INFORMATION SECURITY AND CYBERSECURITY POLICY

MACROPROCESS

MANAGE INFORMATION RISK

Approvals	
Process Owner: Jairo Francisco González Matallana	Helber Alonso Melo Hernández
Position: Cybersecurity, Information Security, Privacy and Continuity Manager	Position: Risk Vice President

banco popular

TABLE OF CONTENTS

1. GENERAL OBJECTIVE

Establish the principles, guidelines, responsibilities, and expected conduct required to maintain a secure information environment, through guidelines focused on protecting the confidentiality, integrity, availability, and privacy of the Bank's information and IT resources, as well as mechanisms to anticipate and defend against attacks that may compromise the Bank's sustainability, thereby contributing to the strengthening of organizational resilience.
It also defines the governance structure, individual policies, and verification and control mechanisms that support their updating and continued validity over time.

2. ACTIONS AND TOOLS

The actions and tools to be implemented to achieve the general objective are as follows:

- Define guidelines for access to, use of, and management of the Bank's information and/or IT resources by Users (such as direct employees or temporary staff, administrators, shareholders, statutory auditors), Financial Consumers, Third Parties (suppliers and contractors), Control Entities, Related Entities, and the Bank's Subsidiaries.
- Define guidelines for managing Information Security and Cybersecurity risks, aligned with the Corporate risk management framework and in accordance with the risk appetite defined by the Bank.
- Establish the foundations for defining and developing of the Bank's Information Security and Cybersecurity Management System.
- Define the guidelines to ensure that the Bank's Senior Management remains informed of Information Security and Cybersecurity risks and the actions implemented by Information Owners to address them.
- Promote an Information Security and Cybersecurity culture among the Users mentioned above.
- Protect the Bank's image, interests, and good name.

3. SCOPE

This Information Security and Cybersecurity Policy defines the baseline framework that guides the implementation of any guideline, system, process, procedure, and/or action related to Information Security and Cybersecurity within the Bank.

This Policy applies to all levels of the organization: Users, Financial Consumers, Third Parties, Control Entities, Related Entities, and the Bank's Subsidiaries that access or use the Bank's information and/or IT resources.

In addition, this Policy applies to all information created, processed, stored, or used in support of the Bank, regardless of the medium, format, presentation, or location in which it is held.

The definitions contained in this document may be consulted in the annexed document DE-058-0 Definitions.

4. ORGANIZATION AND RESPONSIBILITIES

The main roles and responsibilities of the Information Security and Cybersecurity Organization are defined in Annex 1 – Description of Roles and Responsibilities, at the end of this document.

5. PRINCIPLES

To support the Bank's objectives, the following fundamental principles have been established as the basis for the Information Security and Cybersecurity Policy:

- **STRATEGIC PRINCIPLE:** Information is one of the Bank's critical assets for its operations and must therefore have an adequate level of protection.
- **GOVERNANCE PRINCIPLE:** Failure to comply with the responsibilities assigned in the Information Security and Cybersecurity Policy and Guidelines shall result in sanctions in accordance with the provisions of this Policy.
- **CONFIDENTIALITY PRINCIPLE:** The confidentiality of business information must be maintained in accordance with applicable laws, policies, and defined guidelines.
- **INTEGRITY PRINCIPLE:** This principle relates to the accuracy, completeness, and validity of information in accordance with the Bank's needs and expectations.
- **AVAILABILITY PRINCIPLE:** Information, as well as the associated resources and capabilities, must be available when required.
- **PRIVACY PRINCIPLE:** This principle refers to the need to preserve and protect personal data collected by the Bank, preventing access by unauthorized third parties.
- **NON-REPUDIATION PRINCIPLE:** Electronic business activities must ensure that logs and transaction traces are established, enabling the Bank to resolve disputes when one or more parties deny their participation.
- **COMPLIANCE PRINCIPLE:** Information Security and Cybersecurity policies, guidelines, and processes must comply with, and be aligned with, the applicable regulatory requirements for the Bank.

6. GENERAL INFORMATION SECURITY AND CYBERSECURITY POLICY

INFORMATION SECURITY AND CYBERSECURITY POLICY: Banco Popular recognizes that information, regardless of the medium in which it is held, is a critical asset and must be protected to ensure the proper development of its operations. Therefore, Senior Management declares its commitment to developing the skills and competencies, and allocating the technical and human resources, necessary to protect its information and that of its financial consumers, through the

implementation of mechanisms and protocols that strengthen its capabilities to protect against, withstand, and respond to internal threats and/or cyberthreats that may compromise the confidentiality, integrity, availability, and privacy of information; taking into account the Bank's size and level of risk exposure.

7. INDIVIDUAL POLICIES

7.1. ORGANIZATION OF INFORMATION SECURITY AND CYBERSECURITY

POLICY: Senior Management shall ensure the development and maintenance of the Bank's Information Security and Cybersecurity Management System, through the allocation of the necessary resources for its implementation and maintenance, within the entity's budgetary parameters.

The Bank shall have an Information Security and Cybersecurity Management System based on leading practices, compliant with national and international regulations, and aligned with the Bank's strategy, objectives, and goals. Likewise, it shall have adequate resources for its operation, including the structure responsible for defining, developing, and operating the System, assigning roles and responsibilities to each of the parties involved as defined in Annex 1, and establishing the budget for its proper operation.

An annual review and update process shall be conducted for the Information Security and Cybersecurity policies, guidelines, system, processes, and procedures, which may also be performed whenever circumstances require, in order to keep them up to date in response to threats and cyberthreats that may affect the Bank.

7.2. INFORMATION SECURITY AND CYBERSECURITY RISK MANAGEMENT

POLICY: Information Security and Cybersecurity risks to which the Bank's information and information assets are exposed must be identified, analysed, evaluated, and addressed in accordance with the value of the information, probability of occurrence, and impact.

The Bank's information and information assets shall be protected based on their criticality and the risks to which they may be exposed; therefore, the Bank shall have a model for Information Security and Cybersecurity risk management, aligned with the Corporate Risk Management framework, that enables the identification of internal threats and cyberthreats, the determination or updating of the relative value of information, the assessment of the level of risk to which information is exposed, and the definition of the actions required for its protection, in accordance with the provisions defined by the Board of Directors.

The Bank shall have a process for reviewing and updating Information Security and Cybersecurity risk management in order to adapt it to threats arising from the use, development, or creation of new technologies (Emerging Risks).

7.3. HUMAN RESOURCE SECURITY

POLICY: The Bank shall provide the necessary mechanisms to ensure that employees comply with their Information Security and Cybersecurity responsibilities from onboarding through separation.

The Bank shall verify the background of its employees and critical third parties prior to hiring, and contracts shall also include clauses specifying obligations related to the handling and protection of the Bank's information.

Additionally, depending on the role performed by the employee or critical third party, Information Security and Cybersecurity responsibilities, as well as compliance with the Bank's Code of Ethics and Conduct, shall be specified within their job duties.

7.4. INFORMATION ASSET MANAGEMENT

POLICY: Information, regardless of the medium in which it is found, is a vital asset for the Bank's operations and therefore must be classified and protected according to its importance and value, and properly managed to ensure its integrity, availability, confidentiality, and privacy.
The Bank shall define an information asset management methodology to identify, inventory, classify, assign, and value information, defining the Information Asset Owners who will ensure that it is properly protected in accordance with the guidelines established by the Bank.

Information assets shall be classified and handled according to their nature, location, and impact. Likewise, controls shall be implemented to address potential threats in accordance with their criticality and value for the Bank.

7.5. ACCESS MANAGEMENT

POLICY: The use of the Bank's information shall be controlled to prevent unauthorized access. Access privileges to information shall be maintained in accordance with business area needs and identified risks, limiting employee access to the information required to perform their duties.

Physical and logical access control mechanisms shall be established to ensure that information assets are protected in a manner consistent with their value to the Bank, and measures shall be implemented to address risks of loss of confidentiality, integrity, availability, and privacy of information.

The Bank shall have a user access lifecycle management methodology, ensuring that each employee or critical third party of the Bank has a unique user account, with restrictions and permissions previously defined by their immediate supervisor. Access to the Bank's resources shall be governed by the principles of need-to-know and least privilege.

7.6. CRYPTOGRAPHY

POLICY: The Bank shall use logical or physical systems to ensure the confidentiality and integrity of information through cryptographic controls such as cryptographic keys, digital signatures, certificates, and/or encryption algorithms.

For the storage and/or transmission of sensitive information, the use of cryptographic controls shall be established to secure the information, while evaluating and implementing the necessary technological mechanisms in each case.

7.7. PHYSICAL AND ENVIRONMENTAL SECURITY

POLICY: All physical business areas shall have a level of security consistent with the value of the information processed and managed within them. Sensitive information shall be kept in restricted-access locations when not in use.

The Bank's physical security shall be based on perimeters and secure areas, which shall be protected through appropriate perimeter controls.

The Bank's own technological infrastructure, or that managed by a third party, shall have physical and environmental security mechanisms to prevent exposure, damage, or loss, as well as security events that could interrupt its activities.

7.8. SECURITY AND CYBERSECURITY CULTURE

POLICY: The Bank shall develop training and awareness programs to provide sufficient guidance to its employees, users, and critical third parties to adopt a culture of Information Security and Cybersecurity.

The Bank shall have an ongoing training and awareness program to inform employees, users, and critical third parties of their responsibilities regarding Information Security and Cybersecurity, as well as the threats and cyberthreats that may affect the Bank. This program shall include testing exercises focused on different levels of the organization to measure the level of awareness achieved, generating indicators to assess the program's effectiveness.

Bank employees shall participate in the activities defined in the program, as well as in annual update sessions, and measures shall be implemented to inform financial consumers of Information Security and Cybersecurity recommendations for the protection of their information

7.9. THREAT AND CYBERTHREAT MANAGEMENT

POLICY: The Bank shall allocate the necessary resources to implement a threat and cyberthreat management program that may affect the confidentiality, integrity, availability, and privacy of the Bank's information.

The Bank shall establish a procedure for periodic review of internal threats and cyberthreats that may affect its information assets, and shall implement identification, anticipation, immediate remediation, and defense plans, prioritizing them according to their level of criticality for the Bank.

7.10. SYSTEMS AND INFRASTRUCTURE ADMINISTRATION PROCESSES

POLICY: The Bank shall manage and administer its systems and technological infrastructure under security standards and leading practices, implementing guidelines and procedures that enable proper control and assurance by the responsible parties.
The areas responsible for managing the Bank's information and technological resources shall implement processes and procedures for systems and infrastructure administration, taking into account: (i) Information Security and Cybersecurity guidelines that include monitoring activities and timely threat management, (ii) records of actions performed by users and/or administrators, (iii) change control over platforms, (iv) establishment and implementation of Information Security and Cybersecurity controls in projects, and (v) information backup and resource usage monitoring;

with the objective of ensuring the required performance of the systems and the platforms that support them.

7.11. TELECOMMUNICATIONS SECURITY

POLICY: The Bank's internal and external network connections shall be authenticated to prevent access to information by unauthorized personnel. Likewise, network connections shall have controls that enable their protection.

The use of communication media and channels shall be governed by the Information Security and Cybersecurity guidelines defined by the Bank and subject to periodic evaluation.

The information security architecture of the Bank's networks shall include the use of network controls based on monitoring, segmentation, encryption, blocking, and restriction of remote systems.

7.12. SOFTWARE ACQUISITION, DEVELOPMENT, AND MAINTENANCE

POLICY: Acquisitions, developments, maintenance, and changes to the Bank's information platforms or systems shall incorporate and implement Information Security and Cybersecurity requirements. Where the minimum required standards are not met, complementary controls shall be established to mitigate the identified risks.

The development of the Bank's technological projects and initiatives shall include, from the initial stages, an Information Security and Cybersecurity risk analysis. Such requirements shall be implemented and tested before transition into production. The security level of a system shall not be reduced as a result of modifications or updates performed.

The adoption of emerging technologies (e.g., cloud computing) shall comply with Information Security and Cybersecurity assessments, in which risks associated with the Bank's adoption of such technologies are identified, and minimum controls are defined to comply with Information Security and Cybersecurity guidelines and existing regulations.

7.13. THIRD-PARTY MANAGEMENT

POLICY: As part of its procurement process for goods and/or services from third parties, the Bank shall conduct an Information Security and Cybersecurity risk assessment of such third parties.

The Bank shall have a methodology for evaluating third-party risks and cyber risks, identifying critical third parties for Information Security and Cybersecurity and establishing action plans for risks that are outside the Bank's accepted risk level.

Bank employees responsible for third-party contracts shall regularly monitor compliance with Information Security and Cybersecurity controls by the third parties assigned to each of the Bank's units.

Communication channels and protocols shall be defined jointly with third parties, enabling the Bank to effectively and promptly understand and manage the status of the services received, as well as mechanisms to jointly respond to security incidents that compromise the Bank's information.

7.14. INCIDENT MANAGEMENT

POLICY: The Bank shall establish an Information Security and Cybersecurity incident management procedure in order to respond to threats and cyberthreats that may compromise the Bank's information.

The Bank shall have the necessary resources to support appropriate monitoring, detection, and management of Information Security and Cybersecurity incidents, establishing procedures for event monitoring, identification, response, notification, recovery, and resumption.

The Bank shall inform its stakeholders in a timely manner when an Information Security and Cybersecurity incident occurs that affects the confidentiality, integrity, availability, and/or privacy of the Bank's information or that of its financial consumers.

7.15. INFORMATION SECURITY ASPECTS IN BUSINESS CONTINUITY

POLICY: Continuity considerations for Information Security and Cybersecurity processes shall be included in business continuity management processes at all stages.

The Bank shall implement Information Security and Cybersecurity aspects within its business continuity management processes, ensuring that, in the event of contingency activation, protection levels are equal to or higher than those defined in normal operations.

The Bank shall include in its business continuity testing processes exercises that simulate the occurrence of cyberattacks in order to assess its response capability.

7.16. REGULATORY COMPLIANCE MANAGEMENT

POLICY: The Bank's Information Security and Cybersecurity policies, guidelines, processes, and procedures shall comply with local and international laws and regulations.

The Bank shall have procedures to review, identify, document, and comply with applicable legislation and legal requirements in Information Security and Cybersecurity. These requirements shall be included in the development of the Information Security and Cybersecurity Management System, taking specific actions to keep the Bank aligned with such provisions on an ongoing basis.

8. IMPLEMENTATION AND SCHEDULING OF POLICIES

The Information Security and Cybersecurity Policy involves the development and implementation of an Information Security and Cybersecurity program integrated into the Bank's operations. In order to achieve the objectives established in this document, these Policies provide for and authorize the development of guidelines, detailed procedures, and other administrative measures, as well as the development or acquisition of preventive and reactive mechanisms, software tools, and other protection techniques.

9. COMPLIANCE AND HANDLING OF POLICY VIOLATIONS

Compliance with the policies and their respective guidelines is mandatory for Users, Financial Consumers, Third Parties, Control Entities, Related Entities, and Subsidiaries of Banco Popular, whenever they access or use the Bank's information. Each stakeholder must understand their

role and assume their responsibilities regarding the management of information security and cybersecurity risks, while maintaining an adequate control environment for their processes.

Any breach of this Policy that compromises the confidentiality, integrity, availability, and/or privacy of information shall result in internal administrative actions as applicable, in accordance with the Collective Agreement and the Bank's Internal Work Regulations, without prejudice to any applicable legal actions.

10. POLICY ADMINISTRATION AND CHANGE PROCEDURE

To ensure the continued effectiveness of the Information Security and Cybersecurity Policy, it shall be subject to an annual review and to periodic reviews as required due to structural or technological changes affecting the Bank, or regulatory modifications, in accordance with established responsibilities.

Any stakeholder may identify the need to modify the Information Security and Cybersecurity Policy, and, in such case, shall follow the Bank's established update procedure.

11. POLICY EXCEPTIONS

There are no exceptions to these Policies.

12. ANNEX 1 – DESCRIPTION OF ROLES AND RESPONSIBILITIES

BOARD OF DIRECTORS

- Review and approve the Information Security and Cybersecurity Policy, as proposed by the Risk Vice Presidency.
- Review and approve the Bank's risk appetite, as proposed by the Risk Vice Presidency.
- Review the reports submitted by the Information Security and Cybersecurity Officer regarding the results of the evaluation of the effectiveness of the Information Security and Cybersecurity program, proposals for improvement in cybersecurity matters, and a summary of incidents that affected the Bank.
- Review and approve the resources required for the proper functioning of the Information Security and Cybersecurity Management System within the budgetary parameters approved by the Board each year and subject to the favorable opinion of the Bank's President.
- Participate in awareness and training programmes on Information Security and Cybersecurity topics.

SENIOR MANAGEMENT

- Ensure implementation of the strategies and policies approved by the Board of Directors regarding Information Security and Cybersecurity.
- Promote projects and/or initiatives aimed at strengthening the Bank's levels of Information Security and Cybersecurity.
- Assess and propose the financial and human resources required for the development and maintenance of the policies, guidelines, processes, and procedures of the Information Security and Cybersecurity Management System, within the Bank's size and level of risk exposure, and likewise within the corresponding budgetary framework.
- Participate in awareness and dissemination programmes on Information Security and Cybersecurity topics.
- Comply with the Bank's Information Security and Cybersecurity policies.

CORPORATE INFORMATION SECURITY AND CYBERSECURITY COMMITTEE

- Define corporate principles, guidelines, and directives (covering the Bank and its subsidiaries) on Information Security and Cybersecurity in alignment with the Group's business objectives.
- Establish the corporate position regarding Information Security and Cybersecurity risk management.
- Coordinate preventive and corrective actions for crisis management arising from events related to incidents affecting Information Security and Cybersecurity.
- Conduct research and remain continuously and professionally updated on new Information Security and Cybersecurity technologies.

INFORMATION SECURITY AND CYBERSECURITY COMMITTEE OF THE BANK

- Approve the Information Security and Cybersecurity strategy and model, in line with the Bank's objectives and based on corporate guidelines.
- Continuously assess the strategies, programmes, and the Information Security and Cybersecurity Management System.
- Promote the development and training of the Information Security and Cybersecurity Unit within the Bank.
- Review indicator results of the Information Security and Cybersecurity Management System and take corrective action when required.

AUDIT COMMITTEE

Review and recommend to the Board for approval the Information Security and Cybersecurity Policy.

RISK VICE PRESIDENT

- Submit the Information Security and Cybersecurity Policy to the Board for approval, subject to prior favorable opinion from the President.
- Ensure implementation of the strategies and policies approved by the Board of Directors regarding Information Security and Cybersecurity.
- Propose to the Board for approval the Bank's risk appetite, subject to prior favorable opinion from the President.
- Manage the resources allocated to the Information Security and Cybersecurity area to ensure the proper functioning of the Information Security and Cybersecurity Management System, in accordance with the authorisation granted by the Board of Directors.
- Support projects and/or initiatives aimed at enhancing the Bank's Information Security and Cybersecurity levels.
- Monitor, oversee, and report the results of Information Security and Cybersecurity risk management to Senior Management.

INFORMATION SECURITY AND CYBERSECURITY OFFICER

- Design, develop, implement, and update the Information Security and Cybersecurity Management System in line with the Bank's requirements and guidelines.
- Define guidelines and policies to protect information according to the value or criticality defined by the Information Owners.
- Advise Senior Management and the Board of Directors on matters considered necessary regarding Information Security and Cybersecurity, so that they can perform oversight and make appropriate decisions.
- Propose the organizational structure required for the development of the Information Security and Cybersecurity Model.
- Design and develop clear, objective, and verifiable management indicators that reflect the performance of the Information Security and Cybersecurity Management System.
- Design and develop the Bank's awareness program.
- Report Information Security and Cybersecurity incidents, their impacts, and the remediation actions taken to Control Entities and other stakeholders.

INFORMATION SECURITY AND CYBERSECURITY UNIT

- Develop, implement, update, and verify the proper functioning of the Information Security and Cybersecurity Management System in line with the Bank's requirements.
- Develop and maintain Information Security and Cybersecurity guidelines, procedures, and standards.
- Develop, implement, and control the Information Security and Cybersecurity incident management program.

- Participate in projects involving critical information assets defined by the Information Owner, ensuring that established Information Security and Cybersecurity guidelines are applied.
- Define the strategy for Information Security and Cybersecurity testing in applications or systems.
- Assess Information Security and Cybersecurity risks in applications, products, operating systems, tools, and networks, as requested by the Information Owner.
- Perform effectiveness testing of implemented controls and take the necessary measures to ensure compliance.
- Research new methods, products, and services for information protection that support the identification and development of initiatives to strengthen the Bank's security levels.
- Conduct security reviews of the Bank's critical third parties to assess compliance with security policies and guidelines.
- Review compliance by the Bank's different areas with Information Security and Cybersecurity guidelines and directives.
- Define and execute the awareness and training programme to be regularly delivered to the Bank's stakeholders on Information Security and Cybersecurity topics, and keep them informed of new cyberthreats.

INFORMATION OWNERS

- Identify, assess, address, and understand the risks to which their information could be exposed, and ensure that the necessary mechanisms are provided so that these risks are mitigated to acceptable levels, considering the cost-benefit relationship for their area.
- Classify information assets according to their criticality.
- Define the security requirements of their information assets in relation to confidentiality, integrity, availability, and privacy.

Additionally, they must define, among others:

- Who can use it?
- What users can do — read, write, modify?
- Under what circumstances can they do it?
- Conditions for use (written approval, specific area, etc.).
- Perform self-assessments of the proper execution of required controls over the information assets under their responsibility, with support from the corresponding areas.

TECHNOLOGY RESOURCE ADMINISTRATORS

- Apply and maintain security standards for the IT resources under their responsibility, in accordance with the Bank's Information Security and Cybersecurity guidelines and directives, and with authorization from the corresponding Information Owner.
- Support the implementation of security tools for the platform under their responsibility.
- Ensure that security controls for IT resources authorised by the Information Owner are maintained over time.

- Monitor, record, and report intrusion events or malicious use of IT resources under their responsibility and report them to the Information Owner and the Information Security and Cybersecurity Officer.

PHYSICAL SECURITY LEAD

- Design, develop, implement, maintain, and control a physical security program that includes the protection of areas that store critical information.
- Maintain direct and effective communication with the Information Security area, participating in investigations where physical assets are compromised.

TRAINING LEADER

- Support the Information Security and Cybersecurity Leader in the implementation and development of the Awareness Program.
- Generate indicators to measure, evaluate, and take action for the management of the Awareness Program.

HUMAN TALENT LEADER

- Support the Information Security and Cybersecurity Leader in the Information Security and Cybersecurity incident management program and risk assessment.
- Lead the internal administrative actions established within the Bank due to non-compliance with information security and cybersecurity policies, and/or legal actions that, in accordance with applicable regulations, may be necessary, with the support of Legal Counsel and other relevant Bank areas.
- Amend employment contracts and internal labour regulations to include information security and cybersecurity responsibilities.

LEGAL COUNSEL

- Advise on compliance with local and/or international legal regulations affecting the Bank in matters of Information Security and Cybersecurity.
- Provide support and advisory services to ensure that the Bank's Information Security and Cybersecurity Management System is within the corresponding legal framework and has the legal basis required to formalise and enable its application.
- Notify the Bank's Security Director when legislative changes or updates are identified that affect the validity or require adjustments to the Bank's Information Security and Cybersecurity Management System.
- Advise the Bank on the implementation or adoption of regulations in Information Security and/or Cybersecurity.

EMPLOYEES

- Apply the guidelines defined by the Information Security and Cybersecurity area to ensure the protection of the Bank's information.
- Identify possible Information Security and Cybersecurity risks and report them to the Information Owners and the Security area.
- Handle the Bank's information under their responsibility in accordance with the defined criticality levels.
- Use information assets exclusively to perform authorised duties within and/or outside the Bank.
- Preserve the security of the information used in the performance of their functions.
- Participate in awareness and training programmes on information security and cybersecurity topics.
- Any other responsibilities included in the job function manuals.
- Do not use your corporate email address to register for services or promotions with unknown third parties; doing so may expose you to phishing or other types of malware.
- All Bank employees, regardless of hierarchical level, and/or third parties are required and responsible for reporting and/or alerting the Bank to the possible occurrence of an Information Security and/or Cybersecurity incident. If you detect an information security incident, report it immediately through the email: segurinfo@bancopopular.com.co

DATA GOVERNANCE OFFICE LEADER OR (CDO)

- Understand and consider the principles, policies, and guidelines of information security and cybersecurity when establishing the mission, vision, and short-, medium-, and long-term goals of information governance.
- Support domain leaders in the implementation of controls and responsibilities defined by information security and cybersecurity, ensuring alignment with the policies.

INFORMATION SECURITY LEADER

- Implement mechanisms and controls to safeguard and protect information and technological resources in accordance with the value assigned by the Information Owners and following the guidelines issued by information security and cybersecurity.
- Administer and operate the Bank's security tools.
- Manage the security level of applications based on the authorisation granted by the Information Owner.
- Monitor, record, resolve, and report intrusion events or malicious use of technological resources, reporting them to the Information Owner and the Bank's Information Security Director.
- Apply and maintain the security standards of the platforms under their custody.

THIRD PARTIES RELATED TO THE BANK

- Implement the guidelines and directives defined by the Information Security and Cybersecurity Unit in the provision of services to the Bank.
- Establish a control environment for information security and cybersecurity risks that may affect the Bank's information assets.
- Establish communication and coordination mechanisms with the Bank in the event of information security and cybersecurity incidents.
- Participate in the Bank's awareness and communication programs on information security and cybersecurity topics.

13. CHANGE LOG

VERSION HISTORY		
Version #	**Publication Date**	**Description of Change**
1	15/01/2021	The document was created to replace policy PO-058-0 Information Security and Cybersecurity Policy.
2	21/09/2021	The Information Security and Cybersecurity Policy document was updated due to the renaming of the Corporate Risk Officer (CRO) Office to the Comprehensive Risk Management Office.
3	17/01/2023	The Information Security and Cybersecurity Policy document was updated with the following adjustments: • In one of the responsibilities of technology resource administrators, "Information Security Director" was changed to "Information Security and Cybersecurity Officer". • In the responsibilities of EMPLOYEES, a specific item was added related to the reporting of events or incidents through the channels established within the Bank.
4	26/02/2024	The Information Security and Cybersecurity Policy was updated as follows: • In section 12. ANNEX 1 – DESCRIPTION OF ROLES AND RESPONSIBILITIES, the role of the AUDIT COMMITTEE was included to comply with circular 008 (as approved in Board Minutes No. 2772, page 11).

VERSION HISTORY		
Version #	**Publication Date**	**Description of Change**
		• The title of Comprehensive Risk Manager was adjusted to Risk Vice President, in accordance with the latest approved organizational chart.