INFORMATION SECURITY POLICY

ISO/IEC 27001:2022

GIGA IT recognizes information security as a strategic pillar and an essential requirement for business continuity, the trust of its clients and the protection of data.

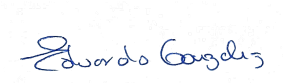
We recognize that information is one of our most valuable assets and that protecting it is essential to providing Staffing services of specialized technology professionals, building trust with our clients and ensuring the continuity of our operations.

This Policy establishes the framework for preserving the confidentiality, integrity and availability of information, in all its forms and media, aligned with the ISO 27001:2022 standard, committing to:

- Protect the confidentiality, integrity and availability of information, applying appropriate controls according to its classification, criticality and the identified risks.
- Systematically manage information security risks, identifying, assessing and treating risks through technical, organizational and administrative controls proportionate to the context of the organization and to the Staffing service.
- Comply with legal, regulatory, contractual and other applicable requirements, as well as the obligations undertaken with clients, suppliers and other interested parties.
- Apply access controls, ensuring that access to information and technology assets is authorized, traceable and periodically reviewed.
- Use only authorized tools, platforms and technology resources, promoting secure practices for handling information throughout its entire lifecycle.
- Develop personnel competence and awareness through training and awareness programs that strengthen the information security culture.
- Manage information security incidents through formal processes for identification, reporting, analysis, response and learning, minimizing their impact and contributing to the continuity of services.
- Monitor the performance of the ISMS, establishing information security objectives and indicators that make it possible to evaluate its effectiveness and support evidence-based decision-making.
- Continually improve the Information Security Management System through the periodic review of risks, internal audits, performance results, changes in the context of the organization and management reviews.

This Policy provides the framework for setting information security objectives. It is communicated to all personnel and to relevant interested parties. It will be reviewed periodically to ensure its continuing suitability, adequacy and effectiveness.

Approved by Top Management:



Verified by signNow
08/12/2026 10:29:17 UTC
2e849b0e5ecd4173a5c2

Eduardo González
Chief Executive Officer (CEO)

Change Control

Date	Revision No.	Change
09-07-26	0	Original issue

Approval

Issued by	Reviewed by	Approved by
People, IT & Efficiency Department	Chief Executive Officer	General Management