CYBERSECURITY POLICY

GRUPO ARGOS

Investments that transform

1. GENERAL OVERVIEW

1.1. Purpose

The purpose of the Occupational Health and Safety Policy is to establish the guiding principles and guidelines on Occupational Health and Safety for Grupo Empresarial Argos.

1.2. Scope

The Occupational Health and Safety Policy is applicable to all operations, employees and contractors, regardless of the region or country where they operate.

Each of the companies will have its own policy that will be adjusted to the reality and needs of each of the organizations, however, all must respect the framework of this policy.

2. CYBERSECURITY POLICY

Grupo Argos in compliance with laws and regulations for the protection of information assets[1] physical, digital and cyber assets[2] in the countries of operation and according to its technology policy; identifies, manages and mitigates associated risks by implementing best practices in cybersecurity[3] seeking to guarantee the confidentiality, integrity and availability of information, information technologies and operations technologies; to ensure the sustainability of business and the safety of people.

Regarding cybersecurity, the company, its employees, and third parties involved with digital assets commit to:

▪ Ensure that the cybersecurity policy is aligned with the company's objectives and is a mechanism to contribute to the permanence and value of the organization.

▪ Actively support cybersecurity within the organization to comply with relevant standards and achieve defined objectives, considering that cybersecurity is a shared responsibility among all members of the organization.

▪ Adopt a risk management-based approach that allows the company and its employees to freely, securely, and reliably carry out their activities in the digital environment.

▪ Use all information stored, created, or transmitted using Grupo Argos resources exclusively for the organization's purposes and business objectives.
▪ Maintain an up-to-date inventory of information assets and existing cyber assets, including their classification and ownership.

[1] Information asset: Set of data collected and transformed that have a value for the business of a strategic, operational, economic, technical, legal or regulatory type; therefore, its need to protect them.

[2] Cyberasset: Devices and communications systems, including hardware, software, data and information. As well as those elements with routable communication protocols, which allow access to the information locally or remotely.

[3] Digital security: Principles that guide information protection measures, information technologies, operating technologies, internet of things in the environment of digital transformation.

- Establish controls to prevent loss, damage, theft, or malfunction of information assets and cyber assets that may lead to business disruptions or harm to the organization through the identification, assessment, and treatment of risks, threats, and vulnerabilities in information and operational systems.

- Ensure the establishment of measures for the proper functioning of the technological infrastructure to guarantee the confidentiality, integrity, and availability of information assets and cyber assets, including measures that ensure the non-repudiation of actions by internal and external actors in the digital environment.

- Engage employees and third parties involved in the digital environment to understand and apply controls to protect information assets and cyber assets, reducing the risk of human errors, theft, fraud, or misuse.

- Access only information related to their job functions and responsibilities. Third parties requiring access to information systems only access the information necessary for the execution of their contractual obligations.

- Disseminate and promote, in a planned manner, the objective of cybersecurity, its characteristics, and individual responsibilities to achieve it, including annual training plans, as well as ongoing activities and induction processes for new staff.

- Effectively manage cybersecurity incidents to minimize the risk of loss of availability, confidentiality, reliability, and integrity of information assets and cyber assets, and to identify the controls to be implemented.

- Ensure that all critical processes and information systems containing information assets have continuity plans that ensure resilience and timely recovery according to business requirements.

- Promote the responsible use of artificial intelligence tools, ensuring their implementation with appropriate security measures to protect the integrity and confidentiality of the data.

- Ensure that the use, operation, and management of information systems comply with the requirements of applicable national and international laws regarding software licensing, copyright, information privacy, information record retention, and all current legal provisions.

- Respect the privacy of customers, employees, suppliers, and other third parties associated with Grupo Argos, and take reasonable measures to guarantee the security of personal data collected, stored, processed, disclosed, and transmitted.

- Collaborate with the technology department in the development, adoption, or procurement of new applications or technological services, ensuring compliance with cybersecurity guidelines and standards, and their proper integration with the company's solutions ecosystem.

- Comply with the cybersecurity policy and its guidelines. Any violations by employees and third parties involved with digital assets will result in incident treatment measures and disciplinary actions by the human resources department.
- Ensure information security and operational continuity by investigating the digital behavior of users, carried out by internal control and cybersecurity departments.

3. CYBERSECURITY GOVERNANCE

GRUPO ARGOS S.A. and its related companies have defined the following organizational structure with instances, roles and responsibilities, in order to ensure adequate compliance with the cybersecurity policy.

Audit, Finance and Risk Committee:

The main purpose of the Committee is to evaluate the accounting procedures, the management of the relationship with the Statutory Auditor and to supervise the effectiveness of the control architecture and the risk management system, including Cyber Risk.

Tactical Cybersecurity Committee:

- Approve the organizational strategy that provides direction in cybersecurity management.

- Approve the cybersecurity policy and its guidelines.

- Manage the cybersecurity risk map and evaluate the effectiveness of treatment measures taken.

- Ensure the adoption of recommendations issued by regulatory bodies, auditors, insurance companies, risk areas, among others.

- Propose guidelines to materialize the cybersecurity policy.

- Propose the intrusion testing program and simulations for cyber attacks.

- Adjust the training and awareness program for all members of the organization.

- Design and implement comprehensive communication and training programs to strengthen the culture and capabilities of the cybersecurity management system.

- Communicate and report the organization's cybersecurity status to senior management and other key members of the organization.

Owners of Information and Cyber Assets: Responsible for the assets assigned to them, as well as the classification, control, and monitoring of the use and management of these assets.

Custodians of Information and Cyber Asset: Responsible for safeguarding the assets, enforcing access restrictions and classifications given by the owners.

Control Areas (Risk, Audit): Responsible for managing and evaluating the measures taken to mitigate the risk associated with cybersecurity.

Chief Information Security Officer (CISO): Responsible for developing the comprehensive cybersecurity management model, framing the cybersecurity policy within this ecosystem, and managing the risks associated with information security and cybersecurity.
Users: Any employee, supplier, contractor, or other authorized third party who uses the companies' information in the execution of their daily work activities.

4. ANNEXES AND REFERENCES

- Norma NIST Cybersecurity Framework CSF
- ISO 27000 standards
- Laws and regulations
- Cybersecurity guidelines and annexes
- Personal Data Treatment Policy

5. EXCEPTIONS

Not applicable.

6. POLICY REVIEW PERIODICITY

Every year or as required.

7. APPROVED BY

Approval instance: Tactical Cybersecurity Committee
Review: Chief Information Security Officer

VERSION CONTROL

No.	Capítulo	Fecha	Descripción Versión / Cambios
V_001	All	February, 2015	• Initial Issue
V_002	All	February, 2022	• Adjustments to improvement opportunities - Audit of the process
V_003	All	June, 2023	• General definitions - Approval Instance
V_004	All	February, 2024	• Adjustment on Artificial Intelligence in Cybersecurity