



INFORMATION SECURITY POLICY

The Management of NAVARRA DE TÉCNICAS DE SOLDADURA Y FIJACIÓN (TSF) approves this Information Security Policy as a top-level document of the Information Security Management System (ISMS), developed in accordance with the ISO/IEC 27001 standard and integrated with the organization's other management systems.

The activity of TSF, dedicated to the manufacture and supply of fasteners and fixing elements for sectors with high quality requirements, relies on information that is essential to produce and serve our customers: drawings and technical specifications, data of customers, suppliers, and our own personnel, as well as the management and plant systems that process it. Protecting this information, in any format and throughout its entire lifecycle, is a necessary condition to fulfill our commitments and to maintain the trust placed in us by customers, employees, suppliers, and other interested parties.

This Policy applies to all persons working at TSF or on its behalf, to the processes, systems, and work centers included in the scope of the ISMS, and to suppliers and third parties who access the organization's information or systems, under the terms agreed with each of them.

MANAGEMENT COMMITMENTS

- Preserve the confidentiality, integrity, and availability of our own information and that entrusted to us by customers, suppliers, and other interested parties.
- Comply with applicable legal, regulatory, and contractual requirements regarding information security, and in particular personal data protection regulations.
- Provide the ISMS with the human, technical, and financial resources necessary for its implementation, operation, and continual improvement.
- Establish information security objectives consistent with this Policy, measurable where possible, and review them within the framework of the Management Review. This Policy provides the framework for setting them.
- Integrate information security into organizational processes and business decisions, so that it forms part of the standard way of working at TSF.

GUIDING PRINCIPLES

- **Risk-based management.** Security controls are selected and prioritized based on periodic risk assessments, allocating resources where justified by risk and formally accepting residual risks.
- **Shared responsibility.** Information security concerns all individuals in the organization, each within the scope of their functions, and compliance forms part of job performance.
- **Justified access.** Access to information and systems is granted according to the needs of each role, kept up to date, and periodically reviewed.
- **Supply chain security.** Relationships with suppliers and third parties with access to TSF information or systems incorporate security requirements proportionate to the service provided.
- **Incident preparedness.** Security incidents are reported, recorded, and managed to limit their impact, recover activities within acceptable timeframes, and learn from them.



INFORMATION SECURITY POLICY

- **Security culture.** Personnel training and awareness are planned on an ongoing basis and sustain the effectiveness of all other measures.

ORGANIZATION AND RESPONSIBILITIES

Management approves this Policy and the risk acceptance criteria, and designates an Information Security Officer who coordinates the operation of the ISMS, supervises compliance with this Policy, and reports to the Integrated Management and Security Committee, the body in which Management monitors the system. This Policy is further developed through specific policies, procedures, and technical instructions, which are mandatory for the personnel to whom they apply.

COMPLIANCE, COMMUNICATION AND REVIEW

Failure to comply with this Policy or the internal regulations developing it may result in the application of the current disciplinary regime, in accordance with labor legislation and the applicable collective agreement.

This Policy is communicated to all personnel, made available to interested parties upon request, and reviewed at least once a year, or earlier if significant changes occur, to ensure it remains suitable for TSF's purpose and context.

Arazuri, julio 2026

