Information Technologies Governance and Management Policy

Ayesa strives to build a more efficient and fairer world by seamlessly combining cutting-edge engineering and technology. We offer engineering, consulting, information technology and outsourcing services across multiple lines of business and industries, as well as design, back and front office outsourcing, installation, and support services for technology and digital services.

Aesa Top Management is aware and has assumed the importance of Information Technologies for the efficient management of internal processes and the achievement of the Strategic Business Objectives.

hat is why the Top Management assumes the responsibility to implement, maintain and continuously improve the IT governance practices, according to the following **principles**:

- **Responsibility**: responsibilities are defined and every single employee in Ayesa understands and accepts such responsibilities. In particular, it ensures that the roles and responsibilities related to IT Governance and IT management systems are defined and communicated, keeping updated the document *DO-GD01 Manual of functions related to Management Systems*.
- **Strategy**: Information Technology plans will be aligned with the company's business objectives and strategies and will add value to the company's business, focusing on cost optimization.
- **Procurement**: IT investments and acquisitions are prioritized based on business needs and are carried out following procedures that ensure their suitability and contribution to business strategies, focusing on optimizing costs.
- **Performance**: the Information Systems Management ensures the provision of services, service levels and quality of service required to meet current and future business requirements.
- **Compliance**: procedures and measures have been established to ensure compliance with legislation and regulations (special emphasis on the guidelines of the European Data Protection Regulation); periodic reviews and audits are carried out to ensure that they are implemented, and they are enforced.
- **Human Factor**: Ayesa will provide the necessary human resources to meet the Business needs and communication, training, awareness and motivation activities are carried out to all Ayesa employees for the proper use of IT.

Ayesa's IT Governance is supported by the different IT Management Systems implemented: Information Security (ISO 27001 and ENS), IT Service Management (ISO 20000-1), Software Development (CMMI) and Continuity Management (ISO 22301). As well as ISO 27002 (Information Security Control) and its extensions ISO 27018 (Code of practice for protecting personal data in the cloud) and ISO 27701, reference standard for data protection compliance.

To ensure compliance with the requirements and continuous improvement of these systems, Ayesa Top Management acquires the following **commitments**:

Regarding its **Security Management System**:

- To ensure access, integrity, confidentiality, availability, authenticity, traceability of information and the continuous provision of services, acting preventively, supervising daily activity and reacting promptly to incidents.
- Protect Ayesa's information resources and the technology used for its processing, against threats, internal or external, deliberate or accidental, in order to ensure compliance with the confidentiality, integrity, availability, legality and reliability of the information.
- Evaluate and treat the risks and threats to which Ayesa's information, services and systems are exposed, including the risks derived from the treatment of personal data and the key risks for the continuity of the processes considered critical by the organisation.
- To implement the necessary measures for the recording of activity and the analysis of the same in search of abnormal patterns and the

implementation of the appropriate actions for their treatment. To ensure that, for any acquisition of products, both software and hardware, security requirements are taken into account.

- Ensure that security requirements are taken into account for any procurement of products, both software and hardware.

Regarding its **Continuity Management System**:

- The first premise and priority objective is the protection and security of personnel, both in normal and contingency situations.
- Provide the necessary procedures in order to respond appropriately to the occurrence of a disruptive incident, from the moment it is declared until complete recovery of normality in the different business activities, minimizing the impact on operations.
- Minimize the impact that could be derived from any emergency situation on the services identified as critical as well as their level of provision.
- Return the affected location to a state of normality as soon as possible once the consequences of the disruptive incident have been mitigated.
- Ensure that Continuity Plans are adequately developed, implemented and maintained, taking into account critical services and processes, all of this based on risk assessment.
- Continuous testing of the Business Continuity Management System to ensure its adequacy to Ayesa's needs and adapt it whenever necessary in view of the results of such tests.

Regarding its **IT Service Management System**:

- Ensure the customer and users' needs and expectations satisfaction according to the agreed services.
- To be able to detect, analyse, inform and correct possible deficiencies and shortcomings in relation to the established service level agreements.
- Ensure the service levels agreed between Ayesa and its customers compliance, as well as to manage any incident or problem that may arise.

Regarding its **Software Development Management System**:

- Ensure customer requirements and Information Security requirements compliance throughout the development life cycle.
- Ensure customer needs and expectations satisfaction.
- Carry out all the practices established in the CMMI model.

Regarding its **Privacy Management System:**

- Comply with the legislation of each country, related to the protection of personal data.
- Implement adequate controls for the protection of personal data.
- Collect only essential personal data.
- Use personal data only for the stated purposes.
- Establish retention periods for personal data commensurate with the purpose and legal obligations to retain the information.
- Implement appropriate channels to allow users to exercise their rights over their personal data.

To carry out this policy, Ayesa has established work patterns documented in procedures, instructions, documents and templates that are available on the intranet to all employees, being mandatory for all of them, as well as for third parties supplying goods or services to Ayesa.

Firmado por Costa Muñoz, Andrés, CIO de AYESA el día 31/03/2025 con un certificado emitido por VMADENTCA01-CA

Andrés Costa Muñoz
CIO