1. PURPOSE AND SCOPE

This document establishes the guidelines, applicable 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, for the proper management of cybersecurity incidents in order to ensure incident management to protect information, operational continuity and compliance with regulations.

2. POLICY

At Grupo UNACEM we manage events and potential Information Security and Cybersecurity incidents in an effective, timely and structured manner, in order to minimize their impacts and promptly recover operational continuity and learn from each situation to strengthen our defense and prevention capabilities.

3. GUIDELINES

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

a) We develop a prevention approach through a plan with activities focused on detection and preparation for response through the Business Impact Analysis (BIA), Crisis Management Plan and Business Continuity Plan (BCP) that contemplates prioritized scenarios.

b) We detect, analyze and respond in a timely manner to Information Security and Cybersecurity incidents, in order to limit their adverse effect on Grupo UNACEM's operations and assets.

c) We manage, report and escalate Information Security and Cybersecurity incidents according to the classification of the affected information and its impact.

d) We establish preventive and response measures to maintain the integrity and availability of critical data and systems that may have been affected.

e) We develop timely and coordinated efforts with the crisis management, technology, operations and general management teams in the business units and at the corporate level, in accordance with the incident communications matrix.

f) We promote the restoration of operations in the event of disruptive incidents aligned with the objectives of the Business Continuity Plan (BCP).

g) We conduct periodic audits and evaluations to verify compliance and update escalation and reporting criteria, as appropriate.

h) We comply with applicable laws and regulations, as well as with contractual agreements signed with third parties.

i) Promote continuous improvement in incident response processes through root cause identification, lessons learned and corrective actions.

j) We conduct periodic exercises and simulations to improve our incident response capabilities.

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'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 the independent responsibility to comply with the rules and guidelines set forth herein, as well as to seek guidance in case of any doubt or need to analyze whether an activity may violate the rules described in this policy.

5. REFERENCE DOCUMENTS

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

Document Name	Corporate Information Security and Cybersecurity Incident Management Policy			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 Director of Risk and Compliance	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