



Quality and Safety Policy

Quality and Safety Policy

Clorian, as a company dedicated to the development of a technological platform for the integral management of ticket sales, openly states its intention to offer competitive services to all its clients; for this reason, it has implemented a **Quality and Information Security Management System**.

The main objective is to achieve the satisfaction expected by customers, through established processes based on a process of continuous improvement, guaranteeing the continuity of the information systems, minimising the risks of damage and ensuring compliance with the objectives set to ensure the confidentiality, integrity and availability of the information at all times.

To this end, it assumes its commitment to quality and information security in accordance with the reference standards **UNE/EN-ISO 9001:2015 and ISO /IEC 27001:2013**, for which the Management Committee establishes the following principles:

- **Competence and leadership** by the Management Committee as a commitment to develop the Quality and Information Security Management System.
- Identify **internal and external stakeholders** that are relevant to the quality management system and meet their requirements.
- Understand the **organisational context** and identify organisational opportunities and risks as a basis for action planning to address, assume or deal with them.
- Ensure the **satisfaction of our customers**, including stakeholders in the company's performance, in all aspects of the conduct of our business and its impact on society.
- Establish **objectives and goals focused on the evaluation of performance** in terms of quality, as well as continuous improvement in our activities, regulated in the Management System that develops this policy.
- **Comply** with the requirements of the legislation applicable and regulatory to our activity, the commitments acquired with clients and interested parties and all those internal rules or guidelines for action to which the company is subject.
- **Ensure the confidentiality** of the data managed by the company and the availability of the information systems, both in the services offered to clients and in internal management, avoiding undue alterations to the information (integrity).
- Ensure the **capacity to respond to emergency situations**, re-establishing the operation of critical services in the shortest possible time.

- Establish the appropriate measures for **the treatment of risks** derived from the identification and evaluation of assets.
- **Motivate and train** all personnel working in the organisation, both for the correct performance of their job and to act in accordance with the requirements imposed by the reference standard, providing a suitable environment for the operation of the processes.
- Maintain fluid **communication** both internally, between the different levels of the company, and with clients.
- Evaluate and **guarantee the technical competence of the personnel** for the performance of their functions, as well as ensuring adequate motivation for their participation in the continuous improvement of our processes.
- **Guarantee** the correct **state** of the **facilities** and the appropriate **equipment**, in such a way that they are in correspondence with the activity, objectives and goals of the company.
- Guarantee a **continuous analysis** of all relevant processes, establishing the relevant improvements in each case, depending on the results obtained and the established objectives.

Documentary control

Date	Version
22/01/2024	1.1