Enagás Cybersecurity and Data Governance Policy

This Policy includes the commitments that Enagás (the "Company") assumes in terms of Cybersecurity and Data Governance to comply with Cybersecurity standards and current legislation, providing greater certainty to the management of its assets and the achievement of its objectives.

Enagás considers that Cybersecurity has become a strategic pillar on which to base the digital revolution that all sectors of society have experienced, including the energy sector.

Additionally, data forms the basis of the Company's information assets and supports its business processes. Data must be governed securely and aligned with current legislation, to maximize its potential and its contribution to the Company's objectives.

This Policy applies to and is communicated to all employees, managers, and administrators of all companies that make up the Enagás Group, including those participating companies not integrated into the Group over which the Company has effective control, within the limits provided for in applicable regulations. In those participating companies in which the Enagás Group does not have effective control, it will be proposed to their Board to promote principles and guidelines consistent with those established in this Policy.

Likewise, the Company will also promote as far as possible the application of the principles of this Policy with respect to temporary business unions, joint ventures, and other associations or equivalent entities. In the case of contractors, suppliers, and those who collaborate with Enagás or act on its behalf, Enagás will promote principles and commitments consistent with this policy, with special emphasis on the supply chain.

Commitments

This Policy defines the governance model of Cybersecurity and Data Governance of Enagás, based on the following principles of action and commitments:

- All employees must collaborate with the correct implementation of Cybersecurity, participating in the necessary training and awareness, and being willing to prevent cyberattacks, identify and report any incident they are aware of, and provide an early response to any Cybersecurity breach.

- The data of Enagás and its subsidiaries are critical assets that must be governed and protected to ensure the Company's operations.

- Data must comply with the principle of quality, they must be adequate, representative, correct, and complete, they must always be real and guarantee their traceability.

- Enagás commits to adopting the necessary measures that guarantee ease of access, its ethical and appropriate use, in accordance with any applicable law, its confidentiality, protection, integrity, accuracy, quality, and consistency to facilitate decision-making, allowing the detection of possible deficiencies and their rectification.

- Enagás establishes the Data Governance function that will exercise authority and control over the management of data assets by coordinating the people, processes and technologies aimed at this purpose.

- Cybersecurity management will be based on the continuous measurement and management of risk, defining and adapting control measures in a way that allows the risk level to be maintained as acceptable or acceptable to the Company.

- The coordination and cooperation with public administrations, national and international organizations, suppliers, clients, etc., in order to promote the exchange of information and best practices in Cybersecurity. Likewise, all Cybersecurity incidents will be managed, escalating to the competent authorities those that are defined in the legislation and collaborating with any third party that allows optimal recovery after the same.

- The global control of the entire chain of processes involving supply chains in a global management of Cybersecurity.

Management Model

Enagás has established a Cybersecurity and Data Governance management model for the entire Society, aimed at compliance with the principles described in this Policy, which can be summarized in the following elements:

- The responsibility and leadership for the approval of risk management measures and continuous monitoring of the level of Cybersecurity falls on the Board of Directors, through the Audit and Compliance Committee, which is also responsible for ensuring that the necessary resources are available to implement and maintain adequate security measures, and that these measures are reviewed and updated regularly to respond to changing threats.

- A framework for the management of Cybersecurity and Data Governance based on continuous risk management aligned with the company's risk management model and with the business strategy and objectives, and consistent with the legislative framework where the Company's activities are developed.Mechanisms are in place to ensure that the objectives of Cybersecurity and Data Governance align with legislative, regulatory, and contractual requirements.

- The existence of mechanisms to align Cybersecurity and Data Governance objectives with compliance with legislative, regulatory and contractual requirements.
- The existence of a set of differentiated functions and responsibilities in terms of Cybersecurity and Data Governance clearly defined and assigned in the corporate organization chart, following a model of three separate lines of defense in execution, supervision and assurance.
- The establishment of a process of continuous review and updating of the Cybersecurity and Data Governance management model to adapt it at all times to the context of the organization, as well as the legislation and recommendations and best practices.

This Policy was approved by the Board of Directors of Enagás, on 22/04/2024