1. PURPOSE AND SCOPE

This document establishes Grupo UNACEM Information Security and Cybersecurity risk assessment and management policy in the face of cyber threats. It seeks to provide a structured approach to identify, analyze, assess and address risks. It applies to all information and IT assets of Grupo UNACEM operations, and which are part of the Information Security Management System (ISMS) and Cybersecurity Framework (CSF).

This policy applies to Grupo UNACEM, which is comprised of UNACEM CORP S.A.A.A. (hereinafter, the "Company"), its Subsidiaries (hereinafter, "Business Unit"), and its directors, managers and other employees (hereinafter, "employees").

2. POLICY

We apply an Information Security and Cybersecurity risk management methodology that includes the identification of risks through the periodic updating of the inventory of information and technology assets, the definition of the risk appetite, and the evaluation of existing controls. This evaluation process is continuous and documented, prioritizes risks for treatment and is supervised at the business unit, corporate and board level.

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. Identification of Information Security and Cybersecurity Risks

a) We identify and periodically update the inventories of Information Assets and technology to assess risks.

b) Information Assets are categorized according to their nature (facilities, services, applications, data, media, computer equipment, auxiliary equipment, networks, cryptographic keys, etc.).

c) Information Assets are classified according to the Information Classification and Treatment Policy, for their protection and risk management.

d) We analyze the threats and vulnerabilities of the Information Assets in coordination with the owners of the information, in order to obtain a comprehensive view of the risks that may compromise the Information Assets.

3.2. Risk Appetite

a) The risk appetite is approved by the Board of Directors and determines the maximum acceptable level of impact and probability of a risk, for decision making and resource allocation.

b) The Business Units quantify the potential impact based on EBITDA (if close to zero, another metric defined by the Risk and Compliance Committee is used).

c) The Board of Directors approves thresholds for key indicators, which define the minimum acceptable level, based on the maximum probability of the occurrence of the risk.

3.3. Identification of existing controls

a) We constantly evaluate whether current controls effectively mitigate risks, documenting their design, operation and maintenance.

b) We perform periodic audits, including penetration tests and incident simulations to measure their effectiveness.

c) We define KPIs and KRIs to monitor the performance of controls, ensuring their contribution to risk reduction.

d) We review and adjust controls following security incidents, identifying root causes, opportunities for improvement and strengthening existing controls.

3.4. Risk assessment

a) We perform a periodic risk assessment, where we analyze the Information Assets and detect new risks.

b) We analyze the risks identified and determine the level of prioritization based on their probability and impact.

c) We classify as critical the risks that exceed the risk appetite, establish the appropriate treatment, and report them to the Board of Directors for evaluation and supervision.

d) We estimate the probability of occurrence and impact using historical records or expert judgment and document it for reporting at the required levels.

3.5. Risk response

a) We assess and define actions to address all risks, in coordination with the Corporate CISO, Information Asset owners and management.

b) We apply risk response strategies, such as accepting, sharing, mitigating or avoiding risk, as appropriate.

c) When we establish controls and mitigation plans, we detail their objective, responsible party, evidence and follow-up to achieve their effectiveness and facilitate auditing.

d) We monitor the implementation of controls and mitigation plans, presenting progress to Corporate Risk and Compliance Management.

3.6. Risk reporting

a) We report and manage Information Security and Cybersecurity risks, to ensure decisions aligned with the Group's strategy and risk appetite.

b) We establish effective communication mechanisms to report risks and impacts to the appropriate levels of the organization.

c) We use risk reporting in strategic and operational decision making.

3.7. Monitoring and review

a) We continuously monitor the implementation and effectiveness of risk management controls and governance.

b) We periodically analyze changes in Information Assets, threats, vulnerabilities and treatment strategies, incorporating them into risk management.

c) We review the execution of risk response plans, ensuring that the actions implemented are effective and sustainable.

d) The Local CISO documents and presents the status of Information Security and Cybersecurity risk management to the Local CIO and the Information Security and Cybersecurity Operating Committee chaired by the Corporate CISO.

4. RESPONSIBLE FOR THE POLICY AND ITS REVIEW

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

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 shall 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 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.

5. REFERENCE DOCUMENTS

Code	Document
-	Code of Ethics and Conduct
-	ISO/IEC 27001
-	NIST Cybersecurity Framework version 2.0
UC-SI-POL003	Corporate Classification and Treatment of Information Policy
-	Corporate Integrated Risk Management Policy

Document Name	Corporate Policy on Evaluation and Management of Information Security and Cybersecurity Risks			Version
Prepared by	Luis Budge Corporate Cybersecurity Manager	Date of Preparation	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 Chief Executive Officer	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

- Information asset - Is everything that is or contains information to which the Company directly attributes a value and, therefore, requires protection.
- IT Asset - A component or resource, both physical and logical, used in the Information Technology (IT) environment that provides value to the Company.
- Threat - A potential cause of an unwanted incident, which may result in damage to assets such as information, processes and systems and consequent harm to the organization.
- Risk appetite - The level of risk that the Company is willing to assume in order to meet its objectives.
- Confidentiality - A characteristic of information that is available only to authorized persons or systems.
- Availability - A characteristic of information that can be accessed only by authorized persons when necessary.
- Impact - Economic, legal or operational consequences suffered by the Company when a risk materializes.
- Information - Any form of electronic, optical, magnetic or other similar media, capable of being processed, distributed and stored.
- Integrity - A characteristic of information that is modified only by authorized persons or systems and in a permitted manner.
- Probability - The possibility of an event materializing and causing an impact on the Company.
- Risk: An event, action or omission, from an internal or external source, that may occur and adversely affect the achievement of objectives.
- Vulnerability: The weakness of an asset (personnel, hardware, software, physical or logical information) or a control (policy, procedure, guideline, practice) that can be exploited by one or more threats.
- Corporate CISO (Chief Information Security Officer): The leadership figure in charge of information security strategy and overseeing 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.