ARTIFICIAL INTELLIGENCE POLICY

GRUPO ARGOS

Investments that transform

1. OBJECTIVE

Establish frameworks and guidelines for the ethical, responsible, and secure development, implementation, and use of artificial intelligence (AI) across Grupo Argos S.A. and its subsidiaries. This policy guides the behavior of employees and third parties in relation to AI systems, ensuring compliance with applicable laws and regulations, transparency, risk and bias mitigation, protection of personal data and environmental responsibility. It provides clear guidelines for the adoption of technical and organizational measures to ensure the cybersecurity and integrity of AI-driven processes.

2. GLOSARY

- **Artificial Intelligence (AI):** Artificial intelligence refers to the simulation of human intelligence processes by computer systems. These processes include learning (the acquisition of information and rules for using it), reasoning (using rules to reach approximate or definitive conclusions), and self-correction.
- **AI Systems:** An AI system is any system that uses artificial intelligence technology to perform tasks that normally require human intelligence, such as speech recognition, decision-making, language translation, and visual perception. These systems can be software, hardware, or a combination of both.
- **AI Technology:** AI technology encompasses the tools, techniques, and methodologies used to develop and operate artificial intelligence systems. This includes machine learning algorithms, neural networks, natural language processing, and computer vision, among others.
- **AI Application:** An AI application is a specific use of artificial intelligence technology to solve problems or improve processes in various areas, such as healthcare, education, manufacturing, commerce, security, and many other fields. Examples include virtual assistants, recommendation systems, and predictive analytics.
- **Data bias:** Data bias occurs when the data used to train an AI model does not adequately represent the population or phenomenon being analyzed. This can result in models producing unfair or inaccurate results, inadvertently favoring, or disadvantaging certain groups. The cause of the bias can be in data collection, sampling, annotation, or processing.
- **Algorithm:** An algorithm is a finite sequence of steps or instructions followed to solve a problem or perform a specific task. In the context of AI, algorithms are fundamental to the development of machine learning models and other artificial intelligence applications.
- **Machine Learning:** Machine learning is a branch of artificial intelligence that focuses on the development of algorithms and techniques that allow computers to automatically learn and improve based on experience without being explicitly programmed for each task. This is achieved by analyzing substantial amounts of data and identifying patterns.
- **Neural Networks:** Neural networks are a type of machine learning algorithm inspired by the workings of the human brain. They consist of layers of nodes (or "neurons") that process information and can learn to perform complex tasks by adjusting the connections between nodes in response to input data.

- **Natural Language Processing (NLP):** Natural language processing is a subdiscipline of artificial intelligence that deals with the interaction between computers and humans using natural language. The goal of NLP is to enable machines to understand, interpret, and respond to human language input in useful and meaningful ways.
- **AI Ethics:** AI ethics refers to the principles and guidelines that should be followed in the development and deployment of artificial intelligence technologies to ensure they are fair, transparent, and benefit society. This includes considerations of privacy, fairness, accountability, and bias mitigation.
- **Human Oversight:** The requirement that qualified humans review, validate, and remain accountable for AI-generated outputs, particularly in high-impact decisions. Human oversight does not merely mean that a human is present in the process, but that they actively exercise judgment before an AI-generated outcome is acted upon.
- **Prohibited AI Systems:** AI applications banned due to their potential to infringe fundamental rights, as defined by the EU AI Act (Regulation 2024/1689) and by this policy. Examples include mass biometric surveillance systems, social scoring systems, and AI systems designed to manipulate or exploit human vulnerabilities.
- **Ecological Footprint of AI:** The environmental impact associated with the computational resources required to train, run, and maintain AI systems, including energy consumption, water use, and carbon emissions from data centers.
- **Institutional AI Accountability:** The organizational responsibility for the outcomes and behavior of an AI system in production, assigned to a designated business owner and technical owner — as distinct from the individual-level responsibility of users for the outputs they generate.

3. SCOPE

This artificial intelligence policy applies to all areas and departments of Grupo Argos S.A. and its subsidiaries (Cementos Argos, Celsia, Odinsa and Summa), including the development of new AI systems or applications, the implementation of existing AI systems, the updating or modification of AI systems in use, and any other process involving the use, application, or integration of artificial intelligence technologies. Likewise, this policy must be respected by all employees, as well as by all people or entities that develop, implement, use, or interact with artificial intelligence systems in the companies.

4. POLICY

Grupo Argos S.A. and its subsidiaries (Cementos Argos, Celsia, Odinsa and Summa), in compliance with applicable laws and regulations, are committed to using Artificial Intelligence (AI) responsibly and ethically, seeking to obtain operational and business benefits, while protecting the rights and safety of its employees, customers, and other stakeholders.

By implementing AI governance and risk management practices, Grupo Argos S.A. and its subsidiaries will identify, assess, and mitigate potential adverse impacts in areas such as privacy, equity, transparency, and accountability. Furthermore, the Business Group will ensure that the development and use of AI systems is aligned with the ethical and human rights principles established in the policies and guidelines framed within the companies' corporate governance.

Regarding the use of Artificial Intelligence, companies, their employees and third parties undertake to:

4.1. Governance and Accountability Framework

- Establish a clear governance and accountability framework for the development, implementation, and use of AI systems. This framework should consider best practices and be periodically updated based on evolving technologies, related risks, and applicable regulations.
- Promote responsible use of artificial intelligence technologies, ensuring their implementation with appropriate security measures to protect confidentiality, integrity, and availability of data.
- Embrace an organizational culture that promotes the trustworthy and beneficial use of AI by providing training and resources to its employees.
- Define institutional accountability for AI models deployed in production: each AI system must have an identified business owner (responsible for outcomes and use cases) and a technical owner (responsible for performance, drift, and maintenance). Accountability does not rest solely with individual users but with the organizational entity that authorizes and deploys the system.

4.2. Data Privacy and Personal Data Protection

- Adopt technical and organizational measures to ensure the protection of personal data processed by AI systems, respecting individuals' right to privacy, including strict measures to prevent information leakage in AI applications and ensuring that sensitive and confidential data is not exposed or misused. Data subjects shall have the right, at any time and without restriction, to obtain information about the processing of their personal data by data controllers. This includes details about the type of data processed, the purposes of the processing, the security measures implemented, and the rights of data subjects in relation to their personal data.
- Process personal data according to the principles of suitability, necessity, reasonableness, and proportionality to ensure that the data is used appropriately and without disproportionately affecting the rights of individuals.
- Comply with the principle of privacy by design and by default, ensuring that privacy and data protection are incorporated from the initial stages of AI systems development.
- Develop and operate all AI systems in compliance with applicable data protection and privacy laws and regulations, ensuring transparency about the use of AI in business processes.

4.3. Bias Mitigation and Risk Assessment

- Conduct comprehensive impact assessments of AI systems to identify and mitigate potential risks, harms, and biases in data, algorithms, and outcomes, to avoid discrimination and unfair treatment.
- Identify and classify high-risk AI systems used in the organization (for example, in critical areas such as technological infrastructure, human management, judicial processes, etc.) and comply with the obligations established for these systems, such as risk assessment, privacy impact assessment, usage logging, human oversight, etc.

4.4. Transparency and Explainability

- Implement transparency mechanisms that allow users to clearly identify when they are interacting with or making decisions about content generated by AI systems, establishing processes to clearly label text, images, audio, video, and communications generated and/or manipulated by AI systems.

4.5. Human Oversight in Critical Decisions

Artificial intelligence is a tool to support human work. It does not replace professional judgment or the formal decision-making processes of the organization. Specifically:

- All AI-generated content, analyses, or recommendations that inform significant business, financial, legal, or operational decisions must be reviewed and validated by a qualified human before being adopted as a final output.
- In high-risk AI applications — including those affecting hiring, performance evaluation, credit assessment, legal compliance, or critical infrastructure — human intervention must be formally embedded in the process. No automated decision in these domains may be executed without human review and explicit approval.
- Employees retain the right to escalate any AI-generated output they believe is inaccurate, biased, or inconsistent with the organization's values. A designated review path must be established by the AI Governance Officer for such escalations.
- The deployment of AI as an autonomous agent capable of executing consequential actions without human approval is subject to explicit authorization by the AI Ethics and Governance Committee, with documented safeguards in place.

4.6. Permitted and Prohibited Uses of AI

The following uses of AI are permitted within the organization, subject to the conditions set forth in this policy and applicable internal guidelines:

- Drafting, summarizing, and improving documents, reports, presentations, and internal communications.
- Analyzing and processing non-confidential or properly anonymized data to generate insights.
- Supporting learning, research, and knowledge exploration activities.
- Automating repetitive, low-risk administrative tasks with appropriate human oversight.

- Developing AI-powered solutions for operational improvement, subject to governance and review processes established by the Center of Excellence for Data and AI.

The following uses of AI are expressly prohibited:

- Generating discriminatory, biased, offensive, or reputationally harmful content against individuals, communities, or the organization.
- Simulating communications as if originating from another person (identity impersonation).
- Bypassing internal controls, audit trails, or compliance mechanisms of the organization.
- Processing classified sensitive business information through unauthorized or non-enterprise AI tools.
- Deploying AI systems that engage in manipulative, exploitative, or deceptive behavior toward users or third parties.
- Using AI for surveillance or monitoring of individuals without explicit legal basis and appropriate disclosure.

4.7. Environmental Responsibility and Ecological Footprint

Grupo Argos S.A. and its subsidiaries recognize that the development and operation of AI systems require significant computational resources with associated environmental impacts. The organization commits to:

- Prioritizing AI infrastructure is hosted on cloud platforms with verified public commitments on environmental sustainability. The organization currently operates AI workloads primarily on Microsoft Azure, whose parent company Microsoft has: (i) publicly committed to becoming carbon negative by 2030 across all three emission scopes (Scope 1, 2 and 3); (ii) achieved, as of February 2026, 100% matching of its annual global electricity consumption with renewable energy through power purchase agreements (PPAs); and (iii) maintained an Environmental Management System independently certified under ISO 14001, the internationally recognized standard for environmental management.
- Incorporating environmental efficiency as a criterion in the evaluation and selection of AI platforms, models, and third-party AI service providers, with preference for providers that disclose and actively reduce the carbon footprint of their AI infrastructure.
- Tracking and reporting, to the extent feasible, the energy consumption and associated carbon footprint of material AI workloads, using data made available by cloud infrastructure providers.
- Aligning AI infrastructure decisions with the organization's broader climate strategy and Grupo Argos's sustainability commitments.

4.8. Prohibited AI Systems — Alignment with EU AI Act

- Employ subliminal techniques, manipulative strategies, or exploitation of cognitive vulnerabilities to influence individuals' behavior in ways that could cause them harm.

- Exploit the vulnerabilities of specific groups of people, including people with disabilities, children, or elderly individuals, in ways that distort their behavior and cause harm.
- Classify or score individuals based on their social behavior or personal characteristics in ways that result in detrimental or unjustified treatment (social scoring systems).
- Perform real-time remote biometric identification of individuals in publicly accessible spaces for law enforcement or surveillance purposes, except where expressly permitted by applicable law.
- Make fully automated decisions with significant effects on individuals — including employment, credit, access to services, or legal proceedings — without meaningful human review and a clear appeals mechanism.

5. AI GOVERNANCE

Grupo Argos S.A. and its subsidiaries (Cementos Argos, Celsia, Odinsa and Summa) define the following organizational structure with entities, roles, and responsibilities to ensure proper compliance with the Artificial Intelligence policy.

AI Ethics and Governance Committee

- Review, approve, and monitor the use of AI.
- Define the responsibilities and roles of the different departments and teams involved in the AI systems lifecycle (e.g., IT, Legal, Human Resources, Ethics/Compliance).
- Define a periodic review and update process for this policy, considering regulatory, technological, and best practice changes in the field of AI.
- Detail the measures that will be taken in case of non-compliance with the guidelines established in this policy.
- Establish the consequences and disciplinary sanctions applicable to serious violations.
- Authorize high-risk AI deployments and autonomous AI agents that require enhanced oversight mechanisms, as defined in section 4.5 of this policy.

AI Governance Officer

- Oversaw the implementation and enforcement of AI policy.
- Maintains the organizational AI system registry, documenting the business owner and technical owner for each AI system in production.
- Manages the escalation path for employees wishing to contest AI-generated outputs or flag potential policy violations.

Business and Technical AI Owners

- Each AI system deployed in production must have a designated business owner (accountable for outcomes and use cases) and a technical owner (accountable for model performance, drift, and maintenance). These roles are documented in the AI system registry maintained by the AI Governance Officer.

Users

- Any collaborator, supplier, contractor, or other authorized third party who uses the companies' information in the execution of their daily work activities.

6. EMPLOYEE TRAINING AND AI LITERACY

6.1. Training Commitments

Grupo Argos S.A. and its subsidiaries are committed to building responsible AI literacy across the organization. Specific initiatives include:

- Mandatory training on the ethical use and security of AI for all employees who use AI tools in their daily work.
- Role-specific training for AI developers, data scientists, and technical staff on responsible AI design, bias testing, and model governance.
- A Citizens Developers program enabling non-technical employees in all business areas to build AI-assisted solutions within a governed framework, with advisory support from the Center of Excellence for Data and AI.
- Annual review of training content to reflect new regulatory requirements, organizational AI deployments, and emerging risks.

7. ANNEXES AND REFERENCES

- Artificial Intelligence Law – European Union Regulation
- Draft AI Bill of Rights – United States
- Cybersecurity Policies
- Personal Data Processing Policies – Applicable in the countries of influence of the business group
- National Policy for Digital Transformation and Artificial Intelligence (CONPES 3975) – Colombia
- External Circular 02 of 2024 – Superintendency of Industry and Commerce - Colombia
- Code of Conduct of the companies of the business group - GRUPO ARGOS S.A. and its subsidiary companies (Cementos Argos, Celsia, Odinsa, Summa)
- Artificial Intelligence Guidelines
- Acceptable Use Guidelines for Artificial Intelligence — Summa (internal document, 2026)
- EU Artificial Intelligence Act — Regulation 2024/1689 (explicit reference added in v2026)
- Microsoft environmental commitments — three primary sources for section 4.7 evidence: (1) Carbon negative journey and 100% renewable energy milestone (Feb 2026): https://blogs.microsoft.com/blog/2026/02/18/a-milestone-achievement-in-our-journey-to-carbon-negative/ | (2) Azure datacenter sustainability page: https://datacenters.microsoft.com/sustainability/ | (3) ISO 14001 Environmental Management System certificate: https://www.microsoft.com/en-gb/legal/compliance/environmental-compliance

8. VERSION CONTROL AND APPROVAL

Approval instance: The Artificial Intelligence Policy is approved by the AI Ethics and Governance Committee, and its implementation is supervised by Grupo Argos' Board of Directors and its subsidiary companies (Cementos Argos, Celsia, Odinsa, and Summa), ensuring that the Board of Directors are the highest endorsing decision-making body.

Review frequency: Every year or whenever required.

VERSION CONTROL

No. Rev.	Chapter	Date	Author	Description
V_001	All	April 2024	Cybersecurity Team	Draft - Initial Issue
V_002	All	July 2024	Cybersecurity Team	Shared in Cybersecurity committees
V_003	All	August 2024	Cybersecurity Team	Circular Recommendations Superintendency of Industry and Commerce
V_004	All	September 2024	Cybersecurity Team	Artificial Intelligence Guidelines
V_005	All	June 2026	AI CoE-Summa	CSA 2026 update: added 4.5 Human Oversight, 4.7 Permitted/Prohibited Uses, 4.8 Ecological Footprint; updated 4.9 EU AI Act prohibited systems; strengthened institutional accountability framework; updated Glossary with four added terms