I. PURPOSE AND SCOPE

This Policy establishes the guidelines governing the responsible promotion and use of Artificial Intelligence (AI) systems, with the objective of identifying, assessing, and mitigating the potential risks arising from their development and use. It also seeks to safeguard the rights and freedoms of individuals by ensuring that AI is used in accordance with the values set forth in our Code of Ethics and Conduct (CODEC), ethical principles, transparency, and applicable regulations.

This Policy applies to all employees, regardless of the nature of their employment relationship, as well as to all directors of Grupo UNACEM (hereinafter, the "Employees"), including employees and directors of UNACEM CORP S.A.A. and its subsidiaries (hereinafter, the "Business Units").

This Policy applies to all initiatives and projects that incorporate AI technology, whether developed internally or resulting from the acquisition, implementation, or integration of AI-based products, services, or solutions from external sources, as well as hybrid solutions.

Where the applicable laws of any jurisdiction in which Grupo UNACEM operates impose more stringent requirements than those set forth in this Policy, the applicable local legal provisions shall prevail.

II. POLICY

Section 4, Our Responsibilities to Grupo UNACEM and Its Shareholders, subsection (f), of our CODEC provides as follows:

"We use artificial intelligence to enhance our capabilities and support decision-making, always under human judgment and accountability. To harness its benefits, significant decisions are subject to human oversight to validate the quality, accuracy, and relevance of AI-generated outputs, as well as the appropriate management of associated risks. We use these technologies diligently, ethically, and responsibly, mitigating bias while promoting informed, inclusive, and rights-respecting decisions."

III. GUIDELINES

The following guidelines shall govern the use of AI:

1. Strategic Alignment and Legitimate Purpose

a) AI systems at Grupo UNACEM are intended to augment, complement, and enhance human cognitive and social capabilities. Accordingly, we maintain appropriate oversight of work processes performed using such systems.
b) We ensure that AI systems protect human dignity and the physical and mental integrity of individuals, preventing any harm to human beings.
c) We use AI responsibly and in alignment with our business strategy to improve the well-being of our stakeholders while respecting established governance structures.
d) We promote the development and use of AI systems and environments that are technically secure and robust and that are never intended for malicious purposes.
e) We encourage the use of providers whose data centers have a low environmental footprint.

2. Fairness, Inclusion, and Non-Discrimination

a) We promote the development and use of AI systems in a safe, responsible, ethical, transparent, and human rights–respecting manner, consistent with the guidelines established in our Corporate Human Rights Policy.

b) We foster the development and use of AI solutions that support fair, inclusive, and objective decision-making. To this end, we identify and mitigate risks of bias that may affect individuals and/or stakeholders, thereby promoting the responsible use of AI.

3. Transparency and Explainability

a) We promote the use of AI in a transparent and trustworthy manner by providing relevant internal and external users with timely information regarding its capabilities, intended purposes, and operation, thereby facilitating understanding and responsible adoption.

b) We promote AI-generated outputs and decisions that are understandable to their intended users.

c) We maintain clear records that facilitate traceability and trustworthy use of AI, to the extent technically feasible, including documentation of decisions and responsibilities throughout the AI lifecycle.

4. People and Accountability

a) Each AI solution shall have a clearly designated owner responsible for ensuring its appropriate use.

b) We use AI with sound judgment, validating its outputs within the scope of our respective roles and responsibilities. The use of AI solutions does not relieve employees of their responsibility for the decisions they make within the organization or under applicable regulatory frameworks.

c) Critical decisions shall always be subject to an appropriate level of human oversight.

5. AI Governance

The Corporate AI Function (see Annex 2) enables the responsible, secure, and scalable use of AI through accountability structures established at both the Corporate and Business Unit levels, together with corporate oversight and support processes designed to:

a) Enable and oversee the development of AI-based solutions to ensure alignment with business strategy and the availability of the necessary resources.

b) Promote the adoption of AI initiatives and facilitate their oversight based on the following three governance levels:

i. Basic

ii. Operational

iii. Ultra

c) Enable the trustworthy use of AI agents through meaningful human oversight and approval at key control points.

d) Establish KPIs and report on the achievements, benefits, and capabilities resulting from the implementation of AI solutions.

e) Promote the preparation of Business Cases, according to the applicable category (see subsection (b) and Annex 2), with input from business, technology, cybersecurity, compliance, legal, and risk management functions to facilitate the approval and responsible use of AI solutions.

f) Oversee the assessment of AI solution providers, taking into account security, privacy, compliance, and intellectual property considerations, as well as compliance with the Supplier Code of Conduct.

g) Ensure the responsible management of AI and its associated risks through the interdependent Three Lines of Defense Model, aligned with the standards of the Institute of Internal Auditors (IIA) and international best practices, whereby:

i. The First Line of Defense consists of those who use, develop, or support AI systems and are responsible for managing AI-related risks in accordance with corporate policies.

ii. The Second Line of Defense comprises two functions:

- The Corporate AI Function, responsible for establishing rules and overseeing, assessing, approving, providing training, monitoring, and reporting on the impacts of and matters related to the promotion, development, and deployment of AI (see Annex 2).
- The Corporate Risk and Compliance Department, responsible for establishing, monitoring, overseeing, and reporting on the implementation of the Corporate Enterprise Risk Management Policy.

iii. The Third Line of Defense consists of the Corporate Internal Audit Function, which is responsible for conducting independent assessments of AI governance, the internal control environment, compliance, and the effectiveness of policies governing the use of AI.

6. AI Use

We encourage employees to explore the use of AI and provide them with the necessary corporate support. Accordingly, AI systems may be used based on the associated level of risk, as follows:

a) Permitted Use: Uses that do not involve sensitive data or result in significant impacts on users or business decisions. Grupo UNACEM maintains a list of AI tools authorized for corporate use (see Annex 3).

b) Restricted Use: Uses involving personal data, critical processes, or automated decision-making, which require additional controls and prior approval from the Information Technology, Cybersecurity, and Data Privacy functions[1].

c) Prohibited Use: Any of the following:

i. The use of confidential, sensitive, or strategic information without proper authorization (see Sections **¡Error! No se encuentra el origen de la referencia.** and **¡Error! No se encuentra el origen de la referencia.**);

ii. The use of unauthorized AI platforms;

iii. The use of AI solutions that enable automated decision-making without human oversight;

iv. Any use that infringes fundamental rights or violates applicable regulations.

[1] The Data Privacy Officer shall involve other specialized functions, as appropriate.

7. Scalability and Cybersecurity

a) We integrate AI into corporate systems and applications to enable its scalable, resilient, and sustainable deployment, including during updates and maintenance;

b) We strengthen AI cybersecurity to enable the trustworthy use of AI, prevent vulnerabilities, protect information, and ensure operational continuity;

c) Accordingly, only AI tools and applications that meet both of the following requirements may be used:

i. They have been authorized by the Corporate Chief Information Officer (CIO) and the Corporate Chief Information Security Officer (CISO), or their duly authorized delegates (see Annex 3);

ii. They have been installed by the IT team;

8. Data Protection

a) We facilitate access to the data required for the responsible use of AI, in accordance with the criteria established by the Corporate Chief Data Protection Officer (CDPO) and based on the principles of need-to-know, least privilege, and applicable regulations.

b) We promote the responsible use of Grupo UNACEM's data in AI solutions through access controls, technically feasible traceability mechanisms, and periodic reviews to help prevent unauthorized access to or misuse of data.

9. Risk Management

a) We apply the risk appetite established in the Corporate Enterprise Risk Management Policy to the use of AI. The Corporate AI Function shall coordinate with the Corporate Risks and Compliance Department on consultations or reviews relating to this framework.

b) As applicable (see levels in Annex 2), our AI initiatives shall be supported by an appropriate Business Case that enable the assessment of associated risks and the definition of mitigation measures. High-risk initiatives shall also be supported by an AI Impact Assessment based on a double materiality approach, taking into account potential bias and ethical, social, and fundamental rights impacts prior to implementation;

c) The methodology for identifying, assessing, and managing risks shall be based on the Corporate Enterprise Risk Management Manual;

d) The AI risk taxonomy encompasses, in addition to risks relating to individuals' rights, bias, data, security, and compliance, traditional AI risks, AI-specific risks, risks amplified by generative AI, prompt injection risks, as well as risks associated with synthetic data and distortions;

e) Business Units shall establish AI Incident and Crisis Response Plans. These plans shall include escalation protocols, incident classification (e.g., cyberattacks or data breaches), root cause analysis, fault resolution procedures, as well as the development of crisis scenarios and simulation exercises;

f) The CIO, CISO, and CDPO shall periodically report on the management of technology, cybersecurity, and data protection within the scope of AI.

10. Training

We promote and encourage the responsible use of AI by providing practical, ongoing training to employees involved in the use of AI, enhancing their competencies in AI ethics, bias mitigation, data protection, cybersecurity, the responsible use of generative AI, and secure prompting, in accordance with the requirements established by the solution owner and Grupo UNACEM's Training Plan.

11. Audits and Monitoring

We conduct annual audits of high-risk AI systems and projects to strengthen their trustworthy use by assessing data management, bias management, the benefits identified in the applicable Business Case, and compliance with applicable regulations.

In addition, the owners of Operational and Ultra AI solutions shall assess enhancement opportunities every two years and annually, respectively, in order to improve their performance, reliability, and alignment with technological, regulatory, and operational developments.

IV. POLICY OWNER AND REVIEW

The Corporate Chief Executive Officer is the owner of this Policy, which forms part of the Enterprise Risks and Compliance System. The Risks and Compliance Committee oversees the implementation of this Policy through the monitoring, assessments, and reports submitted by the Corporate Director of Risks and Compliance.

The Corporate Risks and Compliance Department shall periodically review this Policy to ensure that it remains aligned with applicable AI-related legal and regulatory requirements, whenever there is a significant change in Grupo UNACEM's environment, or at least once every two years.

The Corporate AI Function and the General Managers of the Business Units shall take all necessary measures to ensure that the guidelines set forth in this Policy are effectively implemented and complied with.

All members of Grupo UNACEM are individually responsible for complying with the rules and guidelines established herein and for seeking guidance whenever they have any questions[2].

V. POLICY VIOLATIONS

Failure to comply with the guidelines set forth in this Policy shall be considered inappropriate conduct. Accordingly, Grupo UNACEM's Business Units and the Corporate Center reserve the right to take such employment-related disciplinary, civil, and/or criminal actions as may be appropriate in response to such non-compliance.

VI. REFERENCE DOCUMENTS

a) Code of Ethics and Conduct
b) Corporate Enterprise Risk Management Policy
c) Corporate Personal Data Processing Policy

[2] Employees should seek guidance from the CIO, CISO, CDPO, the appropriate Legal representative, the Compliance and Personal Data Protection Officer, the Corporate Legal Manager, the Corporate Compliance Manager, or the Corporate Director of Risks and Compliance.

d) Supplier Code of Conduct
e) Corporate Supply Chain Policy
f) Corporate Information Classification and Handling Policy
g) Corporate Information Security and Cybersecurity Risk Assessment and Management Policy
h) Corporate Information Security and Cybersecurity Organization Policy
i) Corporate Human Rights Policy
j) Corporate Enterprise Risk Management Manual
k) Business Unit Internal Work Regulations
l) AI legislation applicable to each Business Unit

VII. REVIEW HISTORY AND APPROVAL

	CORPORATE ARTIFICIAL INTELLIGENCE POLICY			VERSION
Department	CORPORATE RISKS AND COMPLIANCE DEPARTMENT			
Prepared by	**Fernando Dyer** Corporate Director of Risks and Compliance **Silvana Pérez Yalán** Corporate Compliance Manager and Corporate Chief Data Protection Officer	Preparation Date	05.29.2026	1.0
Reviewed by	**SALTO Project Team**	Review Date	06.10.2026	1.0
Reviewed by	**Luis Budge** Corporate Cybersecurity Manager and Corporate Chief Information Security Officer	Review Date	06.10.2026	1.0
Reviewed by	**Juan José Dorich** Corporate Enterprise Risk Management Manager	Review Date	06.10.2026	1.0
Reviewed by	**José Luis Perry** Corporate Legal Manager	Review Date	06.10.2026	1.0
Reviewed by	**Álvaro Morales** Corporate VP of Finance	Review Date	06.10.2026	1.0
Reviewed by	**Marlene Negreiros** Corporate VP of Talent and Culture	Review Date	06.10.2026	1.0
Reviewed by	**Eduardo Sánchez** Corporate VP of Industrial Operations	Review Date	06.12.2026	1.0
Reviewed by	**Pedro Lerner** Corporate Chief Executive Officer	Review Date	06.12.2026	1.0
Approved by	**Risks and Compliance Committee**	Approval Date	06.16.2026	1.0
Approved by	**Board of Directors**	Approval Date	07.01.2026	1.0

ANNEX 1 - DEFINITIONS

1. **Artificial Intelligence (AI):** The field focused on the research and development of mechanisms, systems, applications, and software capable of simulating human cognitive abilities;
2. **AI-based System:** A machine-based system that, either explicitly or implicitly, infers, from the inputs it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments;
3. **Personal Data:** Any information relating to an identified or identifiable natural person, whether directly or indirectly, through means that may reasonably be used for that purpose;
4. **Personal Data Processing:** Any technical operation or procedure, whether automated or otherwise, involving the collection, recording, organization, storage, retention, creation, modification, retrieval, consultation, use, blocking, deletion, transfer, dissemination, or any other processing that facilitates access to, correlation of, or interconnection of Personal Data;
5. **Personal Data Subject:** The natural person to whom the Personal Data pertains;
6. **AI Regulatory Framework:** The body of applicable laws, regulations, and mandatory requirements governing the use of AI;
7. **Corporate AI Function:** The governing body responsible for directing and overseeing Grupo UNACEM's AI-related activities. As of the issuance of this Corporate Policy, this role is performed by the executive team of the SALTO Project, known as the "SALTO Team," comprising Jaime Bedoya, Innovation Manager, and Elena Mujica, Corporate Transformation, Effectiveness, and Change Manager;
8. **Corporate Chief Information Security Officer (CISO):** The corporate executive responsible for Grupo UNACEM's information security strategy and for overseeing its implementation across the organization. As of the date of issuance of this Corporate Policy, the role is held by Luis Budge, Corporate Chief Information Security Officer;
9. **Corporate Chief Data Protection Officer (CDPO):** The corporate executive responsible for Grupo UNACEM's personal data protection strategy and for overseeing the processing of Personal Data in accordance with the functions established under applicable Personal Data Protection legislation. As of the date of issuance of this Corporate Policy, this role is held by Silvana Pérez, Corporate Compliance Manager and Corporate Chief Data Protection Officer;
10. **Corporate Chief Information Officer (CIO):** The corporate executive responsible for Grupo UNACEM's information technology strategy and for overseeing its implementation across the organization. As of the date of issuance of this Corporate Policy, this role is held by Mr. Javier Chang, Corporate Chief Information Officer.
11. **Hallucination:** The generation by an AI system of false, inaccurate, or fabricated information presented as factual, without any basis in its training data or in reality.
12. **Prompt Injection:** A technique that manipulates the inputs to a generative AI system in order to bypass its security controls or alter its intended behavior.

13. **Deepfake:** AI-generated or AI-manipulated audiovisual content (including images, video, or audio) that realistically simulates the appearance or voice of a real person.
14. **Model Drift:** The gradual degradation of an AI model's performance due to changes in data, the operating environment, or user behavior over time.
15. **Red-Teaming:** An adversarial testing methodology in which a specialized team deliberately attempts to induce failures, identify vulnerabilities, or elicit unintended behaviors in an AI system in order to identify risks before deployment.
16. **Guardrails:** Automated technical controls built into AI systems to constrain their outputs within predefined safety, ethical, and quality boundaries.
17. **AI Risk Appetite:** The level and types of AI-related risk Grupo UNACEM is willing to accept to achieve its strategic innovation and operational efficiency objectives.
18. **Synthetic Data:** Artificially generated data produced through algorithms that replicate the statistical characteristics of real-world data and are used to train or test AI models.

ANNEX 2 – RESPONSIBILITIES OF THE CORPORATE AI GOVERNANCE FUNCTION

1. Ensure that all AI initiatives, solutions, and projects—whether developed internally or acquired from third parties—comply with the principles and requirements set forth in this Policy.
2. Oversee the development of all AI solutions across Grupo UNACEM and monitor their entire lifecycle to ensure: (i) compliance with applicable laws and regulations, as well as with the requirements established by Grupo UNACEM's Corporate Functions for such purposes; (ii) adherence by such AI solutions to ethical principles and values; and, (iii) the technical and social robustness of AI solutions.
3. The Corporate AI Governance Function exercises oversight through following three governance levels:

a) Basic Level – Exploration and Unrestricted Use

This level includes internal prototypes, proofs of concept, personal or team productivity tools, and any use of AI that neither processes sensitive data nor generates decisions that affect third parties.

Applicable requirements:

i. The relevant AI Champion for the area or team shall be notified; however, prior approval is not required. The AI solution owner shall operate with full autonomy.

ii. Within thirty (30) calendar days of the initiative's commencement, the AI solution owner shall complete the Registration Form for the corporate AI initiatives repository.

iii. The SALTO Team may review notified initiatives at any time and, where justified, reclassify an initiative to a higher governance level if it identifies previously unconsidered risk factors.

b) Operational Level – Supervised Implementation

This level includes AI solutions that process customer, employee, or third-party data; support business decisions with tangible impacts on individuals; or are integrated into the organization's operational processes.

Applicable requirements:

i. The AI solution owner shall register the initiative in the corporate AI initiatives repository, using the Registration Form, prior to its development or acquisition.

ii. The technical and ethical review shall be conducted by the AI Champion for the relevant area before the initiative commences. The AI Champion is a role designated and certified by the Corporate AI Function. Direct involvement of the SALTO Team is not required unless expressly requested.

iii. The SALTO Team shall maintain read-only access to the repository and may request duly justified reviews at any time throughout the solution's lifecycle.

c) Ultra Level – Centralized Approval

This level includes AI solutions that: produce automated decisions with legal effects or significant impacts on fundamental rights; are embedded in external products or services; or involve any use of AI that poses a high reputational, regulatory, or societal risk to Grupo UNACEM.

Applicable requirements:

i. The development, acquisition, or implementation of any Ultra-Level initiative shall require the prior express approval of the SALTO Team.

ii. The SALTO Team shall actively monitor the solution throughout its entire lifecycle, including its development, implementation, operation, and eventual decommissioning.

iii. Impact assessments shall be conducted periodically, at least annually, or whenever a material change occurs to the solution or to the context in which it is used.

iv. Ultra-Level initiatives shall be subject to internal or external audits, as determined, and the results of such audit shall be reported to Grupo UNACEM's senior management.

v. Automated decisions generated by Ultra-Level that produce legal effects or have a significant impact on individuals shall not be based solely on the AI system. An effective mechanism for human oversight shall always be in place.

4. Monitor the registry of AI initiatives undertaken across Grupo UNACEM.
5. Advise the various business functions and Business Units on all legal and ethical matters relating to AI projects.
6. Evaluate AI systems throughout their development, implementation, and use to promote compliance with the following principles:

a) Privacy by Design and by Default: Respect for privacy through the application of Privacy by Design and Privacy by Default principles during the development, acquisition, implementation, and use of AI systems, in compliance with applicable laws and regulations.

b) Technical Robustness and Security: Ensure that the technical and security measures implemented for AI initiatives comply with the required security standards, thereby minimizing risks associated with AI use.

c) Transparency: Provide clear, accurate information to users whenever their data is processed by AI systems, enabling comprehensive understanding of and traceability for AI-related processes, decisions, and algorithms. In addition, promote AI awareness and digital literacy through appropriate education and training.

d) Human Oversight and Fundamental Rights: Ensure respect for fundamental rights during the development and use of AI.

e) Diversity, Non-Discrimination, and Fairness: Promote inclusion, diversity, and equal treatment throughout the AI system lifecycle.

f) Social and Environmental Well-Being: Promote the integration of social well-being, operational efficiency, and sustainable development principles.

g) Accountability: Implement appropriate controls and mechanisms to ensure accountability and responsibility in the development and use of AI.

h) Data Governance: Ensure compliance with the principles of data minimization, quality, and accuracy.

i) Copyright and Related Rights: Ensure respect for copyright, related rights, intellectual property laws, and applicable legal and regulatory requirements.

j) Automated Decision-Making and Profiling: Ensure that decisions with legal effects or significant impacts on users are not based solely on AI systems.

7. Communicate, in a clear and timely manner, information to the relevant business functions regarding the capabilities, intended purpose, and limitations of AI systems. Be transparent about the use of AI systems.
8. Promote the traceability and auditability of AI systems, particularly in critical contexts or situations.
9. Encourage the participation of the relevant business functions throughout the entire lifecycle of AI systems.
10. Promote education and training to ensure that all relevant business functions understand the principles of Responsible AI and receive appropriate training on the subject.
11. For Ultra-Level AI systems, the Corporate AI Function (or its duly authorized delegate) shall, prior to production deployment, oversee the execution of the following validation activities:

    a) Red Teaming: Conduct adversarial testing by an independent team to identify vulnerabilities, failure modes, and unintended behaviors in AI systems.

    b) Safety Testing: Conduct systematic assessments of potentially harmful behaviors, including the generation of harmful content, data leakage, and circumvention of security controls.

    c) Implementation of Technical Guardrails: Implement automated technical controls that constrain the outputs of AI systems within predefined safety, ethical, and quality boundaries.

    d) For all Operational-Level and Ultra-Level AI systems deployed in production, the following measures shall also apply:

    e) Continuous Model Drift Monitoring: Implement mechanisms to detect the gradual degradation of model performance resulting from changes in data, the operating environment, or user behavior.

    f) Boundary Definition: Formally define and document the operating parameters for each AI system, including permissible data types, acceptable confidence thresholds, and usage restrictions.

    The results of all validation activities shall be documented and included in the technical documentation for each AI system.

ANNEX 3 – LIST OF AUTHORIZED AI TOOLS AND APPLICATIONS

Only AI tools and applications installed by Grupo UNACEM's Information Technology (IT) team are authorized for use.

The following AI tools and applications may be requested for use. To obtain access, an installation request must be submitted via the IT Service Desk.

I. General-Purpose AI Tools:

The following general-purpose AI tools may be requested for use. To obtain access, an installation request must be submitted via the IT Service Desk:

1. (Microsoft) Copilot
2. (Anthropic) Claude

II. AI Capabilities Embedded in Corporate Systems

The following AI capabilities may be requested for use, provided that their implementation is supported by the Business Case for the relevant AI solution:

3. SAP Joule or other AI capabilities enabled in SAP S/4HANA
4. Salesforce Einstein or other AI capabilities available in Salesforce
5. Monday Sidekick or other AI capabilities available on Monday.com

III. Foundational Model Access Platforms

The following platform may be requested for use, provided that its implementation is supported by the Business Case for the relevant AI solution:

1. AWS Bedrock

Note: This list will be updated periodically to incorporate additional AI tools, capabilities, and/or platforms that may be requested for use.