warpcom SERVICES

Information Security Policy

Statement on the implementation of the Information Security Management System in Warpcom, according to ISO 27001A

Warpcom is engaged and committed regarding Information Security towards its Customers, Employees, Partners and remaining stakeholders.

Thus, this Policy constitutes the basic pillar for the safe data processing and describes the general principles that must be applied in Warpcom, integrating the following objectives:

- Working actively to achieve security levels that help us comply with the principles of confidentiality, integrity and availability.
- Establishing the Statement of Applicability (SoA), applying adequate controls to the risks to which Warpcom and its assets are exposed;
- Grant the Information Security Commission the authority and resources it needs to establish and create appropriate guidelines to a correct security of the information assets identified by Warpcom, ensuring the operational application of SoA;
- Raising awareness among employees and suppliers of the importance of their contribution in achieving these goals;
- Guaranteeing resources and physical conditions that allow for a full information security within the Information Security Management System;
- Identifying, monitoring and complying with the legal and regulatory requirements applicable to Warpcom;
- Establishing, maintaining and testing a plan that allows you, in case of a breach, to maintain the continuity of services and systems deemed critical in a specific period of time;
- Establishing a methodology that enables the identification, research and control/communication of information security incidents, as well as the mitigation of their impact and recurrence;
- Maintaining, adjusting and improving this policy, as well as all the rules and documents that support this system in accordance with the internal, external and technological context of Warpcom and consequently identified risks;

This Policy is disclosed to all Employees, Suppliers and remaining stakeholders in order to guarantee:

- Awareness of the importance and relevance of information security;
  That there is no communication failure capable of preventing the implementation of this policy and the alleged lack of knowledge of the latter.

February 2022
CEO