Information Security Policy

This Security Policy applies to all personnel who access Zitro information or communications networks, whether used by employees, collaborators, or third parties.

In particular, this policy applies to:

- Zitro group staff.
- Contractors and subcontractors who provide a service to the Organization, in the areas provided for in the contract and respective agreements.
- Personnel who, without having an employment relationship with the Organization, have access to information at any time during its life cycle.

Zitro Group Management believes that achieving these objectives is subject to compliance with various requirements aimed at ensuring information security within the company.

In this way, Information Security is established as a priority for the Zitro group and, to this end, this Policy establishes the following guidelines:

- Information owned by the Zitro Group must be accessible only to duly authorized individuals, whether or not they belong to the Organization.
- This Security Policy, as well as all other documents related to information security standards, must be accessible to all members of the Company, as well as to non-Company personnel who interact with one or more of the group's companies through any of its processes.
- The Zitro Group, its employees, and related personnel to whom this policy applies must comply with all applicable legal, regulatory, and statutory requirements, as well as contractual requirements.
- The confidentiality of information must be guaranteed at all times and considered a principle within the Company.
- The integrity of information must be ensured throughout all processes that are managed, processed, and stored.
- The availability of information and internal processes must be guaranteed through appropriate backup and business continuity measures.
- All staff must have adequate training and awareness in Information Security.
- Any incident or weakness that may compromise or has compromised the confidentiality, integrity, and/or availability of information must be reported through the Company's available means and analyzed to implement the corresponding corrective and/or preventive measures.
- Assuming security risks must be approved by an appropriate management level, the higher the risk, and always keeping in mind that the person assuming the risk must have authority or decision-making power over the affected area.
- The Company's management establishes and maintains a Security Committee, responsible for implementing, maintaining, and improving this Policy as well as establishing, monitoring, measuring, and improving security controls and needs related to the Company.
- Every member of the Zitro group must ensure compliance with this policy and the regulations derived from it.

This policy came into effect on February 15, 2012, and will remain in effect during subsequent revisions until the Company is notified of its discontinuation.

Update date: January 2024