Procedures Manual

INFORMATION SECURITY MANUAL

MAN-APY-177

Date: 20/05/2025
Version: 2.5

Indoor Use

Content

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 INFORMATION SECURITY STANDARDS 4

1.2.1 Scope 4

1.2.2 Compliance 5

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 safe environment at Banco de Occidente. This Policy sets forth the guidelines and guidelines related to the secure handling of information.

1.1.1. Principles

In order to comply with its business objectives, Banco de Occidente has established the following principles that support the Information Security and Cybersecurity Policy as fundamental:

- 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 and third-party information must be maintained, regardless of the medium or format in which it is located.
- Business information must preserve its integrity regardless of its temporary or permanent residence, or the way in which it is transmitted.
- Business information should be available when requested.
- 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 its business functions (Confidentiality); that is protected from unplanned modifications, made intentionally or unintentionally (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:
- To establish the foundations for the development and implementation of the Information Security Model.
- Define the conduct to be followed in relation to access, use, management and administration of information resources.
- Establish and communicate responsibility in the use of information assets, which support business processes and systems.
- Manage risks in Information Security and Cybersecurity.
- Establish communication channels that allow Senior Management to stay informed of the risks and inappropriate use of information assets, and the

actions taken for its mitigation and correction, generating culture and commitment at all levels.

- To raise awareness in the Community about cybersecurity risks and ensure that they have the knowledge, skills and technological means necessary to maintain the objectives of Information Security.
- To protect the image, interests and good name of Banco de Occidente.

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

This Policy is part of Banco de Occidente's Security Model headed by the Information Security Leader, they are reviewed and approved by Banco de Occidente's board of directors and Information Security Committee and disseminated to the Information Owners, the Community and the different Information Security roles.

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

1.2 OBJECTIVES OF INFORMATION SECURITY STANDARDS

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

By applying the standards set forth in this document, Banco de Occidente defines how information is protected homogeneously, and in a manner consistent with its criticality for the business, in all computer 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, which is supported by the internal Information Security and Cybersecurity procedures, which aim to document the main operational actions to be executed in order to safeguard confidentiality. integrity and availability of information, maintaining the levels of security accepted by Banco de Occidente.

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

1.2.2 Compliance

The rules must be complied with by all those who have access to or make use of Banco de Occidente's information through software, hardware, networks and associated facilities.

Compliance with the rules is mandatory and any exceptions 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 rules and the responsibilities of their strict compliance.

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

For new developments or new acquisitions of computer resources, the rules are in force from the period of validity of the same. A detailed plan must be established to adjust the computer resources acquired prior to this validity to make effective compliance with the standard.

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