

and Management Policy

Ayesa Digital works to build a more efficient and fairer world by applying cutting-edge technology in an integrated manner. Ayesa Digital provides consulting, information technology, and outsourcing services across multiple business lines and industry sectors, as well as design services, back- and front-office outsourcing, installation and support of technological infrastructures, and digital services.

Ayesa Digital Top Management is fully aware of and acknowledges the importance of Information Technologies for the efficient management of internal processes and the achievement of the Business's strategic objectives.

Therefore, Top Management assumes responsibility for implementing, maintaining, and continually improving IT governance practices in accordance with the following **principles**:

- **Responsibility:** responsibilities are clearly defined, and all Ayesa Digital personnel understand and accept them. This includes ensuring that the roles and responsibilities related to IT Governance and IT Management Systems are defined and communicated, while keeping updated the document DO-GD01 – Manual of functions related to Management Systems.
- **Strategy:** information technology plans shall be aligned with the company's business objectives and strategies and shall deliver value to the business, focusing on cost optimization.
- **Acquisition:** IT investments and acquisitions are prioritized based on business needs and carried out in accordance with procedures that ensure their suitability and contribution to business strategies, focusing on cost optimization.
- **Performance:** the Information Systems Management function ensures the provision of the services, service levels, and service quality required to meet the present and future needs of the business.
- **Compliance:** procedures and measures have been established to ensure compliance with applicable laws and regulations (with particular emphasis on data protection legislation guidelines), and periodic reviews and audits are conducted to ensure they are implemented and complied with.
- **Human Factor:** Ayesa Digital shall provide the necessary human resources to meet business needs and shall carry out communication, training, awareness, and motivation activities for all personnel to ensure the proper use of IT.

Ayesa Digital IT Governance framework is based on ISO 38500 and is supported by the different implemented IT Management Systems: Information Security (ISO 27001 and ENS), IT Service Management (ISO 20000-1), Software Development (CMMI), Business Continuity Management (ISO 22301), and Privacy Management (ISO 27701), as well as ISO 27002 (Information Security Controls) and its extension ISO 27018 (Code of practice for protecting personal data in the cloud).

To ensure compliance with requirements and continuous improvement, Ayesa Digital Management undertakes the following **commitments**:

Regarding **the Information Security Management System**:

- Ensure the access, integrity, confidentiality, availability, authenticity, and traceability of information, as well as the continuous delivery of services, by acting preventively, monitoring daily activity, and responding swiftly to incidents.
- Protect Ayesa Digital's information resources and the technology used for their processing against internal or external, deliberate or accidental threats, in order to ensure compliance with legal requirements and the reliability of information.
- Assess and treat the risks and threats to which Ayesa Digital's information, services, and systems are exposed, including risks arising from the processing of personal data and key risks affecting the continuity of processes considered critical by the organization.
- Implement the necessary measures for activity logging and analysis to detect abnormal patterns and initiate the appropriate corrective actions.
- Ensure that security requirements are considered in any acquisition of products, whether software or hardware.

and Management Policy

Regarding the **Continuity Management System**:

- The primary premise and top priority objective is the protection and safety of personnel, both under normal conditions and contingency situations.
- Establish the necessary procedures to respond appropriately to the occurrence of a disruptive incident, from declaration through full recovery of normal operations across the different business activities, minimizing the impact on operations.
- Seek to minimize the impact that any emergency may have on services identified as critical or on their service levels.
- Restore normal conditions at the affected location as quickly as possible once the consequences of the disruptive incident have been mitigated.
- Ensure that Business Continuity Plans are properly developed, implemented, and maintained, taking into account critical services and processes and using risk assessment as a reference.
- Periodically test the Business Continuity Plan to ensure its adequacy to Ayesa Digital's needs and adapt it whenever necessary considering test results.

Regarding the **IT Service Management System**:

- Ensure satisfaction of client and user needs and expectations with respect to the agreed services.
- Guarantee compliance with the service levels agreed between Ayesa Digital and its clients, as well as the management of any incident or problem that may arise.
- Detect, analyze, report, and correct any possible deficiencies or gaps related to the established Service Level Agreements.

Regarding the **Software Development Management System**:

- Ensure compliance with client requirements and Information Security requirements throughout the entire development lifecycle.
- Ensure satisfaction of clients' needs and expectations.
- Carry out all practices established in the CMMI model.

Regarding the **Privacy Management Systems**:

- Comply with the legislation of each country related to the protection of personal data.
- Implement the appropriate controls for the protection of personal data.
- Collect only the personal data that is strictly necessary.
- Use personal data solely for the declared purposes.
- Establish personal data retention periods proportionate to the purpose and legal information retention obligations.
- Implement appropriate channels to enable users to exercise their rights regarding their personal data.

To implement this Policy, Ayesa Digital has established documented working methods in procedures, instructions, documents, and templates that are available to Ayesa Digital personnel on the intranet and are mandatory for all employees, as well as for third parties supplying goods or services to Ayesa Digital.