1. PURPOSE AND SCOPE

This document establishes the governance model and structure for the protection of Grupo UNACEM's policy applies to Grupo UNACEM, which is comprised of UNACEM CORP S.A.A. (hereinafter, the "Company"), its Subsidiaries (hereinafter, "Business Unit"), and its directors, managers and other employees (hereinafter, "employees").

2. POLICY.

Grupo UNACEM applies a strategy through a comprehensive approach to cybersecurity and risk management, aligned with NIST, ISO 27001 and IEC 62443, protecting the assets that store and process critical information, as well as the critical information itself, applies the three lines of defense model and monitors regulatory compliance.

3. GUIDELINES

The following are the guidelines that the Business Units must implement, in accordance with the roles and responsibilities described in Chapter 4.

3.1. Regulatory Compliance

3.1.1. Adherence to International Standards

We adopted the "Cybersecurity Framework NIST" guidelines to improve the group's cybersecurity posture, identifying and prioritizing actions against the most significant threats.

3.1.2. National Legislation and International Agreements

a) We adhere to the laws of each country in which Grupo UNACEM has a presence, integrating their requirements into our safety processes and practices of the respective Business Units.

b) We respect the sectorial or bilateral agreements between countries that affect the handling and transfer of data in the jurisdictions that apply to us.

c) We develop technological protection capabilities in our Business Units that facilitate compliance with personal data protection laws in the jurisdictions that apply to us.

3.1.3. Establishment of the 3 lines of defense

Grupo UNACEM uses the 3 lines of defense model to assign the roles of responsibility for comprehensive risk management

a) First line of defense: Business Unit

They are responsible for risk identification and assessment (establishing the risks associated with their processes), as well as the implementation and effectiveness of internal controls to prevent, detect and mitigate risks, ensuring that activities are carried out in accordance with established policies and procedures.

b) Second line of defense: Risk and Compliance Management

It supervises and monitors risk-related matters in its role as second line of defense. This line is in charge of the Corporate Cybersecurity team of Grupo UNACEM, led by the corporate CISO and includes functions such as risk management, Cybersecurity strategy, as well as regulatory compliance. This level of defense does not execute operations but oversees and monitors the controls of the first line, helping to improve risk management and compliance with internal and external regulations. This line develops and updates policies, procedures, manuals and training to address existing, new and emerging risks.

c) Third line of defense: Corporate Internal Auditing

Performs assurance of the integrated risk management program in its role as the third line of defense. Internal Audit reviews in the first and second line of defense the strategy, design, implementation and effectiveness of the corporate information security and cybersecurity program, and issues recommendations for improvement.

3.1.4. Contractual Relationships

a) We include specific clauses in contracts with employees, suppliers, business partners and other third parties that require compliance with information security, cybersecurity and personal data processing policies.

b) Our information security and cybersecurity governance strategy encourage the evaluation of regulatory compliance in relationships with third parties that handle or access the group's internal or confidential information.

3.1.5. Information Backup and Recovery

We establish information backup and recovery plans in accordance with our needs and best international practices, to preserve business continuity in the event of incidents that may affect the availability and integrity of data.

3.1.6. Recording, documenting and reporting

We record, document and report information security and cybersecurity controls, complying with the transparency, integrity and traceability requirements demanded by best practices.

3.2. Asset and Risk Identification

a) We identify, document and classify information assets and associate cybersecurity risks, ensuring their updating and assigning responsible for their management.

b) We perform periodic risk assessments on information assets to detect threats and vulnerabilities and implement treatment strategies.

c) We communicate and train in risk management policies and strategies aligned with applicable regulations.

d) We implement mechanisms for the continuous identification of information assets, as well as the constant updating of their inventory.

3.3. Access Control and Identity Management

a) We manage and restrict access as needed, applying minimum privilege and reviewing permissions periodically.

b) We implement strong authentication (e.g. two-factor authentication) and secure credential management, with immediate revocation when necessary.

c) We use identity management systems to control the lifecycle of users and respond to security compromises.

d) We monitor authorized identities and accesses on an ongoing basis and perform periodic audits.

3.4. Information Security and Cybersecurity Risk Management

a) We adopt a reproducible information security and cybersecurity risk management methodology, aligned with best practices, based on probability and impact. We ensure its documentation and communication to identify, mitigate and manage cybersecurity risks that threaten the operational continuity and information of Grupo UNACEM.

b) We identify, analyze and prioritize information security and cybersecurity risks, determining critical thresholds to facilitate decisions and resource allocation.

c) We design and implement mitigation plans adapted to each risk, reducing its impact or probability to acceptable levels, considering efficiency and cost-benefit.

d) We develop reports, key performance indicators (KPIs) and risk indicators (KRIs) to measure and report the evolution of risk probability, the effectiveness of controls, and determine adjustments and improvements.

e) We maintain and report an updated record to senior management and the board of directors for effective management, oversight and monitoring, promoting feedback and continuous improvement.

3.5. Continuous Monitoring

a) We implement systems to monitor information assets and cybersecurity risks in cyberspace (infrastructure, networks, systems, internet), identifying threats and generating security alerts.

b) We analyze and respond to security alerts through procedures that allow us to prioritize them and differentiate possible real incidents from false positives, with defined action protocols.

c) We periodically update our monitoring system and policies to strengthen our response to new threats.

3.6. Incident Response and Business Continuity

a) We implement incident response plans, defining procedures for the detection, evaluation, containment and eradication of threats.

b) We set up CSIRT (Cyber Security Incident Response Team) teams in the Business Units, which are activated in the event of incidents and notify interested parties.

c) We establish recovery and business continuity plans, perform periodic tests and maintain backups updated as needed and protected to ensure the restoration of information.

d) In the event of incidents, we perform a root cause analysis, adjusting procedures, policies and response plans to improve resilience to new threats.

3.7. Security Technologies and Tools Management

a) We evaluate security technologies according to risk analysis, industry standards and validation by the Corporate CISO, prior to their acquisition.

b) We implement and configure technological tools following security guidelines, documenting their use to ensure continuity and consistency.

c) We establish a maintenance and constant updating program, applying security patches and periodically reviewing their effectiveness.

d) We monitor the performance and effectiveness of the tools, performing penetration tests to detect failures and optimize the cybersecurity infrastructure, as well as its risk mitigation capabilities.

3.8. Exception to policy compliance

Faced with events that require an exception to policy enforcement:

a) We identify, record, evaluate and timely report to the Local CISO, who will formally evaluate and approve the exception requested, prior to its execution, with a copy to the Corporate CISO.

b) We follow internal and external communication protocols to communicate relevant impacts to affected internal and external stakeholders.

c) We maintain preventive monitoring to detect and prevent them and include the implementation of new technologies and training practices.

d) We reinforce the Group's information security culture to communicate the importance of adhering to policies.

e) When exceptions are not approved in a timely manner and/or adequately supported, the respective disciplinary procedures will be applied.

4. RESPONSIBLE FOR THE POLICY AND ITS REVIEW

The Corporate Director of Risk and Compliance is responsible for this Policy and ensures its compliance.

The Corporate CISO, appointed by the person responsible for this Policy, is in charge of ensuring its implementation, leading the information security and cybersecurity strategy, supervising compliance with the established objectives and coordinating the definition and alignment of budgets and resources at corporate and local level.

The General Managers of the Business Units shall ensure compliance with this Policy, its guidelines and the information security and cybersecurity strategy. To this end, they must designate and supervise the Local CISO responsible for its implementation, as well as ensure the availability of the necessary resources to achieve the objectives established in their Business Unit.

The Corporate CISO shall review and update this Policy when any significant change occurs in Grupo UNACEM's environment or at least every two years, submitting any changes to the corresponding levels of approval.

Local CISOs are responsible for the direct operation of information security and cybersecurity, and shall adapt, implement, maintain operations and deploy technology solutions in accordance with this policy in their respective Business Units, and escalate any necessary exceptions to the Corporate CISO & CDO in a timely manner.

Everyone in Grupo UNACEM has an independent responsibility to comply with the rules and guidelines set forth herein, as well as to seek guidance when in doubt or need to analyze whether an activity may violate the rules described in this policy.

Disciplinary measures and sanctions will be applied to those who fail to comply with the provisions of this policy, as regulated in the Internal Regulations (e.g., Internal Work Regulations of each Business Unit).

5. REFERENCE DOCUMENTS

Code	Document
-	Code of Ethics and Conduct
-	ISO/IEC 27001
-	NIST Cybersecurity Framework version 2.0

Document Name	Corporate Policy on Information Security and Cybersecurity Organization			Version
Prepared by	Luis Budge Corporate Cybersecurity Manager	Date of Elaboration	05/15/2025	1.0
Prepared by	Guillermo Cortijo Corporate Information Security and Cybersecurity Supervisor	Date of Elaboration	05/15/2025	1.0
Reviewed by	Fernando Dyer Corporate Risk and Compliance Director	Revision Date	05/26/2025	1.0
Reviewed by	Pedro Lerner Corporate CEO	Revision Date	05/26/2025	1.0
Reviewed by	Risk and Compliance Committee	Revision Date	06/25/2025	1.0
Approved by	Board of Directors	Approval Date	06/25/2025	1.0

6. ANNEX - DEFINITIONS

- **Relevant information assets**: Information assets necessary for Grupo UNACEM to meet its objectives and whose valuation measured by the damage when the asset is damaged in terms of confidentiality, integrity and availability of information is high, very high and extreme.

- **Cybersecurity:** The set of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage or unauthorized access.

- **Confidentiality:** Refers to the property that ensures that information is not available or disclosed to unauthorized individuals, entities or processes.

- **Integrity:** It is the property that safeguards the accuracy and completeness of the information and processing methods.

- **Availability:** Is the property that ensures that information is accessible and usable upon request by an authorized entity when required.

- **Risk Management:** The process of identifying, evaluating and treating risks that threaten the achievement of Group UNACEM's business objectives.

- **Corporate CISO (Chief Information Security Officer):** The leadership figure in charge of the information security strategy and the supervision of its implementation at the corporate level.

- **Local CISO (Chief Information Security Officer):** Responsible for implementing and maintaining the corporately defined information security strategy in their respective business unit.

- **Security Incident:** An adverse event or threat with the capacity to negatively impact the information infrastructure or the information itself.

- **Risk**: An event, action or omission, from an internal or external source, that may occur and adversely affect the achievement of strategic or operational objectives.

- **Strategic risks**: These are events that could adversely impact the achievement of the strategic purpose or objective, whether due to impacts to initiatives, capabilities or other enablers. Project risks are included in this category.

- **Operational risks:** These are events that could adversely impact on the performance or efficiency of ongoing operations. This category includes, among others, production, logistics, cybersecurity, financial reporting, legal and compliance risks.