General Principles of Information Security

Hipoges IT

Document for public use

General Principles of Information Security

At Hipoges, meeting the requirements, needs and expectations of our stakeholders is a shared value that demands the highest levels of security and quality.

Hipoges attaches priority interest and maximum support to the protection of information because of its strategic nature and as a way to ensure the improvement of services in its operations.

In this sense, Hipoges Management, and consequently the entire organization, are committed to Information Security, based on the requirements of the ISO/IEC 27001:2013 Standard.

Likewise, Hipoges pursues the adoption, implementation and continuous operability of protocols and procedures that consider the preservation, at least, of the basic components of information security:

- **Confidentiality**: Ensure that only duly authorized persons have access to data and systems.

- **Integrity**: Ensure the accuracy of information and systems against alteration, loss or destruction, whether caused accidentally or intentionally.

- **Availability:** Ensure that information and systems can be used as and when required.

This policy will be considered in the execution of all phases of the information life cycle: generation, distribution, storage, processing, transport, consultation and destruction, and of the systems that process it (analysis, design, development, implementation, operation and maintenance).

Information security is the responsibility of all the organization's personnel, so this policy must be known, understood and assumed by all levels of the organization and must be reliably communicated to the entire organization, to its own personnel and to external collaborating companies, and be available stakeholders.

Relations with third-party collaborating companies must always be covered by the due guarantees in the use and treatment of information.

In summary, the basic principles covered by this policy are as follows:

- Ensure that all information systems, networks and business applications that Hipoges manages are effectively and efficiently protected from security threats and risks that cannot be directly countered are minimized.

- Ensure that all Hipoges users are aware of the duty to comply with national and supranational laws.
- Ensure that all Hipoges users understand and are aware of their personal responsibilities for protecting the confidentiality, integrity and availability of accessed data.
- Assign the necessary security roles and responsibilities and provide the necessary support.
- Ensure that all Hipoges users are aware of the duty of compliance, as well as all other applicable internal regulations
- Safeguard the reputation and business of Hipoges brand, as well as compliance with legal obligations and its protection.
- Consider information security at suppliers and subcontractors.
- Establish and periodically review the level of security (risk appetite) based on risk analysis.
- Demonstrate management leadership by ensuring that the Information Security Policy and security objectives are established and are consistent with the strategic direction of the organization.
- Meet the needs and expectations of stakeholders involved within the scope of information security, preserving the availability, integrity and confidentiality of information.
- Ensure a periodic review of policies and procedures for proper compliance of the changes (legal, technical or any other) for continuous safety improvement.

The Information Security Management System is based on the requirements of ISO/IEC 27001:2013 and must be followed by all employees. The Management is responsible for the development, implementation, updating and supervision of compliance of the entire Management System and has designated the ISMS Manager for its executive implementation.