

Quality and Information Security Policy

Quality and Information Security Policy

Clorian, as a company dedicated to developing a technology platform for the comprehensive management of ticket sales, openly states its intention to provide competitive services to all its customers. For this reason, it has implemented a Quality and Information Security Management System.

The main objective is to achieve the level of satisfaction expected by customers through established processes based on continuous improvement, ensuring the continuity of information systems, minimising the risk of damage and meeting the objectives set to guarantee the confidentiality, integrity and availability of information at all times.

To this end, Clorian is committed to quality and information security in accordance with the ISO 9001 and ISO 27001 reference standards, as well as the Spanish National Security Framework. Accordingly, the Management Committee establishes the following principles:

- **Competence and leadership by the Management Committee as a commitment to developing the Quality and Information Security Management System.**
- Identify the internal and external interested parties that are relevant to the quality management system and meet their requirements.
- Understand the organisation's context and determine its opportunities and risks as a basis for planning actions to address, accept or treat them.
- Ensure the satisfaction of our customers, including the interested parties concerned with the company's results, in all matters relating to the performance of our activities and their impact on society.
- Establish objectives and targets focused on evaluating quality performance and continuously improving our activities, as governed by the Management System that implements this policy.
- **Comply with the legal and regulatory requirements applicable to our activities, the commitments made to customers and interested parties, and all internal rules or operating guidelines to which the company is subject.**
- **Ensure the confidentiality of the data managed by the company and the availability of information systems, both in the services provided to customers and in internal management, while preventing unauthorised alterations to information (integrity).**
- Ensure the ability to respond to emergency situations by restoring the operation of critical services as quickly as possible.
- Establish appropriate measures for treating risks arising from the identification and assessment of assets.
- **Motivate and train all personnel working in the organisation, both to perform their duties correctly and to act in accordance with the requirements imposed by the relevant standard, providing a suitable environment for the operation of processes.**

- Maintain effective communication both internally, among the different levels of the company, and with customers.
- Assess and ensure the technical competence of personnel in performing their duties, and ensure they are appropriately motivated to participate in the continuous improvement of our processes.
- **Ensure that the facilities are properly maintained and that suitable equipment is available in line with the company's activities, objectives and targets.**
- Ensure the continuous analysis of all relevant processes and implement the appropriate improvements in each case, based on the results obtained and the objectives established.

This document has been approved by Management.

Document control

Date	Version
09/02/2026	1.2