Information Security Policy (ISO/IEC 27001 and National Security Framework – ENS

PENINSULA CORPORATE INNOVATION, as a company dedicated to the development, implementation, and operation of innovative digital solutions for digital transformation—including web platforms, software as a service, data analysis tools, indicator visualization, extended reality, artificial intelligence, sensors, and hosting and technological infrastructure services—has implemented an information security management system within the organization.

Its main objective is to achieve business goals and customer satisfaction by ensuring information security at all times through established processes based on a continuous improvement approach, guaranteeing the continuity of information systems, minimizing the risk of damage, and ensuring compliance with the objectives set to always safeguard the confidentiality, integrity, and availability of information.

To this end, it commits to information security in accordance with the ISO/IEC 27001 standard and Royal Decree 311/2022 of May 3, which regulates the National Security Framework. Therefore, General Management establishes the following principles:

- Competence and leadership by management as a commitment to developing the Information Security Management System.
- Identification of internal and external interested parties relevant to the Information Security Management System and compliance with their requirements.
- Understanding the context of the organization and determining its information security risks and opportunities as a basis for planning actions to address, assume, or treat them.
- Ensuring the satisfaction of our clients and other stakeholders in all matters related to the execution of our activities and their impact on society.
- Establishing objectives and goals focused on evaluating performance in terms of Information Security and on the continuous improvement of our activities, as regulated in the Management System that supports this policy.
- Compliance with applicable legal and regulatory requirements related to our activities, commitments acquired with clients and stakeholders, and all internal rules or guidelines the company adheres to.
- Ensuring the confidentiality of the data managed by the company and the availability of information systems, both in services offered to clients and in internal management, preventing unauthorized alterations to the information.
- Ensuring responsiveness in emergency situations, restoring the operation of critical services as quickly as possible.
- Establishing appropriate measures for addressing risks identified through asset identification and assessment.
- Motivating and training all personnel working within the organization, both for the proper performance of their job and to act in accordance with the requirements imposed by the referenced Standard, providing an adequate environment for process operations.
- Maintaining smooth communication internally, across all company levels, as well as with clients.
- Evaluating and ensuring the technical competence of personnel in performing their duties, and ensuring their appropriate motivation to participate in the continuous improvement of our processes.
- Ensuring the proper condition of facilities and appropriate equipment, aligned with the company’s activities, goals, and objectives.
- Continuously analyzing all relevant processes and establishing the appropriate improvements in each case, based on the results obtained and the goals set.

These principles are embraced by General Management, which provides the necessary means and allocates sufficient resources to its employees to ensure compliance, making them known through this Information Security Policy.

General Director
Simón Lee