Procedures Manual

INFORMATION SECURITY MANUAL

MAN-APY-177

Date: 20/05/2025

Version: 2.5

Uso interno

Uso interno

Banco de Occidente

TABLE OF CONTENTS

1. OBJECTIVE AND SCOPE 3
1.1 OBJECTIVE OF THE INFORMATION SECURITY AND CYBERSECURITY POLICY 3
1.1.1 Principles 3
1.1.2 General Objective 3
1.1.3 Specific Objectives 3
1.2 OBJECTIVES OF THE INFORMATION SECURITY STANDARDS 4
1.2.1 Scope 4
1.2.2 Compliance 5
2. GENERAL 6
2.1 POLICIES 6
2.1.1 Organization of the Policies 6
2.1.2 Scope of the Policies 6
2.1.3 Organization and Responsibilities 6
2.1.4 Audit 7
2.1.5 Compliance and Management of Policy Violations 7
2.1.6 Administration of Change Policy and Procedure 8
2.1.7 Exceptions to the Policy 8
2.1.8 Policy Implementation and Program 8
2.1.9 Cybersecurity Risk Management Framework 8
2.1.10 Individual Policies 8
2.1.11 Glossary for the Security Model Policies 15
3. OPERATING PROCEDURE 16
3.1 USER IDENTIFICATION AND AUTHENTICATION 16
3.2 ACCESS CONTROL 16
3.3 AVAILABILITY 16
3.4 CONFIDENTIALITY 16
3.5 INTEGRITY OF INFORMATION 16
3.6 DISASTER RECOVERY 16
3.7 PHYSICAL SECURITY 17
3.8 CERTIFICATION OF INFORMATION 17
3.9 ALERT MANAGEMENT 17
3.10 AUDITABILITY MANAGEMENT 17
3.11 SECURITY MANAGEMENT 17
3.12 POLICY MANAGEMENT 17
3.13 RISK ASSESSMENT 17
3.14 SAFETY AWARENESS 18
3.15 STRUCTURE AND ORGANIZATION 18

1. OBJECTIVE AND SCOPE

1.1 OBJECTIVE OF THE INFORMATION SECURITY AND CYBERSECURITY POLICY

This Information Security and Cybersecurity Policy is a statement of the responsibilities and accepted conduct to maintain a secure environment at Banco de Occidente. This Policy establishes the guidelines and directives related to the secure handling of information.

1.1.1 Principles

In order to fulfill its business objectives, Banco de Occidente has established the following principles as fundamental, supporting the Information Security and Cybersecurity Policy:

- Information is one of Banco de Occidente's most important assets and therefore it is expected to be used in accordance with business requirements.
- The confidentiality of business information and that of third parties must be maintained, regardless of the medium or format in which it is held.
- Business information must preserve its integrity regardless of its temporary or permanent residence, or the way in which it is transmitted.
- Business information must be available when required.
- The privacy of Banco de Occidente's information must be preserved.

1.1.2 General Objective

The main objective of the Information Security and Cybersecurity Policy is for Banco de Occidente to ensure that its information is accessed only by those who have a legitimate need for the performance of their business functions (Confidentiality); that it is protected against unplanned modifications, made with or without intent (Integrity); that it is available when required (Availability); and that it is used for the purposes for which it was obtained (Privacy).

1.1.3 Specific Objectives

The specific objectives pursued by the Information Security and Cybersecurity Policy are:

- Establish the foundations for the development and implementation of the Information Security Model.
- Define the conduct to be followed regarding access, use, handling, and management of information resources.
- Establish and communicate responsibility in the use of information assets that support business processes and systems.
- Manage risks in Information Security and Cybersecurity.

- Establish communication channels that allow Senior Management to remain informed about risks and improper use of information assets, and the actions taken for their mitigation and correction, generating culture and commitment at all levels.
- Raise awareness among the Community about cybersecurity risks and ensure they have the necessary knowledge, skills, and technological means to maintain Information Security objectives.

- Protect the image, interests, and good name of Banco de Occidente.

This document provides the standards to support the Information Security and Cybersecurity Policies of Banco de Occidente.

This Policy is part of Banco de Occidente's Security Model under the responsibility of the Information Security Leader, is reviewed and approved by the Board of Directors and the Information Security Committee of Banco de Occidente, and is communicated to Information Owners, the Community, and the different Information Security roles.

Changes that arise due to technological dynamics or for other reasons during the implementation of these standards, and that impact the Information Security and Cybersecurity Policies, will be documented and may lead to modifications of the Policy.

The Board of Directors of Banco de Occidente has at least one member with experience in information assurance, which is aligned with the strategic oversight of Information Security and Cybersecurity.

Banco de Occidente is committed to the continuous improvement of its Information Security and Cybersecurity framework through the ongoing enhancement of its ISMS, including the periodic review, updating, and strengthening of controls, capabilities, and incident response processes, in line with the evolving of risks, technological developments, and stakeholder expectations.

1.2 OBJECTIVES OF THE INFORMATION SECURITY STANDARDS

The Information Security standards of Banco de Occidente aim to develop the Information Security and Cybersecurity Policy by formally documenting the rules for the protection of the Institution's information that are processed, transported, or stored through IT means such as software, hardware, networks, and other associated facilities.

Through the application of the standards set out in this document, Banco de Occidente defines how information is protected in a homogeneous manner and consistently with its criticality for the business, across all IT resources.

1.2.1 Scope

The Information Security Standards respond to and develop the guidelines established by the Information Security and Cybersecurity Policy and are required to implement a reliable and flexible Information Security Model. This is supported by internal Information Security and Cybersecurity procedures, whose objective is to document the main operational actions to be executed in order to safeguard the confidentiality, integrity, and availability of information, maintaining the security levels accepted by Banco de Occidente.

These standards are part of the Information Security Model and apply to all levels of the organization: Users (including employees and shareholders), Clients, Third Parties (including suppliers and contractors), Oversight Bodies, Related Entities, and Subsidiaries of Banco de Occidente, who access, either internally or externally, any information asset that is stored, processed, or transported using hardware, software, networks, and other associated facilities.

1.2.2 Compliance.

The standards must be complied with by all those who have access to or use Banco de Occidente's information through software, hardware, networks, and associated facilities.
Compliance with the standards is mandatory, and any exception must be documented as a risk incurred by Banco de Occidente, which must be formally accepted by the Information Owner. The Community must understand the implications of the standards and the responsibilities for their strict compliance.

Failure to comply with the standards may result in disciplinary or financial actions in the case of suppliers or contractors, which may even lead to the termination of the contractual relationship and/or legal actions. Ignorance of the standards does not exempt their application.

For new developments or new acquisitions of IT resources, the standards apply from their effective date. A detailed plan must be established to adjust IT resources acquired prior to this effectiveness in order to ensure compliance with the standards.

2. GENERAL

2.1 POLICIES

2.1.1 Organization of the Policies

The document is fundamentally organized into two parts: the first describes the general objective of the Information Security and Cybersecurity Policy, its characteristics, the responsible parties, and the way in which it must be developed, implemented, and maintained. In the second part, individual policies directly related to the general one are developed, specifying the conduct accepted by Banco de Occidente in the handling of its information and the actions that must be taken to achieve the objectives of this Policy.

2.1.2 Scope of the Policies

The Information Security and Cybersecurity Policy provides the guidelines required to implement a reliable and flexible Information Security Model and defines the basic framework that will guide the implementation of any standard, process, procedure, and/or action related to Information Security at Banco de Occidente.

This Information Security and Cybersecurity Policy applies to all levels of the organization: Users (including employees and shareholders), Clients, Third Parties (including suppliers and contractors), Oversight Bodies, Related Entities, and Subsidiaries of Banco de Occidente that access, either internally or externally, any information asset regardless of its location. Additionally, this Policy applies to all information created, processed, or used in support of the business, and to employees' personal information, regardless of the medium, format, presentation, or location in which it is found.

2.1.3 Organization and Responsibilities

The administration of this Policy will be the responsibility of the Information Security Organization as follows:

2.1.3.1 Information Security Committee

It is the executive group responsible for ensuring the planning, implementation, and maintenance of the Information Security and Cybersecurity Policy, as well as the execution and timely reporting to Senior Management of the actions required to maintain the established security levels.

2.1.3.2 Information Security Leader

This role is part of the second line of defense and must establish the guidelines in this area and continuously monitor compliance with all Information Security and Cybersecurity Risk obligations.

The Information Security Leader is also responsible for presenting management results directly to Senior Management or the Audit Committee. This role must have sufficient resources to effectively perform all functions and play a central and proactive role in the Information Security Management System. To do so, they must be fully familiar with current policies and standards, their legal and

regulatory requirements, and the Information Security risks derived from the business, including specific Cybersecurity issues.

2.1.3.3 Cybersecurity Leader

This is the executive responsible for ensuring the secure operation of the Organization's technological platform and meeting security and trust expectations for clients. Likewise, they support value creation through business-enabling Cybersecurity strategies and proactively defend the Organization against cyber threats, preventing the occurrence and recurrence of cybersecurity incidents.

2.1.3.4 Information Owner

This is the executive for whom the information was created in order to carry out their business and is responsible for managing and classifying it according to its value and criticality. They must also implement the Information Security and Cybersecurity Policy within their area, and to do so, they must know the value of their information, the users who should have access to it, and the privileges in its use.

2.1.3.5 Community

They are responsible for protecting Banco de Occidente's information assets by complying with the Information Security and Cybersecurity Policy. Likewise, they must remain alert to identify and report any non-compliance or breach of established standards or procedures.

Banco de Occidente will define the roles and responsibilities required to complete the definition of the Information Security organization, always promoting the segregation of duties as a method to reduce risks in the misuse of information.

2.1.4 Audit

The disclosure of information related to internal audit processes in the Management Report, as part of the third line of defense, plays a fundamental role by enabling the independent and periodic evaluation of the management and controls of information security and cybersecurity risks, as well as the policies, standards, and system procedures. This process is carried out through the disclosure and explicit formalization of periodic internal audits of the IT infrastructure and the information security management system, which are executed in accordance with the annual audit plan or based on the behavior of IT and information security risks.

2.1.5 Compliance and Management of Policy Violations

Compliance with the Information Security and Cybersecurity Policy and its respective standards is mandatory; each member of the Community must understand their role and assume responsibility regarding Information Security risks and the protection of Banco de Occidente's information assets. Any breach of this Policy that compromises the Confidentiality, Integrity, Availability and/or Privacy of information will result in disciplinary action, which may include termination of the employment contract and a possible initiation of legal proceedings under applicable national or international laws.

The Information Security and Cybersecurity Policy is based on best security practices and is aligned with national and international legislation; therefore, it will take the necessary steps, including applicable legal measures, to protect its assets and their use.

2.1.6 Administration of Change Policy and Procedure

The Information Security and Cybersecurity Policy is expected to be maintained over time. However, it must be reviewed annually or when structural changes affecting Banco de Occidente occur, to ensure it meets evolving business needs. The Information Security Leader is responsible for this task and must carry it out considering Corporate and Bank guidelines.

Any member of the Community may identify the need to modify the Information Security and Cybersecurity Policy; such concerns and suggestions must be communicated to the Information Security and Cybersecurity Leader, who is responsible for its maintenance.

If an addition or change to the Policy is required, the Information Security and Cybersecurity Leaders will carry it out and submit it for approval to the Board of Directors and the Bank's Information Security Committee. The formalization of the new Information Security and Cybersecurity Policy will be carried out by the Information Security Leader.

2.1.7 Exceptions to the Policy

There are no exceptions to this Policy.

2.1.8 Policy Implementation and Program

The Information Security and Cybersecurity Policy involves the development and implementation of a broad Information Security program integrated into the day-to-day operations of Banco de Occidente. An effective Information Security program is a continuous process, not an event. To achieve the objectives set forth in this document, this Policy anticipates and authorizes the development of standards, detailed operational procedures, and other administrative measures; as well as the development or acquisition of preventive and reactive mechanisms, software tools, and other protection techniques.

2.1.9 Cybersecurity Risk Management Framework

The Cybersecurity risk management framework establishes a system to identify, analyze, assess, mitigate (treat), monitor, and communicate associated cyber risks in a way that enables Banco de Occidente to mitigate the likelihood of occurrence, the materialization of risk, and its impact. The Cybersecurity risk management system is an integral part of the corporate SARO methodology.

2.1.10 Individual Policies

2.1.10.1 Information Security

Policy: Business information is a vital asset of Banco de Occidente and must therefore be protected.

Banco de Occidente's information, regardless of its representation, medium, or format, in which it is created or used to support business activities, is classified as business information or an information asset.

Banco de Occidente must have the necessary means to ensure that each member of the Community preserves and protects information assets in a consistent and reliable manner. Any person attempting to disable, bypass, or override any security control will be subject to immediate disciplinary action.

Business Information Security is the set of protection measures taken by Banco de Occidente against accidental or malicious disclosure, modification, theft, or destruction of its information. These protection measures are based on the relative value of the information and the risk to which it may be exposed.

Information Owners are responsible for ensuring that business information has appropriate protection to preserve the Confidentiality, Integrity, Availability, and Privacy of information.

2.1.10.2 Cybersecurity

Policy: Cybersecurity is oriented toward the development of capabilities and practices to defend against and anticipate cyber threats.

Banco de Occidente must have the necessary means to ensure information supported by IT systems by developing business capabilities and practices to defend against and anticipate cyber threats, in order to protect and secure data, systems, services, and applications that are essential to the business across internal corporate networks and in cyberspace.

2.1.10.3 Intellectual Property

Policy: Ownership of information must be maintained.

Intellectual Property is defined as any patent, copyright, invention, or information that is the property of Banco de Occidente.

All material developed while working for the Bank is considered its intellectual property and is for its exclusive use; therefore, it must be protected against disclosure, discovery, or use that undermines the Bank's competitiveness.

2.1.10.4 Information Owners

Policy: Each information asset of Banco de Occidente must have an owner who is responsible for its security.

Banco de Occidente uses information to carry out its activities. This information is created and assigned to each executive so they can develop and fulfill their respective goals within the framework of the business.

The information that the Bank uses to achieve its business objectives must have an assigned owner, who uses it within their area and is responsible for its proper use. Therefore, they are in charge of making the decisions required to protect their information and determining who the users are and their usage privileges.

2.1.10.5 Compliance with Regulations

Policy: Banco de Occidente must comply with local and international Privacy and Information Security regulations.

The Information Security and Cybersecurity Policy is aligned with and supports compliance with local and international laws and regulations related to Information Security. Therefore, such requirements must be included in the development of the Security Model, and specific actions must be taken to keep the Bank permanently aligned with such provisions. Examples of such provisions include banking secrecy, software licensing, circulars issued by the Banking Superintendency, and those from international groups such as the Basel Committee on Banking Supervision.

Likewise, and to maintain a good level of security, this Policy must be supported by Information Security best practices such as ISO 27001:2015 and ISO 27032:2013 / NIST 800-53.

2.1.10.6 Information Security and Cybersecurity Risk Management

Policy: The risks to which Banco de Occidente's information is exposed must be identified, assessed, and mitigated according to their value, likelihood of occurrence, and impact on the business.

Business information must be protected based on its value and the risk to which it may be exposed. Therefore, a high-level analysis of business impact in Information Security must be conducted periodically to determine or update the relative value of the information, the level of risk to which it is exposed, and the respective Information Owner.

Once the level of risk and the value of the information are established, each Information Owner must carry out a formal risk assessment so that risks are identified, evaluated, and necessary actions are implemented to address or mitigate them according to the risk levels permitted by the Bank.

Each user of the information must be aware of procedures for reporting risks that could impact the Bank's Information Security and is required to immediately report any suspicion or observation of an incident to Information Security.

2.1.10.7 Training and Culture Building in Information Security and Cybersecurity

Policy: Banco de Occidente must establish an ongoing program to build a culture of Information Security and Cybersecurity for users and third parties.

Banco de Occidente must have a permanent program to ensure that users and third parties are informed about their responsibilities in Information Security and the ongoing threats that put the information they handle at risk.

Users and third parties must be aware of the Information Security procedures they must apply in addition to those required to perform their job functions. As part of the training program, new personnel must attend, during the induction period, a session on the Bank's Information Security and Cybersecurity requirements..

2.1.10.8 Personnel Security

Policy: Banco de Occidente must provide the necessary mechanisms to ensure that its employees fulfill their Information Security responsibilities from hiring to termination.

New employees joining Banco de Occidente or those changing positions must undergo an investigation process to mitigate risks in the use of business information. The degree of investigation will depend on the level of contact they will have with the information.

Employee contracts must include clauses specifying the care that must be taken with the Bank's information. Additionally, depending on the role performed by the employee, their responsibilities regarding Information Security and compliance with the code of conduct must be clearly defined, making them aware of the consequences in case of non-compliance. A record of each employee's understanding and adherence to the Information Security and Cybersecurity Policy must be maintained.

The Bank will develop a program for handling suggestions in Information Security and Cybersecurity, through which employees will report vulnerabilities and risks they detect. Likewise, personal work objectives must include goals related to compliance with this Policy.

2.1.10.9 Third Parties Accessing Banco de Occidente Information Locally or Remotely

Policy: Third Parties that use Banco de Occidente's information locally or remotely must comply with the Information Security and Cybersecurity Policy.

The use of Banco de Occidente's information by Third Parties, Related Entities, and Subsidiaries, whether locally or remotely, must be formalized through agreements that make compliance with this Policy mandatory. Such personnel must be investigated according to their level of contact with the information. Service contracts must include a formal Information Security Service Level Agreement detailing their commitments regarding the care of the Bank's information and the penalties they would face in case of non-compliance. Compliance with these Information Security Service Levels must be verified periodically.

Each relationship with a Third Party, Related Entity, or Subsidiary must have a high-level representative within the Bank who ensures the proper use and protection of business information. This person will be responsible for the activities of such personnel during the term of the contract.

2.1.10.10 Individual Identification and Authentication

Policy: All members of the Community accessing Banco de Occidente's information must have a means of identification, and access must be controlled through personal authentication.

Each member of the Community is responsible for their actions while using any information resource of Banco de Occidente. Therefore, the identity of each member accessing IT resources must be uniquely established and authenticated and must not be shared.

Members of the Bank's Community will be required to authenticate themselves before gaining access to information. Depending on the value of the information and the level of risk, the Bank will define appropriate authentication methods, which must not be shared (such as passwords) and must only be enabled during the Bank's established working hours. These authentication means contain confidential information that must not be disclosed or stored in places accessible to unauthorized persons.

2.1.10.11 Control and Administration of Access to Information

Policy: The use of Banco de Occidente's information must be controlled to prevent unauthorized access. Privileges over information must be maintained in accordance with business needs, limiting access only to what is required.

Mechanisms for physical and logical access control must be established to ensure that information assets are protected consistently with their value to the business and the risks of loss of Confidentiality, Integrity, Availability, and Privacy.

Access rights must not compromise the segregation of duties and responsibilities. Access to the Bank's information must be granted only to authorized users, based on what is required to perform their responsibilities. Access must be restricted in all cases, following the principles of need-to-know and least privilege.

2.1.10.12 Information Classification

Policy: Information Owners must classify information based on its value, sensitivity, risk of loss or compromise, and/or legal retention requirements.

Like other assets, not all information has the same use or value and therefore requires different levels of protection. All Banco de Occidente information will be classified by the Information Owner based on a high-level analysis of business impact in Information Security, determining its relative value and level of risk.

Each classification level will have a set of controls defined by the Information Owner and the Information Security Leader to ensure appropriate and consistent protection throughout the Bank, regardless of medium, format, or location. These controls must be applied throughout the information lifecycle.

2.1.10.13 Business Continuity

Policy: All information resources and mission-critical processes must have a Business Continuity Plan, a Disaster Recovery Plan, and be prepared for Information Security and Cybersecurity attacks.

Information must be available for authorized use when required. Procedures must be developed, documented, implemented, and periodically tested to ensure timely recovery of critical information.

The Bank will establish immediate response measures to detect and mitigate the effects of Cyber attacks against Information Security, such as denial-of-service and the introduction of unauthorized code. These measures will be based on procedures and elements that allow the Bank to remain informed about the existence of these threats, detect attacks immediately, and execute the corresponding actions.

2.1.10.14 Physical Security

Policy: All physical business areas must have a level of security consistent with the value of the information processed and managed within them. Confidential or business-sensitive information must be kept in restricted-access locations when not in use.

The physical security of Banco de Occidente must be based on perimeters and secure areas, which will be protected through appropriate surrounding controls. These must be consistent with the value of the information they contain, and minimum access rights must be granted considering whether the workplaces are permanent or not.

The Bank's IT resources must be physically protected against unauthorized access threats and environmental threats to prevent exposure, damage, or loss of assets and interruption of business activities.

Information classified as confidential or restricted must not be left unattended or uncontrolled; therefore, the Bank will develop a program to prevent critical business information from being accessed without authorization.

2.1.10.15 Non-Repudiation

Policy: The authenticity of any business or electronic transaction carried out by Banco de Occidente must be ensured.

Banco de Occidente increasingly relies on electronic means to conduct its business. Therefore, for any business or transaction carried out through these means, the Bank must ensure the authenticity of each involved party and prevent any of them from denying their participation (non-repudiation).

When conducting electronic business, traceability must be generated to allow the Bank to resolve conflicts when any party denies participation. These must be generated, stored, and accessed in accordance with the Bank's internal Policies and local law.

2.1.10.16 Alert Management

Policy: Banco de Occidente must be alerted at the exact moment when violations of the Information Security and Cybersecurity Policy occur.

Situations or actions that violate this Policy must be detected, recorded, and immediately reported to Senior Management (alerts). An incident management program must be developed that prioritizes such alerts and resolves them according to the criticality of the information for the Bank. Such program must include the definition of an immediate response organization to address these and other situations that the Bank considers critical.

2.1.10.17 Auditability of Information Security Events

Policy: Banco de Occidente's Information Security records must be continuously reviewed to ensure compliance with the Information Security Model.

Information Owners must define events considered critical and the respective Information Security records that must be generated. These must be activated, stored, and continuously reviewed, and unexpected situations must be reported in a timely manner to the Information Owners, as well as to the required levels. Records and the means that generate and manage them must be protected by controls that prevent unauthorized modification or access, to preserve the integrity of the evidence.

2.1.10.18 Connectivity

Policy: All connections to public networks must be authenticated to prevent information from being disclosed or altered.

Connections to Banco de Occidente's private network must be carried out securely to preserve the confidentiality, integrity, availability, and privacy of the information transmitted over the network. Likewise, all outgoing access to other companies must be conducted over networks approved by the Bank.

Members of the Community connecting to the private network must comply with this Policy before the connection is made. This also applies to any current or future connection within the Bank's network that uses public means to integrate geographically dispersed locations.

Approval from the Information Owner is required to remotely access the Bank's information, and such access must comply with the Identification and Authentication Policy.

2.1.10.19 Use of IT resources for busines

Policy: IT resources are provided to the Community for exclusive business use.

Banco de Occidente's IT resources are exclusively for business purposes and must be treated as assets dedicated to providing the tools required to perform the work. Members of the Community who attempt to access information for which they do not have an authorized business requirement are violating this Policy.

When using the Bank's information, privacy should not be assumed; therefore, when it is used, records of the activity performed must be created, which may be reviewed in order to detect abuses and threats. If this is the case, the corresponding procedures will be executed in accordance with the Bank's regulations.

The Bank reserves the right to restrict access to any information at any time it deems appropriate. Selected personnel of the Bank may use restricted-use technology such as network monitoring, operational data, and Information Security event monitoring. No unauthorized hardware or software may be loaded, installed, or activated on IT resources without prior formal authorization from the Information Security Leader.

2.1.10.20 Information Security in System Administration Processes

Policy: Each system administration process of Banco de Occidente must comply with this Information Security and Cybersecurity Policy.

Activities, standards, and responsibilities in Information Security must be included within each of the Bank's system administration processes in order to comply with the Information Security and Cybersecurity Policy.

The systems development area must create and maintain a methodology that controls the full lifecycle of secure system and infrastructure development and maintenance. Information Security requirements must be identified prior to the design of information technology systems. During development, these

requirements must be included within the systems, and if a modification is required, it must strictly comply with the previously established Information Security requirements. The Information Security level of a system must not be reduced; therefore, production information and systems will not be used for development, testing, or maintenance of applications.

The implementation of a new system or a significant change to existing ones must be reviewed through a risk assessment that enables the detection of risks, the identification of appropriate controls to mitigate or eliminate them, and secure operation.

Implementing a technological change that does not consider Information Security requirements exposes the Bank to risks. Therefore, each technological change must ensure compliance with the Information Security Policy and its respective standards, and in case of exposing the Bank to an Information Security risk, it must be identified, evaluated, documented, assumed, and controlled by the respective Information Owner.

The problem management process records, assigns, monitors, and resolves situations (problems) that compromise the availability of services that technology provides to the business. The sources of this process are problems derived from situations that break or compromise the Information Security and Cybersecurity Policy. Therefore, all Information Security problems of the Bank must be managed through this process, which, based on subsequent analysis, will determine whether they correspond to violations, problems, or vulnerabilities in Information Security, leading to the procedures established for each case.

2.1.11 Glossary for the Security Model Policies

The following definitions are some of the concepts used within the Information Security and Cybersecurity environment with which Community members must be familiar:

- **Controls:** Safeguards based on devices or mechanisms required to comply with Policy requirements.
- **Information resources:** All categories of information, including but not limited to records, files, and databases, and (2) information technology facilities, equipment (including personal computing systems), and proprietary or licensed software of Banco de Occidente.
- **Information Owner:** An individual or organizational unit that has responsibility for classifying and making control decisions regarding the use of its information.
- **Physical security:** Protection of information processing equipment from physical damage, destruction, or theft; protection of facilities assigned for information processing from damage, destruction, or unauthorized access; and protection of personnel from potentially harmful situations.
- **Cybersecurity:** Development of organizational capabilities to defend against and anticipate cyber threats in order to protect and secure data, systems, and applications in cyberspace that are essential for the entity's operations.
- **Risk:** The probability that an Information Security event will occur, causing loss to Banco de Occidente.

- **Perimeters or secure areas:** An area or grouping within which a defined set of Security Policies and measures is applied to achieve a specific level of security. Areas or zones are used to group entities with similar security requirements and risk levels, ensuring that each zone is properly separated from others.

- **Community member:** An individual who has limited and specific authority from the Information Owner to view, modify, add, disclose, or delete information.

3. OPERATING PROCEDURE

The security management processes mentioned in the Cybersecurity Standards are:

3.1 USER IDENTIFICATION AND AUTHENTICATION

Identifies and verifies the identity of users and programs accessing systems.

3.2 ACCESS CONTROL

It protects computer resources by ensuring that they can only be used by authorized individuals or programs. Access control techniques can be used to protect a variety of resources including hardware, operating systems, communications centers, programs, and files or databases.

3.3 AVAILABILITY

Ensures that all system facilities, including security services, are available as required for business applications and system infrastructure.

3.4 CONFIDENTIALITY

It ensures that information controlled by the system is not used or accessed in violation of access control policies. Confidentiality mechanisms can protect the content of communications, the contents of files and databases, programs, program tables, and other files required by the system. Encryption techniques are used to provide confidentiality.

3.5 INTEGRITY OF INFORMATION

It ensures that the information in any form has not been modified either inadvertently or deliberately. Integrity mechanisms also make it possible to recognize when the integrity of a resource has been violated.

3.6 DISASTER RECOVERY

Verify that the security controls that were established for the operation of the computer resources are not diminished by the fact of operating under the environment defined in the disaster recovery plan.

3.7 PHYSICAL SECURITY

It involves the physical protection of resources such as office work areas, desks, computers, and communication lines. Physical resources are exposed to risks created by accidental and deliberate threats.

3.8 CERTIFICATION OF INFORMATION

It demonstrates that the communication of the information indicated as having been sent to a recipient was, in fact, sent and received, and that the communication of the information indicated as having been received from a sender was, in fact, issued by the sender.

3.9 ALERT MANAGEMENT

Notify security managers and resource owners when security breaches occur. The most effective security alert processes automatically notify the appropriate party as soon as a security breach occurs. A security alert should result in the initiation of an analysis, review, and, if necessary, disciplinary proceedings.

3.10 AUDITABILITY MANAGEMENT

Review safety-related practices and activities. Review the security privileges granted to users of the system, the information files related to the security logs that are recorded as the system is used, and the manual and automatic procedures related to Information Security.

3.11 SECURITY MANAGEMENT

It involves the ongoing activities of security administrators who implement security policies, standards, and procedures using a variety of manual and automated techniques.

3.12 POLICY MANAGEMENT

It defines the security policies that will be managed, published as part of the security awareness process, and executed with manual and automated procedures.

3.13 RISK ASSESSMENT

Identify, analyze, and document the threats and risks that the business faces due to the lack of adequate protection of the Institution's information. It assesses the degree of exposure to which the Institution can

be subjected for each risk assumed and determines the degree of importance of eliminating them. It also helps to identify the Business Information Owners (we understand by Owner the executives responsible for the origin of the information). Risk assessment provides the basis for developing security policies.

3.14 SAFETY AWARENESS

It involves an ongoing program designed to train and transform staff on the importance of safety and on tools and techniques to enforce security policies. Awareness programs are aimed at effective system-oriented, system-oriented policies and procedures, work environment, work style, and safety procedures.

3.15 STRUCTURE AND ORGANIZATION

It consists of the organization and personnel that is responsible for identifying and analyzing security threats, developing security policies, auditing security practice, and responding to security breaches.

NOTE: These processes are pending documentation and will later be available with a higher level of detail and description in this manual.

-END OF THE PROCESS-



The Information Security Policies are a statement of the responsibilities and accepted conduct to maintain a secure environment at Banco de Occidente. These Policies establish the guidelines and the guidelines related to the secure handling of information.

Political Outreach

The Information Security and Cybersecurity Policy provides the guidelines required to implement a reliable and flexible Information Security Model.

It defines the basic framework that follows the implementation of anynorm, process, procedure, standard and/or action, related to Information Security in the Bank of Occidente and subsidiaries.

It applies to all levels of the organization that access, either internally or externally, to any information asset regardless of its location.

- Users (which includes employees and shareholders)
- Customers (which includes employees and shareholders)
- Third parties (including suppliers and contractors)
- Controlling Entities
- Related and Affiliated Entities of the Bank of the West

The policy applies to all information created, processed or used in support of the business, and information provided to employees, regardless of the medium, format, presentation or location in which it is found.

Defined policies

Information Security
- Cybersecurity
- Intellectual property
- Owner of Information
- Regulatory Compliance
- Risk management in security of the information (IS) and cybersecurity (CS).
- Training and culture creation in IS and CS
- Personnel safety

- Third Parties Accessing Bank Information West Local or Remote
- Individual Identification and Authentication
- Access Control and Management
- Information Classification
- Business Continuity
- Physical Security

- Non-Repudiation
- Alert Management
- Auditability
- Connectivity
- Use of Computer Resources
- System Administration Security