ENS TP INFORMATION SECURITY POLICY

TP, as a company dedicated to customer service, commercial service, technical support, back office, complaint and quality management, collections/billing/retention, consulting and digital marketing, has implemented an information security management system whose main objective is to guarantee at all times the security of the information of its customers and its own 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 information security in accordance with the reference standard to Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme, for which the Directorate-General establishes the following principles:

- **Competence and leadership** on the part of the management as a commitment to develop the Information Security Management system.
- Determine the internal and external stakeholders that are relevant to the Information Security Management System and meet their requirements.
- Understand the **context of the organization** and determine the opportunities and **risks** of the organization with respect to information security as a basis for planning actions to address, assume or treat them.
- To ensure the **satisfaction of our customers**, including stakeholders in the company's results, in everything related to the performance of our activities and their impact on society.
- Establish **objectives and goals** focused on the evaluation of performance in the field of Information Security, as well as continuous **improvement** in our activities, regulated in the Management System that develops this policy.
- Compliance with the requirements of the **applicable legislation and regulations** for our activity, the commitments made to customers and interested parties and all those internal rules or guidelines of action 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 offered to customers and in internal management, avoiding undue alterations in the information.
- Ensure the **capacity to respond to emergency situations**, restoring the operation of critical services in the shortest possible time.
- Establish the appropriate measures for **the treatment of risks** arising from the identification and evaluation of assets.
- **Motivate and train all personnel** working in the organization, both for the correct performance of their job and to act in accordance with the requirements imposed by the Reference Standard, providing an **adequate environment** for the operation of the processes.
- Maintenance of fluid **communication** both internally, between the different levels of the company, and with customers.
- To evaluate and guarantee the **technical competence of the personnel** for the performance of their functions, as well as to ensure their adequate motivation for their participation in the continuous improvement of our processes.
- Guarantee the **correct condition of the facilities and the appropriate equipment** , so that they are in accordance with the activity, objectives and goals of the company
- Guarantee a continuous **analysis** of all relevant **processes**, establishing the relevant improvements in each case, based on the results obtained and the established objectives.

These principles are assumed by the General Management, which has the necessary means and provides its employees with sufficient resources to comply with them, embodying them and making them publicly known through this ENS Information Security Policy.

	Fernando González Mesones **Chief Executive Officer** **TP Spain - 15.06.2026**