1. Objective and Scope of the Document

This policy establishes the principles, commitments, and strategic guidelines for the protection of information across all organizational processes, services, and technological assets. It applies to all individuals, resources, and systems involved in the operation, management, and support of corporate information, and serves as the foundation of the Information Security Management System (ISMS), in accordance with the guidelines of the ISO/IEC 27001 standard.

2. Policy Statement

At BPM Consulting S.A.S., Top Management establishes its commitment to implement, maintain, and continuously improve the Information Security Management System (ISMS), recognizing the protection of information assets as a strategic element for business continuity, customer trust, and compliance with applicable requirements.

For the effective management of information security, the organization commits to:

Compliance with applicable legal, regulatory, contractual, and relevant stakeholder requirements.
• Alignment with the organizational strategy and business objectives.
• Systematic management of information security risks.
• Strengthening organizational capabilities in information security

3. Information Security Principles

Information security management is based on the following principles:

- • Confidentiality: Information is accessible only to authorized individuals.
  • Integrity: Information is accurate, complete, and reliable.
  • Availability: Information is accessible when required.

4. Information Security Objectives

1. To protect the organization’s critical information assets.
2. To ensure the availability and continuity of information security.
3. To maintain compliance with applicable legal, regulatory, and contractual requirements.
4. To achieve conformity of the ISMS in accordance with ISO/IEC 27001 requirements.
5. To incorporate technology that supports the management of the Information Security System.

The objectives will be defined, measured, and monitored through indicators established within the ISMS.

5. Risk Management Approach

The organization adopts a risk-based approach to information security management, which enables:

- Systematically identify, analyze, and treat risks.
- Prioritize the implementation of controls based on the level of exposure.
- Maintain risk within the acceptable levels defined by the organization.

6. ISMS Integration

The ISMS is supported by a set of guidelines that enable its operation, including:

- Mobile Devices Policy
- Logical Access Control Policy
- Information Classification, Labeling and Handling Policy
- Cryptographic Controls and Key Management Policy
- Clear Desk and Clear Screen Policy
- Security Policy for Supplier Relationships
- Secure Development Policy
- Information Security Guidelines for Software Development
- Guidelines for the Secure Management of Passwords, Credentials, and Secrets
- Operational Quality Policy
- Physical Access Control Policy
- Acceptable Use of Assets Policy
- Information Backup Policy
- Teleworking Policy
- Implementation and Operation of BPO Services
- Integrated Management System Policy
- Information Transfer Policy
- Personal Data Processing Policy
- Guidelines for the Governance, Security, and Trustworthy Use of Artificial Intelligence
- Cloud Services Security Policy

These guidelines are developed in specific documents that complement this policy.

7. Roles and Responsibilities in Information Security

General Management
General Management provides strategic leadership for the Information Security Management System (ISMS), ensuring its alignment with institutional objectives. Its main responsibilities are:

- Define and approve the strategic information security objectives.
- Allocate the necessary resources for the operation and improvement of the ISMS.
- Approve the system's key policies and guidelines.
- Promote the implementation and culture of information security throughout the organization.
- Oversee compliance with regulatory obligations.
- Evaluate and approve strategic projects related to information security.

Steering Committee

The Steering Committee acts as a tactical and strategic decision-making body that supports the management of the ISMS, ensuring its alignment with organizational objectives and facilitating the effective implementation of institutional information security guidelines.

Its main responsibilities are:

- Periodically review the status of the ISMS and propose actions for its continuous improvement.
- Analyze relevant risks and recommendations derived from Business Impact Analysis (BIA) and vulnerability assessments.
- Validate the suitability of implemented controls and measures, and propose adjustments when necessary.
- Oversee compliance with information security plans and projects approved by General Management.
- Support the integration of information security across all organizational processes.
- Coordinate actions with different areas to ensure regulatory and contractual compliance in information security matters.
- Facilitate decision-making when high-impact security incidents occur.

Area Managers

Area Managers are responsible for ensuring that the activities under their supervision are carried out in accordance with the guidelines established by the ISMS, acting as a bridge between the information security policy and its practical application in the operational environment.

Their responsibilities include:

- Implement and maintain the security controls defined for their respective processes.
- Ensure proper classification, use, and protection of the information they manage.
- Identify and report risks or incidents related to information security.
- Promote a security culture within their teams.
- Actively participate in awareness, training, and internal audit activities.
- Collaborate with the Steering Committee and the Information Security Officer in updating policies, procedures, or controls when gaps or relevant changes are identified.

Information Security Officer (ISO)
The Information Security Officer (ISO) is the designated responsible person for coordinating, advising, and monitoring the implementation of the ISMS. This role acts as the focal point between the organizational strategy and the application of security measures, ensuring compliance with regulatory, contractual, and technical requirements.

Its responsibilities include:

- Coordinate the implementation and maintenance of the ISMS.
- Manage system documentation and ensure its updating.
- Coordinate the identification, analysis, and treatment of information security risks.
- Monitor established controls and propose adjustments when necessary.
- Consolidate information for management review and internal or external audits.
- Promote awareness, training, and information security culture initiatives.
- Act as a liaison with regulatory bodies, competent authorities, and stakeholders when relevant incidents occur.

Employees / Collaborators

All employees of the organization are responsible for complying with and applying the guidelines established in the Information Security Management System (ISMS), acting consciously, ethically, and diligently in the use, handling, and protection of information assets.

Their responsibilities include:

- Comply with information security policies, procedures, and guidelines.
- Ensure the confidentiality, integrity, and availability of the information they handle or manage.
- Report promptly any incident, vulnerability, or anomaly that may affect information security.
- Actively participate in information security training and awareness programs.
- Use technological resources in accordance with the organization's established guidelines.

Contractors and Third Parties
Contractors, suppliers, and third parties who access the organization's technological infrastructure, systems, or information are subject to compliance with the ISMS guidelines, which include:

confidentiality agreements and the commitments established in the corresponding contracts or agreements.

Their responsibilities include:

- Comply with confidentiality agreements and authorized access levels.
- Ensure proper handling of the information they access within the scope of their duties or services.
- Follow the organization's instructions regarding the use of technological resources and security procedures.
- Immediately report any incident, data breach, or abnormal situation affecting information assets or data.
- Participate, when required, in induction or training activities related to information security.

8. GLOSSARY

Information Security: Preservation of confidentiality, integrity, and availability of information.
ISMS (Information Security Management System): A structured framework of policies, procedures, and controls for managing information security risks.
Confidentiality: Ensuring that information is accessible only to authorized individuals.
Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Availability: Ensuring that information is accessible when required by authorized users.
Risk: The possibility of a threat exploiting a vulnerability and causing harm to information assets.
Risk Management: The process of identifying, analyzing, evaluating, and treating risks.
Asset: Anything that has value to the organization, including information, systems, and infrastructure.
Control: A measure or safeguard implemented to manage or reduce risks.
Incident: An event that may compromise the confidentiality, integrity, or availability of information.
Vulnerability: A weakness that can be exploited by a threat.
Threat: A potential cause of an incident that may harm information assets.
Compliance: Adherence to legal, regulatory, contractual, and internal requirements.
Third Party: External individuals or organizations that provide services or have access to organizational information.
BIA (Business Impact Analysis): A process to identify and evaluate the effects of disruptions on business operations.
Cryptography: Techniques used to protect information through encryption and secure communication.
Authentication: Process of verifying the identity of a user or system.
Access Control: Mechanisms that regulate who can access information or systems and under what conditions.

Protection of the confidentiality, integrity, and availability of information, as well as other aspects such as authenticity and traceability.

Information Security Management System (ISMS)
A set of policies, processes, and resources used to manage information security within the organization and continuously improve it.

Change Control		
ersion	**Approval date**	**Description**
01	16-02-2022	Document Creation
02	17-05-2022	• A list of interested parties has been added. • The purpose of each policy that is part of the system is briefly described.
03	27-06-2023	The policy statement was updated, objectives and responsibilities were added, and the items related to the existing security policies were updated.
04	02/01/2024	Change of the document classification from Private to Public.
05	06/03/2024	Update of the following elements: • General policy objective • Information Security objectives in accordance with Management Review • Removal of detailed texts for each policy included in the document • Inclusion of the list of policies applicable to the Information Security System
06	07/05/2024	Update of the chapter “Complementary Information Security Policies”: • Removal of policies related to environment, occupational health and safety, diversity, equity and inclusion, and labor disconnection, as their scope does not include information security. • Inclusion of the document “Information Security Guidelines for Software Development.”
07	06/12/2024	Inclusion of **“Guidelines for Password Management” i**n the chapter “Complementary Information Security Policies.”
08	16/04/2025	• Update of the document name considering its content. • Update of the document structure by chapters for better understanding. • Adjustment of role responsibilities to align them with the ISMS. • Update of contacts for authorities and special interest groups

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCION**
		• Editorial adjustments throughout the document to provide clearer and more easily understandable information for stakeholders.
09	20/06/2025	Update of Chapter 5, “Complementary Information Security Policies,” to include the Cloud Services Security Policy.
10	23/02/2026	Update of the corporate image through the adjustment of the new logo and the adaptation of colors in tables and text, aligned with the new institutional color palette.
11	27-03-2026	The document has been updated in Chapters 2, 3, and 4 in order to optimize its wording, improve clarity, and strengthen its alignment with the organizational strategy and the requirements of ISO/IEC 27001:2022, facilitating its understanding and adoption by stakeholders. The adjustment includes the simplification of content, the organization of information security principles, and the consolidation of commitments related to risk management, information asset protection, legal compliance, and continuous improvement, without modifying its scope or intent.