



Política interna de seguridad de la información

Sistema de Gestión de Seguridad de la Información

Empresa	Ingeniería AT S.A.S. - IAT
Código	IAT-SGSI-POL-001
Versión	1.0
Fecha de emisión	1 de September de 2026
Clasificación	Uso interno
Próxima revisión	Octubre de 2027 o ante cambios significativos

Actividad	Responsable	Cargo	Fecha
Elaboró	Carlos Andrés Angarita Tavera	Co-fundador	01/09/2026
Revisó	Jorge Luis Angarita Tavera	Gerente Técnico	02/09/2026
Aprobó	Alta Dirección	Representante legal	03/09/2026

Estado del documento: APROBADO



Control de cambios

Versión	Fecha	Descripción	Responsable
1.0	01/09/2026	Emisión inicial de la política interna del SGSI de IAT.	Responsable SGSI

Declaración de la dirección

Ingeniería AT S.A.S. establece esta política como marco obligatorio para proteger la información propia y la confiada por clientes, empleados, proveedores y demás partes interesadas. La Alta Dirección se compromete a establecer, operar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, asignando responsabilidades y recursos proporcionales al tamaño, contexto y riesgos de IAT.

Objetivo

Preservar la confidencialidad, integridad y disponibilidad de la información mediante la gestión de riesgos y la aplicación de controles apropiados, cumpliendo los requisitos legales, regulatorios, contractuales y organizacionales aplicables a IAT.

Alcance

Esta política aplica a todas las personas que trabajen para IAT o en su nombre, incluidos socios, empleados, contratistas, consultores, practicantes y terceros autorizados. Cubre la información en cualquier formato, los procesos del negocio, servicios tecnológicos, plataformas en la nube, equipos, redes, aplicaciones, instalaciones y actividades remotas incluidas en el alcance del SGSI.

Referencias

- ISO/IEC 27001:2022 y su Enmienda 1:2024.
- ISO/IEC 27002:2022 como guía de implementación de controles.
- Ley 1581 de 2012, Decreto 1074 de 2015 y demás disposiciones colombianas aplicables.
- Requisitos contractuales de clientes, proveedores y aliados de IAT.

Principios de seguridad

Principio	Aplicación en IAT
Confidencialidad	La información solo estará disponible para personas, procesos o entidades autorizadas.
Integridad	La información deberá mantenerse completa, exacta y protegida contra modificaciones no autorizadas.
Disponibilidad	La información y los servicios deberán estar accesibles cuando sean requeridos por usuarios autorizados.
Gestión del riesgo	Las decisiones de seguridad se basarán en la valoración y tratamiento documentado de riesgos.
Privacidad	Los datos personales serán tratados conforme a las finalidades autorizadas y la legislación aplicable.
Mejora continua	IAT medirá el desempeño del SGSI y corregirá desviaciones para fortalecerlo de manera continua.



Compromisos de IAT

- Cumplir los requisitos legales, regulatorios, contractuales y del SGSI aplicables.
- Establecer objetivos de seguridad medibles y coherentes con esta política.
- Identificar propietarios, clasificar y proteger los activos de información.
- Aplicar controles proporcionales a los riesgos y revisar su eficacia.
- Promover la formación y toma de conciencia del personal.
- Gestionar oportunamente incidentes, vulnerabilidades y debilidades de seguridad.
- Mantener capacidades razonables de respaldo, continuidad y recuperación.
- Evaluar a los proveedores que puedan afectar la seguridad de la información.
- Mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

Responsabilidades

Rol	Responsabilidad principal
Alta Dirección	Aprobar la política, establecer objetivos, asignar recursos, revisar el desempeño del SGSI y promover la mejora continua.
Responsable del SGSI	Coordinar el SGSI, mantener sus documentos, facilitar la gestión de riesgos, consolidar indicadores y reportar a la dirección.
Líderes y responsables de procesos	Identificar activos y riesgos, aplicar controles, conservar evidencias y asegurar el cumplimiento dentro de sus procesos.
Usuarios internos y contratistas	Conocer y cumplir las políticas, proteger los activos asignados y reportar incidentes o debilidades.
Proveedores autorizados	Cumplir las obligaciones contractuales y los controles de seguridad aplicables a los servicios prestados.

Lineamientos internos obligatorios

Uso aceptable de información y activos

- Los activos de IAT se utilizarán exclusivamente para fines laborales autorizados, salvo usos personales ocasionales expresamente permitidos.
- La información no podrá copiarse, publicarse, enviarse ni almacenarse en cuentas, plataformas o dispositivos no autorizados.
- Cada persona es responsable por el cuidado de los equipos, credenciales, documentos y medios que le sean asignados.
- La instalación de software, conexión de dispositivos o modificación de configuraciones requiere autorización cuando pueda afectar la seguridad.

Clasificación y manejo de información

La información será identificada y protegida según su sensibilidad, valor, obligaciones legales y efecto potencial. IAT utilizará como mínimo las categorías Pública, Uso interno y Confidencial. La información confidencial deberá compartirse únicamente con destinatarios autorizados, mediante mecanismos aprobados y aplicando cifrado cuando el riesgo lo requiera.



Identities and access control

- Cada usuario utilizará una identidad individual; se prohíbe compartir contraseñas o mecanismos de autenticación.
- Los accesos se otorgarán por autorización, necesidad laboral y privilegio mínimo.
- Se aplicará autenticación multifactor en servicios críticos y siempre que esté disponible y resulte apropiado.
- Los accesos serán revisados periódicamente y se revocarán oportunamente ante retiros, cambios de función o finalización de contratos.
- Las contraseñas y secretos deberán almacenarse mediante mecanismos seguros aprobados por IAT.

Remote work and devices

- El personal deberá impedir la visualización o acceso no autorizado a la información durante el trabajo remoto.
- Los equipos deberán mantener bloqueo automático, actualizaciones, protección contra malware y cifrado cuando corresponda.
- Las redes públicas o no confiables deberán utilizarse únicamente con las protecciones definidas por IAT.
- La pérdida, robo o compromiso de un equipo deberá reportarse inmediatamente.
- Los documentos físicos y pantallas con información sensible deberán mantenerse protegidos mediante prácticas de escritorio y pantalla limpios.

Data protection and communications

- Los datos personales se tratarán únicamente para finalidades autorizadas y durante el tiempo necesario.
- La información confidencial se transmitirá mediante canales aprobados y se verificará el destinatario antes del envío.
- No se utilizarán servicios públicos de inteligencia artificial, repositorios externos o herramientas no aprobadas para procesar información confidencial, datos personales o información de clientes.
- La divulgación a terceros requiere autorización y, cuando aplique, acuerdos de confidencialidad y tratamiento de datos.

Secure technological operation

- Los sistemas deberán mantenerse soportados, actualizados y configurados de acuerdo con criterios de seguridad aplicables.
- Las vulnerabilidades se evaluarán y corregirán según su criticidad y exposición.
- Los cambios significativos deberán evaluarse, autorizarse, probarse y contar con mecanismos de reversión cuando corresponda.
- Los registros de seguridad y operación se conservarán según el riesgo, las necesidades de investigación y los requisitos aplicables.
- Los respaldos deberán protegerse y su restauración deberá probarse con una periodicidad proporcional a la criticidad.

Incident management

Toda persona debe reportar inmediatamente eventos sospechosos, pérdidas de información, accesos no autorizados, malware, fraude, indisponibilidad significativa, divulgaciones indebidas o incumplimientos de esta política. IAT registrará, clasificará, contendrá, investigará y cerrará los incidentes, preservando evidencias y comunicando a las partes correspondientes cuando exista obligación legal o contractual.

Providers and services in the cloud

Los proveedores serán evaluados de acuerdo con el riesgo de sus servicios. Los contratos incluirán requisitos de confidencialidad, seguridad, privacidad, incidentes, continuidad, subcontratación, devolución o eliminación de



información y derecho de verificación cuando sean aplicables. Los servicios en la nube deberán aprobarse antes de su uso y gestionarse durante todo su ciclo de vida.

Continuidad de las operaciones

IAT identificará los servicios y recursos críticos, definirá medidas de continuidad y recuperación, y realizará pruebas razonables para confirmar que la información y las capacidades prioritarias pueden recuperarse dentro de los tiempos establecidos.

Formación y toma de conciencia

Las personas recibirán inducción de seguridad al vincularse y actividades periódicas de actualización. Deberán conocer sus responsabilidades, los canales de reporte, las consecuencias de incumplimiento y los riesgos asociados con ingeniería social, contraseñas, trabajo remoto, datos personales y uso de servicios tecnológicos.

Objetivos y seguimiento

La Alta Dirección aprobará objetivos de seguridad coherentes con esta política. Cada objetivo tendrá responsable, indicador, meta, plazo y evidencia de seguimiento. El desempeño se evaluará mediante indicadores, incidentes, resultados de auditoría, tratamiento de riesgos, acciones correctivas y revisión por la dirección.

Excepciones

Toda excepción deberá justificarse, evaluar sus riesgos, definir controles compensatorios, contar con aprobación del responsable correspondiente y establecer una vigencia. Las excepciones vencidas se cerrarán o renovarán mediante una nueva evaluación.

Incumplimiento

El incumplimiento podrá generar restricción de accesos, acciones correctivas, medidas disciplinarias o contractuales y acciones legales, según la gravedad, recurrencia e impacto, respetando la legislación y los acuerdos vigentes.

Comunicación disponibilidad y revisión

Esta política deberá mantenerse como información documentada, comunicarse dentro de IAT y estar disponible para las partes interesadas cuando corresponda. Se revisará al menos una vez al año y ante cambios relevantes en el contexto, los riesgos, la tecnología, las obligaciones aplicables o el alcance del SGSI.