Quality and Security Policy

Motivait is an innovative Digital Services and Solutions company whose mission is to enhance the participation, motivation and engagement of individuals through solutions that reflect the culture, context and objectives of our clients.

The management of Motivait wishes to inform its employees, clients, suppliers and other interested parties of its absolute conviction of the importance of both Quality and Information Security as key elements for the effective development of our organisation and the achievement of our overall purpose.

This Quality and Security Policy will be regularly reviewed and adapted, in line with our commitment to continuous improvement, to ensure compliance with the requirements of ISO/IEC 27001:2022, while also integrating recommendations from ISO/IEC 27002:2022.

Motivait's Quality and Security Policy is based on the following core commitments:

- To offer our clients Services and Solutions that are secure, reliable and fit for purpose.
- To achieve and maintain high levels of client satisfaction.
- To establish and maintain a Management System that ensures the continuous improvement of our processes and working practices.
- To comply with all requirements, whether legal, contractual or otherwise, that are applicable and appropriate in relation to our activities and core purpose.

To this end, Motivait commits to ensuring that:

1. The Integrated Quality and Security Management System will include the necessary and appropriate policies, procedures and work instructions to guarantee the application of this Quality and Security Policy, ensuring compliance with legal, contractual and regulatory requirements with our clients and suppliers in terms of both quality and security, including the protection of personal identifiable information (PII).

2. Objectives related to quality and information security are to be established annually, covering relevant aspects such as personal data protection (A.5.34), secure software development (A.8.25) and security within cloud environments (A.5.23).

3. Compliance is ensured with business, legal or regulatory requirements and contractual obligations in matters of quality and security, including the protection of personal identifiable information (PII) and adherence to applicable data protection regulations.

4. Staff are provided with the necessary resources, training and information to carry out their work, as well as protect the information assets used in their daily operations, with the processing of any such information for other unauthorised purposes strictly prohibited. Training and awareness will be prioritised on security, vulnerability management (A.5.14) and threat intelligence (A.5.7).

5. All suppliers and subcontractors are made aware of and bound by this Policy, including specific requirements on supply chain security (A.5.19) and protection of information

in outsourced services (A.8.32).

6. Control objectives are set within the business according to the needs arising from identified risks, considering both threat intelligence and proactive vulnerability management.

7. Necessary measures are established to guarantee the continuity of the company's business, in line with the controls for service continuity and resilience (A.5.10, A.5.11 and A.8.18).

8. All our employees are responsible for ensuring proactive compliance with this Policy, making improvement suggestions, and recording and reporting any suspected threats or security breaches.

9. The CQSO (Chief Quality & Security Officer) holds overall responsibility for maintaining this Policy, which will be reviewed at least annually, or whenever serious security incidents occur, audit issues arise, or organisational changes and new responsibilities require its revision. The Policy will also be reviewed in response to significant changes in the organisational context or threat landscape.

To this end, the specific Quality and Security objectives are defined in the document ***"F.101 Quality & Security Objectives"***.

The review of this Quality and Security Policy, as well as the establishment and revision of specific and measurable objectives, is carried out during management system reviews.
This Policy is an integral part of the Information Security Management System (ISMS), aligned with ISO/IEC 27001:2022, and will be kept up to date to ensure its effectiveness and adaptation to new technological and regulatory challenges.

Information Security is a fundamental element within the culture, values and purpose of Motivait. Senior management requires that all Motivait staff read, study and comply with this Policy, as well as with the specific policies, procedures and work instructions on information security defined by the organisation.

Madrid, 1st of October 2025

This policy has been approved by the CEO of Motivait