sener

Information security policy

Sener, an international engineering and technology company whose purpose is to transform the world by challenging the limits of technology, recognizes information security as an essential pillar to ensure the trust of its clients, partners, employees, and strategic collaborators.

Aware of the importance of protecting the confidentiality, integrity, availability, authenticity, and traceability of the information it manages, Sener's Management establishes this policy as a reference framework for the entire Group, reaffirming its commitment to the highest international standards in information security and cybersecurity.

Sener operates an Information Security Management System (ISMS) in accordance with ISO/IEC 27001 and the National Security Framework (ENS), ensuring a systematic approach to identifying, assessing, and treating the risks associated with the use of information and the systems that support it.

In line with the organization's mission, vision, and values, Sener's Management undertakes the following commitments:

- Protect Sener's information and that of its stakeholders against unauthorized access, loss, alteration, or destruction.

- Comply with applicable legal, regulatory, and contractual requirements related to security and personal data protection.

- Promote a culture of awareness and responsibility among all personnel, fostering best practices and continuous training. Implement appropriate technical and organizational measures according to the level of risk, ensuring the continuous improvement of controls and procedures.

- Ensure the effective management of security incidents and the continuity of critical services.

- Foster collaboration with suppliers and technology partners under equivalent security standards.

- Periodically review this policy and its effectiveness, ensuring alignment with corporate strategy and the evolution of the digital environment.

This policy is mandatory for all Sener personnel, as well as for external collaborators who access its systems or information. Management will provide the human, technical, and financial resources necessary to ensure compliance with these principles and the continuous improvement of the Information Security Management System (ISMS).

Sener makes this policy available to all its stakeholders as a reflection of its commitment to information security, cyber-resilience, and digital trust.

Jorge Sendagorta Cudós
Sener CEO