

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código: IAS-USG SI-PU 02
		Versión:6.00
		Fecha:9/04/2026

Medellín, 9 de abril de 2026

I.A.S. INGENIERÍA, APLICACIONES Y SOFTWARE S.A.S, bajo el liderazgo y compromiso de la Alta Dirección, reconoce la información como un activo estratégico y establece su compromiso con la protección de la confidencialidad, integridad y disponibilidad de la información, así como la privacidad y la ciberseguridad. Este compromiso se materializa buscando establecer un marco de confianza con clientes, proveedores y empleados mediante la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, en cumplimiento de los requisitos de la norma ISO/IEC 27001:2022, y demás obligaciones legales, regulatorias, contractuales aplicables y en concordancia con la misión y visión de la empresa.

En la implementación del sistema, la organización identifica, evalúa y trata los riesgos de seguridad de la información, con el fin de reducir su impacto a niveles aceptables. Todo desde un ejercicio sistemático de gestión, que nos permita mantener la integridad, confidencialidad y la disponibilidad, acorde con las necesidades de las partes interesadas.

Esta política establece el marco de referencia para la definición, seguimiento y mejora de los objetivos de seguridad de la información, descritos a continuación y los cuales permiten orientar la toma de decisiones, la gestión de riesgos y la implementación de controles dentro del Sistema de Gestión de Seguridad de la Información.

1. Mantener la implementación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, asegurando el cumplimiento del 100% de los controles aplicables del Anexo A y la realización de al menos una auditoría interna anual y una revisión por la dirección.
2. Proteger los activos de información de la organización garantizando al menos un 95% de cumplimiento de los controles aplicables relacionados con confidencialidad, integridad y disponibilidad, alineados a la norma ISO 27001:2022
3. Reducir o mitigar al menos el 90% de los riesgos de seguridad de la información clasificados como “altos” o “críticos” a niveles aceptables, a través de un proceso continuo de identificación, evaluación y tratamiento documentado, y validando la efectividad de los controles aplicados.
4. Establecer un proceso eficaz de gestión de incidentes que garantice la detección y respuesta a eventos en un tiempo promedio ≤ 4 horas y la recuperación de servicios críticos en un máximo de 24 horas, con al menos un simulacro anual documentado y evaluado.
5. Asegurar el cumplimiento normativo y contractual al 100% mediante monitoreo continuo, auditorías regulares y gestión proactiva de obligaciones y mejores prácticas en seguridad de la información.
6. Promover la mejora continua del SGSI mediante la ejecución del 100% de los planes de acción derivados de auditorías, revisiones por la dirección, hallazgos y oportunidades de mejora, con seguimiento continuo y evidencias de cumplimiento antes del cierre de cada ciclo anual del SGSI.

ias software	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código: IAS-USG SI-PU 02
		Versión:6.00
		Fecha:9/04/2026

7. Fomentar una cultura de seguridad de la información en todas las partes interesadas, mediante programas de sensibilización, formación y comunicación continua, asegurando como mínimo el 80% de participación del personal.

Principios de seguridad de la información

A continuación, se establecen los principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de I.A.S. INGENIERÍA, APLICACIONES Y SOFTWARE:

1. La organización asume la seguridad de la información como una responsabilidad corporativa, definiendo y manteniendo las condiciones necesarias para su protección.
2. Las políticas, procesos y procedimientos de seguridad de la información son de obligatorio cumplimiento y aplican a colaboradores, clientes, proveedores y demás terceros que tengan acceso a los activos de información.
3. La organización protege la información generada, procesada, almacenada o transmitida en el desarrollo de sus procesos de negocio, así como la infraestructura tecnológica y los activos asociados, incluyendo aquellos gestionados por terceros o en esquemas de outsourcing.
4. La organización clasifica y protege la información de acuerdo con su nivel de criticidad, aplicando controles que prevengan accesos no autorizados, pérdida, alteración o divulgación indebida, minimizando impactos financieros, operativos y legales.
5. La organización gestiona los riesgos de seguridad de la información mediante procesos de identificación, evaluación y tratamiento, con el fin de reducir su impacto a niveles aceptables.
6. La organización protege la información frente a amenazas internas y externas, incluyendo aquellas derivadas del comportamiento humano, mediante controles preventivos, detectivos y correctivos.
7. La organización protege las instalaciones físicas y la infraestructura tecnológica que soportan los procesos críticos del negocio, garantizando condiciones adecuadas de seguridad.
8. La organización controla el acceso a la información, a los sistemas y a los recursos de red, asegurando que este se otorgue bajo el principio de mínimo privilegio y necesidad de conocimiento.
9. La organización integra la seguridad de la información en todo el ciclo de vida de los sistemas de información, desde su diseño hasta su disposición final.
10. La organización gestiona los eventos e incidentes de seguridad de la información de manera oportuna, asegurando su detección, reporte, análisis y respuesta, así como la implementación de acciones de mejora.
11. La organización garantiza la continuidad de sus procesos críticos mediante la implementación de controles de continuidad del negocio y recuperación ante desastres, basados en el análisis de impacto.
12. Garantizamos el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables, incluyendo la norma ISO/IEC 27001:2022, la Ley 1273 de 2009, la Ley 1581 de 2012, el Decreto 1377 de 2013, la Ley 1712 de 2014, los CONPES vigentes y demás disposiciones que se emitan durante la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información

ias software	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código: IAS-USG SI-PU 02
		Versión:6.00
		Fecha:9/04/2026

13. La organización promueve una cultura de seguridad de la información mediante la sensibilización, formación y concienciación continua de sus partes interesada.
14. La presente política es comunicada, comprendida y aplicada dentro de la organización, y se encuentra disponible para las partes interesadas pertinentes.

El incumplimiento a la política de Seguridad de la Información traerá consigo, las consecuencias que apliquen en el reglamento interno de trabajo y/o en la normatividad legal vigente.

Atentamente,



David Augusto Gómez Giraldo
Gerente general
I.A.S INGENIERIA, APLICACIONES Y SOFTWARE
NIT: 811042378