IT Governance and Management Policy

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

1. 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-SI01 "Organizational Structure of Information Technology".
2. 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.
3. 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.
4. Performance: the CTO ensures the provision of services, service levels and quality of service required to meet current and future business requirements.
5. 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.
6. Human Factor: Ayesa will provide the necessary human resources to meet the Business needs and 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). To ensure compliance with the requirements and continuous improvement of these systems, Ayesa Top Management acquires the following commitments:

Regarding its Security Management System, Ayesa is committed to:

- Ensure information access, integrity, confidentiality, availability, authenticity, traceability and a continuous provision of services, acting preventively, monitoring daily activity and reacting promptly to incidents.
- Protect Ayesa’s information resources and the technology used for its processing, against internal or external, deliberate or accidental threats, in order to ensure compliance with confidentiality, integrity, availability, legality and reliability of the information.
- Assess and address the risks and threats to which Ayesa's information, services and systems are exposed, including risks arising from the processing of personal data and key risks to the continuity of processes considered critical by the Organization.
- Ensure that, for any product acquisition, both software and hardware, security requirements are taken into account.

- Implement the necessary measures for recording the activity and analyzing them for unusual or abnormal patterns and implementing the appropriate actions for their treatment.

Regarding its Continuity Management System, Ayesa is committed to:

- 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, Ayesa is committed to:

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

Regarding its Software Development Management System, Ayesa is committed to:

- Ensure customer needs and expectations satisfaction.
- Ensure customer requirements and Information Security requirements compliance throughout the development life cycle.
- Carry out all the practices established in the CMMI V2.0 model.

The regulatory framework of Ayesa's activities related to Information Technologies is, as it follows:

a) Royal Decree 311/2022, which regulates the National Security Scheme in the field of electronic administration.

b) RD 251/2015, October 23th, which regulates the National Security Scheme in the field of e-Government.

c) Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27th 2016 (GDPR).

d) Law 9/2017, November 8th, on Public Sector Contracts.

e) Standard UNE-ISO/IEC 27001.

f) Standard UNE-ISO/IEC 20000-1.

g) UNE-ISO/IEC 22301 Standard.

h) CMMI V2.0 Model.

i) Standard UNE-ISO/IEC 38500.

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 Ayesa employees, being mandatory for all of them, as well as for third parties supplying goods or services to Ayesa.

This IT Governance and Management Policy is available to interested parties who may request it.

Seville, 14 October 2022

CTO