INFORMATION SECURITY POLICY

Rev. 07 – 29/08/2025

The organization Técnicas y Servicios de Ingeniería y Control del Norte SL (hereinafter, TESICNOR) is a company with its headquarters in Noáin, Navarra (Spain), dedicated to Development of Engineering projects, Supply of Safety Material, Teaching of OSH courses, Development of Industrial Safety projects, Installation and preventive and corrective maintenance, Occupational Safety, Document Management (BAC), Development, sale, implementation and maintenance of Computer Applications and Natural Disaster Risk Reduction (DRR).

TESICNOR has implemented an Information Security Management System in the processes of **Document Management (CAE), Development, sale, implementation and maintenance of computer applications (DEV), Development of industrial security projects (SIN)** and **Natural Disaster Risk Reduction (RDD),** based on the requirements of the UNE-EN ISO/IEC 27001:2023 Standard.

TESICNOR Management is committed to providing the necessary resources to comply with these and other applicable requirements, as well as those defined by clients and the applicable legal and regulatory requirements. Through this document, it wishes to express its conviction and commitment that:

- Information security is considered a key factor in the expansion, use, and dependence on a company's information technologies and must be assumed responsibly by all employees.
- TESICNOR complies with the obligations arising from the legislative development associated with the evolution of the information society.
- Protects and prevents the dissemination of confidential information to third parties, which requires the implementation of effective and reasonable security controls.
- It is committed to continuously improving the suitability, adequacy and effectiveness of the information security management system.

In this way TESICNOR assumes as main milestones:

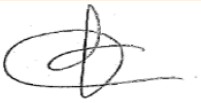
- The effectiveness of **security controls** in ensuring the confidentiality, integrity, and availability of information.
- Ensure the implementation, maintenance, and monitoring of information security policies.
- Compliance and knowledge of **obligations and functions** in relation to information security policies by employees.
- The correct **use, protection and valuation** of information assets by the assigned owner.
- Analyze and address security **risks and vulnerabilities** that may affect the proper functioning of the business and propose appropriate standards, means, and measures to minimize them.

- **Report** all actual or suspected **incidents** of abuse or theft of information assets, as well as potential threats or obvious weaknesses affecting security.
- Ensure the proper **classification and processing** of information.
- Achieve and maintain a level of security that guarantees adequate **business continuity** .
- Integration of the physical and logical aspects of information.
- Information security **training and outreach** plans to improve staff training.

The company's management is aware that it has ultimate responsibility for information security, and in this regard, provides and will provide all the necessary human, technical and financial resources to achieve this and will promote the principles that identify TESICNOR:

- **Work**: Staff willingness to competently meet customer requirements.
- **Respect:** Towards TESICNOR as an organization and towards all its members.
- **Innovation:** Active participation of TESICNOR staff in introducing new ideas aimed at increasing customer and staff satisfaction.

This policy is considered the basis for establishing and reviewing the company's information security objectives.



Santiago Pangua Cerrillo

Manager of Técnicas y Servicios de Ingeniería y Control del Norte SL