Information Security Policy Framework

We maintain a set of information security policies that guide information security management and compliance, including an information security awareness and training policy.

1) General Information Security Policy

- Applies to the Institution's employees and external users, with specific exceptions.
- Requires an information security risk management process to manage risks at acceptable levels through the implementation of information security controls.
- Establishes measures to ensure that personnel and external users are aware of and comply with the policy, and provides for disciplinary or contractual measures in case of non-compliance, in accordance with internal regulations and applicable legislation.
- Defines logical access controls for external users, aligned with the contracted service and assigned by the internal owner.
- Establishes controls to avoid non-compliance with laws and regulations in the countries where we operate, as well as contractual obligations, in line with the scope of the policy.
- Establishes mechanisms and processes to effectively communicate information security-related events to stakeholders and to respond efficiently to such incidents, minimizing business impacts.
- Establishes that business or administrative processes, data subjects, users, and custodians who handle personal data must be clearly identified, and that processes, procedures, and controls must be defined to ensure its processing in accordance with applicable laws and in line with the Personal Data Protection Manual.

2) Information Security Policy for Employees

- Applies to employees and external users.
- States that employees and external users must comply with the information use and handling guidelines set out in the Information Classification and Handling Policy, the General Information Security Policy, and the PCI DSS compliance policy.
- Establishes reporting obligations in case of anomalous behavior:
  - Report through the Institution's established reporting system when anomalous behavior is detected in the work area, as provided for in the Code of Conduct.

- Report through the IT Service Desk (MSTI) when anomalous behavior is detected in performance or unusual application activity on computing equipment, due to the risk of vulnerability to malicious software (malware) or unauthorized configurations.

3) Policy linked to PCI DSS compliance / PCI SSF standard

- States that PCI SSF applies to software manufacturers and components that develop applications where debit and credit card data are stored, processed, or transmitted.
- Establishes the requirement to request the corresponding certificate from the referenced suppliers, in accordance with the technological risk management policy for suppliers, where internal responsibilities are defined.

4) Information Security Awareness Policy

- Defines an ongoing information security awareness and training process based on risk analysis, regulatory compliance, internal regulations, organizational aspects, campaigns, training, information security incidents, and directives and policies approved by the Information Security Officer, among others.

Glossary specifications

- “External user” is defined as a person or entity external to the Institution, which may include suppliers, clients, regulators, or external auditors, among others.
- “Anomalous behavior” is defined as actions or conduct that violate the standards or rules established in the Institution’s internal regulations.
- The “Institution’s established reporting system” is the tool that allows employees to submit anonymous reports regarding detected non-compliance in accordance with the Code of Conduct; it is currently Ethics Point.

Note: For security reasons, the full text of these policies is not publicly disclosed; however, we report their existence, scope, and general guidelines.