nexus energía

Information Security Policy

Ref.: PO – 002 – GNE

General Management approved the Information Security Policy on 31 July 2019
and its latest version on 4 May 2026 - Version 7

Property of Nexus Energía – Total or partial reproduction of this document is prohibited.

CONTENTS

1 INTRODUCTION

2 OBJECTIVE

3 SCOPE

4 LEADERSHIP AND MANAGEMENT COMMITMENT

5 APPLICABLE EXTERNAL REGULATIONS

6 APPLICABLE INTERNAL REGULATIONS

Introduction

Introduction

Protect and secure information

Key asset

Appropriate processing

Confidential

Nexus Energía, S.A. (hereinafter, Nexus) is an electricity and natural gas retailer and, as such, we define ourselves as a service company. Consequently, in addition to the employees who make up Nexus, our main assets are intangible in nature and therefore consist of confidential information, personal data and know-how, among others.

Therefore, the protection and security of the information we handle is key, and we are committed to organising our processes through the establishment and application of an internal regulatory framework that allows us to protect and ensure that the information and personal data of our stakeholders are processed appropriately.

Objective

Objective

The objective of this policy is to provide guidance on how Nexus approaches information security management in accordance with business requirements and the applicable standards. To this end, **ISO 27001, complemented by ISO 27002, is used as the reference framework**. This policy is developed through various internal regulations that guide all employees in complying with the aforementioned ISO standards, the laws and regulations on personal data protection and the contractual obligations undertaken, and in applying best practices in information security and data protection.

At all levels of Nexus, the **real and effective application of the prevention and control measures** set out in this policy and in all the internal regulations that develop it shall be ensured.

The actions arising from the application of the regulatory framework seek the **achievement of the strategic objectives** defined by the organisation within a **process of continual improvement** and in line with the information security requirements set out in ISO 27001.

Nexus's security objectives are aligned with its business objectives, giving priority to compliance with the legal obligations applicable to the activity carried out, preserving the confidentiality, integrity, availability, authenticity and traceability of information, and providing stakeholders with confidence in the proper management of risks.

Scope

Scope

Information systems

The scope of the Information Security Management System (ISMS) to be certified under ISO 27001 is as follows:

The information systems that support the retail supply of electricity and gas in the Processing, Meter Reading, Billing and Collections Management processes.

The information systems that support electricity market representation services in the sales, contracting, metering, billing, payments and producer support processes.

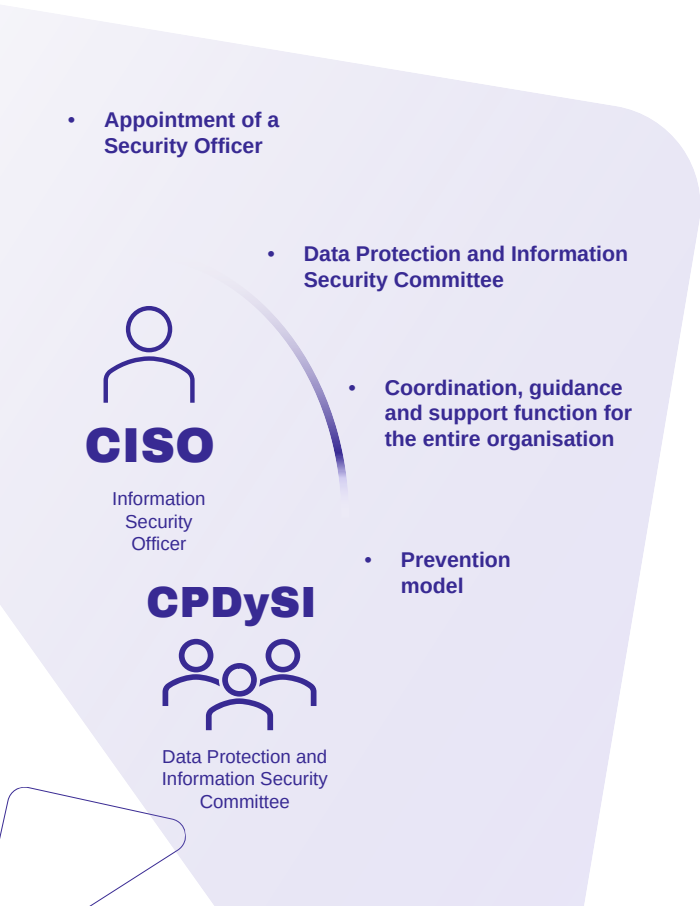
The information systems that support the portfolio management, physical markets and financial markets processes.

The information systems that support the corporate processes of people management, marketing, accounting and finance, information systems, legal services, GRC and internal audit.

The information systems that support the Secondary Concentrator services and processes.

Leadership and management commitment

Leadership and management commitment



Nexus management is committed to facilitating and providing the necessary resources for the establishment, implementation, maintenance and improvement of the organisation's ISMS, as well as to **demonstrating leadership and commitment** with respect to it, **through the appointment of a Security Officer and the establishment of the Data Protection and Information Security Committee.**

This Committee has a **coordination, guidance and support function for the entire organisation**, and especially for those responsible for control functions. It coordinates the preventive function of the **prevention model** described in Nexus's data protection and security policies. It is a body with autonomous powers of initiative and control, reporting to the Nexus Board of Directors through its Audit and Sustainability Committee. Its responsibilities also include:

- **Ensuring that the necessary resources** for the ISMS are available.
- **Communicating and disseminating the policies** related to the ISMS within the organisation and to stakeholders.
- **Ensuring that the ISMS achieves its intended outcomes**.
- Promoting the **continual improvement of the ISMS**.
- Reviewing the policy whenever significant changes occur, or at least once a year.

Applicable External and Internal Regulations

Applicable External Regulations

EXTERNAL REFERENCE REGULATIONS

- Regulation (EU) 2016/679 of 27 April, General Data Protection Regulation (GDPR).
- Organic Law 3/2018 on the protection of personal data.
- Royal Legislative Decree 1/1996 on the Intellectual Property Law.
- Royal Decree 3/2010 of 8 January regulating the National Security Framework (ENS), as amended by Royal Decree 951/2015 of 23 October (in relations with the public sector).
- Spanish Criminal Code.

EXTERNAL REFERENCE FRAMEWORKS

- ISO 27001.
- ISO 27002.

Applicable Internal Regulations

This policy is developed through various internal regulations, most notably:

- **Detailed Information Security Policy:** intended to provide detailed guidance for everyone in the organisation on how information security must be managed. It describes the key human, organisational, technological and documentary elements that Nexus applies to protect information, and especially personal data, preventing security incidents that could put them at risk.

- **Data Protection Policy:** its purpose is to establish the guidelines to be followed regarding data protection. This policy describes the key human, organisational, technological and documentary elements that NEXUS applies to protect personal data, preventing infringements of the rights and freedoms of data subjects.

- **Rules for the use of Information and Communication Technology resources:** intended to regulate the use of ICT resources by their users, both internal and external, and to guarantee their security, as well as that of the personal data and confidential information they hold.

- **Information security incident management procedure:** intended to define the actions to be taken in the management, assessment and, where applicable, notification of a security incident involving a potential personal data breach.

nexus
energía