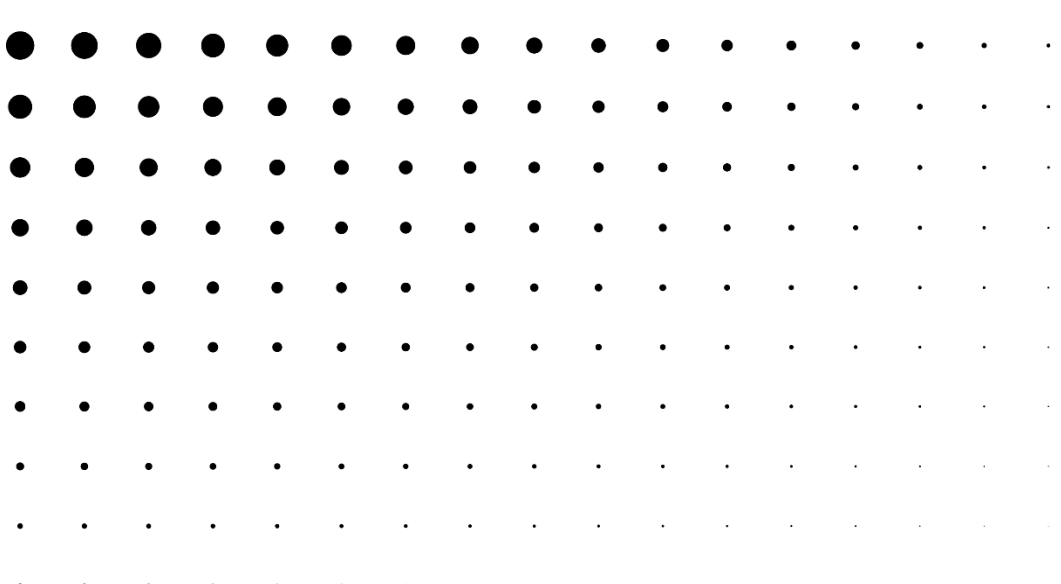
ANDINO
Global

INFORMATION SECURITY POLICY



INFORMATION SECURITY POLICY

Approved by the Board of Directors — 2025 Version

---

1. Purpose and Objective

This Information Security Policy aims to establish the principles, rules, and responsibilities that ensure the protection, confidentiality, integrity, availability, authenticity, and traceability (CIADT) of the information managed by Andino Inversiones Global S.A. and its group of companies. Its purpose is to ensure regulatory compliance, business continuity, and the trust of clients, shareholders, employees, and third parties.

---

2. Scope of Application

This Policy applies to all information, systems, processes, infrastructures, employees, executives, contractors, and third parties with access to data or technological resources of the Andino Group, including its subsidiaries in other countries. Compliance with this Policy is mandatory for all users handling corporate, personal, or confidential information.

---

3. Regulatory and Reference Framework

This Policy is aligned with, among others, the following regulations and standards:

- Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018 (LOPDGDD).
- Royal Decree 311/2022 regulating the National Security Framework (ENS).
- ISO/IEC 27001:2022 – Information Security Management Systems.
- ISO/IEC 27035:2023 – Information Security Incident Management.
- Spanish Criminal Code (Articles 197 and 31 bis) – cybercrime and corporate criminal liability.
- Recommendations issued by CCN-CERT, ENISA, and the Spanish Data Protection Authority (AEPD).
- Applicable legislation in Peru (Law No. 29733) and Mexico (Federal Law on the Protection of Personal Data Held by Private Parties – LFPDPPP).

4. Guiding Principles

The Andino Group manages information in accordance with the following principles:

- **Confidentiality:** information shall be accessible only to authorized individuals.
- **Integrity:** information shall be accurate, complete, and protected against unauthorized modification.
- **Availability:** information and systems shall be accessible when required.
- **Authenticity and traceability:** identities and access shall be verifiable and auditable.
- **Legality:** compliance with applicable laws and regulations.
- **Shared responsibility:** each user is responsible for the secure use of information.
- **Continuous improvement:** the system shall be periodically reviewed to incorporate technological and regulatory developments.

5. Information Classification

All Group information shall be classified according to its level of sensitivity and associated risk:

- **Confidential information:** personal, financial, strategic, or legal data.
- **Internal information:** internal-use documentation, procedures, and communications.
- **Public information:** information intended for external disclosure without access restrictions.

Each category shall determine the applicable protection measures, access controls, and storage requirements.

6. Roles and Responsibilities

- **Board of Directors:** approves this Policy and oversees its implementation.

- **Security and Compliance Committee:** coordinates the implementation of the Information Security Management System (ISMS).
- **Data Protection Officer (DPO):** oversees GDPR compliance and notifications to the AEPD.
- **IT Department:** implements technical security measures and access controls.
- **All employees and collaborators:** must comply with security rules and report incidents.

---

7. Security Controls

The Andino Group shall implement technical and organizational measures based on ISO/IEC 27001 and the ENS, including:

- Logical and physical access controls.
- Multi-factor authentication and strong password policies.
- Encryption of sensitive data and secure communications (SSL/TLS, VPN).
- Encrypted backups and periodic restoration testing.
- Policies governing the use of email, internet, mobile devices, and cloud storage.
- Logging and monitoring of access, audits, and operational traceability.

---

8. Information Security Incident Management

Any security incident (loss, unauthorized access, malware, data leakage, etc.) must be immediately reported to the Security Committee through the designated channel. The response procedure shall follow the phases of identification, containment, eradication, recovery, and notification.

Where an incident affects personal data, the Data Protection Officer (DPO) shall be informed and, where applicable, the Spanish Data Protection Authority (AEPD) shall be notified within a maximum period of 72 hours.

---

9. Training and Awareness

The Group shall develop mandatory annual training programs on information security, data protection, and cybersecurity. Periodic awareness campaigns

shall also be promoted to reinforce good practices and compliance with this Policy.

---

10. Oversight, Audit, and Continuous Improvement

The Security and Compliance Committee shall conduct periodic audits to assess the effectiveness of the system, implemented controls, and recorded incidents. Results shall be documented in an annual report, integrated into the Compliance Management System and the Non-Financial Information Statement (EINF). Lessons learned shall be used to update this Policy and strengthen the security framework.

---

11. International Application

Subsidiaries of the Andino Group outside the European Union shall adapt this Policy to their respective data protection and cybersecurity regulatory frameworks. Each subsidiary shall:

- Comply with national data protection laws (Law No. 29733 in Peru and LFPDPPP in Mexico).
- Implement local access controls, backup procedures, and incident management processes.
- Appoint an information security officer or equivalent role.
- Coordinate incident notifications with the Spanish parent company and ensure consistency with the Group ISMS.
- Participate in Group-wide audits and ESG reporting processes.

---

12. Approval and Entry into Force

This Information Security Policy has been approved by the Board of Directors of Andino Inversiones Global S.A. and enters into force on the date of its approval. It is mandatory for all Group entities and shall be disseminated through internal corporate channels.