

General Information Security Policy

PC.CGEDx.SC.SDI.001.2025

Table of Contents

1. *Introduction* 3
2. *Scope* 3
3. *Guidelines* 3
4. *Commitments* 5
5. *Approval* 6
6. *Change Control* 6

1. Introduction

This General Information Security Policy establishes the reference framework and the principles that govern the protection of CGE's information assets, with the purpose of preserving their confidentiality, integrity and availability, as well as ensuring compliance with the applicable legal, regulatory and normative requirements regarding information security and cybersecurity.

2. Scope

Applies to CGE S.A. and all personnel authorized to access, use or process, at a functional or technical level the information assets of CGE including any third party, whenever they use CGE's systems or their own systems are linked to the organization's corporate network.

3. Guidelines

CGE's mission is to ensure solutions to customers and provide quality electricity supply. Likewise, CGE seeks to generate local identification through knowledge and integration with all the actors in the areas of the country where CGE is present.

To fulfill this mission, CGE recognizes that information is an essential asset for the continuity and excellence of operations, being its security a key pillar to maintain operational reliability, reduce risks and optimize performance, so it protects the information generated or obtained within the framework of its services, and that entrusted by customers, guaranteeing its confidentiality, integrity and availability throughout its life cycle by means of measures and controls that ensure the protection of critical systems, prevent incidents, reduce losses and strengthen customer confidence, promoting continuous improvement and adapting to the needs of the business.

This commitment is materialized through the implementation, maintenance and continuous improvement of an Information Security Management System (ISMS), based on a risk management approach, compliance with applicable legal, regulatory and normative requirements, and the adequate provision of resources. Likewise, a security-oriented organizational culture is fostered, promoting effective communication, continuous awareness and the active participation of stakeholders.

The following are the principles of action of this policy:

- Information security directly supports CGE's mission and strategic and operational objectives, contributing to ensure the safety, continuity, reliability and quality of products and services associated with the electricity market.
- Compliance with legal, regulatory, contractual and normative requirements applicable to information security and cybersecurity, including those specific to the energy sector.

- Continuous improvement of the Information Security Management System (ISMS), through performance reviews, audits, corrective actions and improvement opportunities.
- Security controls based on the identification, analysis, evaluation and treatment of risks that may affect CGE's information or critical processes.
- Confidentiality, integrity and availability of own information, customers, suppliers and third parties, throughout its life cycle and in all environments where it is processed, stored and / or transmitted.
- Information assets inventoried, classified and protected with security controls proportional to their classification level.
- Internal and external personnel periodically trained in secure practices, fostering co-responsibility and a culture of security in CEM.
- Adequate capabilities to detect, analyze, respond and recover from information security incidents, including subsequent learning mechanisms and resilience measures.
- Suppliers and third parties with access to CEM information and/or infrastructures that comply with the established security requirements, being evaluated and monitored on an ongoing basis.
- Integration of information security throughout the life cycle of new products, services, technologies or processes, minimizing vulnerabilities from their origin.
- Internal communication and availability of the policy to relevant stakeholders, promoting their understanding, implementation and feedback, as a basis for its continued effectiveness.
- Formal and updated contact channels with relevant authorities to report information security incidents, comply with legal obligations and anticipate regulatory changes.
- Active relationships with specialized information security groups, in order to access best practices, early warnings, technical advice and relevant news to strengthen its cybersecurity posture and capacity to respond to emerging threats.

4. Commitments

- Senior Management reaffirms its commitment through this policy, promoting its effective implementation through its communication, dissemination and periodic review, as well as by allocating the necessary resources and raising awareness among employees, customers and suppliers. This policy represents an institutional commitment to the continuous improvement of the processes and controls that protect the information of this organization.
- CGE aspires to achieve an optimal management in the field of information security, acquiring the following commitments:

1. Ensure that the information security policy is appropriate to the organization's purpose and compatible with its strategic direction.

2. Achieve the information security objectives, which must be established and aligned with the organizational strategic objectives and have their respective control and monitoring actions.

3. Ensure compliance with the requirements of ISO/IEC 27001, as well as legal, regulatory and contractual requirements related to information security that apply to the organization.

4. Continuously improve the information security management system, and ensure the dissemination, communication and updating of the information security policy in the face of regulatory, technological or organizational changes.

5. Ensure that the information security policy is available as documented information, is communicated within the organization and is available to stakeholders relevant to the information security management system.

- Senior Management, in conjunction with the Centralized Services, Operations and Equipment Management, Commercial and Customer Service, and Quality and Operational Control Departments, will lead the teams that make up the information security management system to achieve the intended results, ensure compliance with applicable requirements, and promote continuous improvement throughout the organization and its value chain.

5. Approval

The General Information Security Policy has been approved by the Executive Committee of Compañía General de Electricidad S.A., dated December 18, 2025.

6. Change Control

Edition	Date	Reasons for the edition and/or summary of changes
1	**28/11/2025**	Initial edition of the document.