cliente, mediante la integración con entidades bancarias, organismos reguladores (SAT y DIAN), sistemas ERP y canales de comunicación como WhatsApp, garantizando el control operativo, la reducción de errores y la mejora de la competitividad empresarial en entornos digitales.

Los principios esenciales que guían a InsideOne son: seguridad de la información, innovación continua, eficiencia operativa, transparencia, cumplimiento normativo, experiencia de usuario y confiabilidad tecnológica.

Para ello, nos comprometemos a:

1. Proporcionar los recursos y el soporte necesarios para lograr el cumplimiento de los objetivos establecidos en referencia a la confidencialidad, integridad y disponibilidad de la información.

2. Actuar dentro del marco de los requisitos legales y reglamentarios aplicables a la organización.

3. Asegurar la disponibilidad y el funcionamiento de los sistemas y activos tecnológicos de la organización.

4. Gestionar de manera adecuada las vulnerabilidades técnicas de nuestra plataforma de servicios.

5. Difundir y promover la cultura de la seguridad de la información entre los miembros de la organización y los terceros asociados.

6. Fomentar la revisión periódica de todos los elementos del Sistema de Gestión de la Seguridad de la Información para lograr la implementación de un proceso de mejora continua.

7. Gestionar los riesgos a la seguridad de la información, identificando las posibles brechas y estrategias de mitigación tendientes a gestionar la seguridad de los activos de información.

8. Garantizar que el uso de sistemas de inteligencia artificial se realice de forma ética, transparente y alineada con los principios de seguridad de la información, la normativa aplicable y los estándares del sector.

9. Establecer criterios de control sobre los datos ingresados, procesados o compartidos con sistemas de IA, evitando la exposición no autorizada de información confidencial o sensible.

10. Verificar la exactitud y trazabilidad de los resultados generados por IA antes de su uso en procesos operativos, decisiones de negocio o comunicaciones, manteniendo supervisión humana efectiva sobre los procesos críticos asistidos o automatizados.

11. Evaluar y gestionar los riesgos específicos asociados al uso de IA —incluyendo sesgos, alucinaciones y dependencia tecnológica— e incorporar su revisión dentro del proceso de mejora continua del Sistema de Gestión.

12. Desarrollar competencias en IA entre los miembros de la organización, promoviendo el conocimiento de sus capacidades, limitaciones y uso responsable.