Information Security Policy

Table of contents

Information Security Policy

1. Purpose

The purpose of **the Dia Group Information Security Policy** is to set out the guidelines intended to protect the Company's information and that of its stakeholders, as well as the assets that process, transmit and/or store it.

This Policy must be supplemented by and governed by all other internal standards, regulations and policies of the same or similar nature as this Policy.

Moreover, the Policy aims to make clear the commitment of the Management, the Board of Directors and their delegated commissions to information security.

2. Scope of Application

The Information Security Policy applies to all companies belonging to Grupo Dia and has the following scope:

- Corporate information of any nature and in any format.
- Personal information of employees and third parties (such as franchisees, suppliers and customers).
- Physical assets (hardware).
- Digital assets (software).
- Communications networks.
- Employees.
- Third parties (suppliers, creditors and franchisees).
- Premises (e.g. offices, warehouses, stores, data centres, etc.).

2.1. Distribution and Control

The Information Security Policy must be disseminated, distributed and provided to all employees and subcontractor staff in an official Grupo Dia repository.

All employees and associated third parties who have access to Grupo Dia assets and/or data (personal and/or business) are obliged to be aware of and comply with the Information Security Policy.

3. Information Security Strategy

The information security management strategy has risk management at its core, and seeks to establish technical and operational measures that enable:

- **Identification** of Grupo Dia's critical processes and assets.
- **Protection** through measures and controls that reduce the likelihood of risk events occurring.
- **Detection** of any event that compromises the security of information and business processes.
- **A Response** to incidents to prevent their spread and reduce or eliminate the impact.

- **Recovery** of processes and assets to normal levels following a security incident.

For this purpose, Grupo Dia Management, with the support of the Information Security team, must oversee the governance of the cybersecurity strategy and the management of the risk lifecycle established within the organization.

4. General Guidelines

Grupo Dia's information security strategy is implemented using the following processes:

- Roles and responsibilities.
- Internal and external communications.
- Human resources security.
- Training and awareness.
- Classification of information.
- Asset management.
- Vulnerability management.
- Identity and access control management.
- Protection of data when stored and transmitted.
- Physical security.
- Operational security.
- Telecommunications security.
- Project and development security.
- Security with third parties.
- Security monitoring.
- Security incident management.
- Legislative and regulatory compliance.
- Continuous monitoring and improvement.

The information security strategy at Grupo Dia is carried out and applied in compliance with current regulations, especially on matters of Information Security and Privacy/Personal Data Protection.

The security levels applicable to Grupo Dia's data, assets and environments are defined and applied according to:

- Business needs.
- Criticality of assets and information.
- The need for confidentiality, integrity and availability.

This Policy has been approved on 12 December 2024 by the Board of Directors of Distribuidora Internacional de Alimentación S.A. and is applicable until the Board of Directors approves its update, review or repeal.