Information Security Policy

I. OBJECTIVE

To establish a governance, operational, and control framework for the protection of information assets and the technological resources that support them, in order to ensure the confidentiality, integrity, and availability of information.

Specific Objectives:

• Strengthen the organizational culture of Information Security and Cybersecurity by promoting awareness, continuous training, and the participation of all employees, with the explicit and sustained support of senior management.

• Manage Information Security and Cybersecurity risks by identifying, assessing, treating, and monitoring risks that may affect information assets, in order to minimize their likelihood and impact, ensuring the confidentiality, integrity, and availability of business-critical information.

• Ensure compliance with legal, regulatory, contractual, and normative requirements applicable to the organization in matters related to Information Security and Cybersecurity by establishing governance and control mechanisms that demonstrate compliance and continuous improvement.

• Implement and maintain technical, administrative, and physical controls aimed at protecting information assets against internal and external threats, ensuring a cybersecurity posture appropriate to the organization's context and risk level.

• Establish guidelines, responsibilities, and minimum requirements to ensure compliance with the Information Security Management System (ISMS) and the protection of the organization's information and services.

II. SCOPE

This Policy shall be complied with by all employees of Rimac Seguros, Rimac EPS, and third parties that exchange the Company's information assets through physical or digital means.

The protection of information assets applies to all environments where information is processed, transmitted, and stored. This includes, but is not limited to, cloud and on-premises environments, prioritizing the protection of the organization's critical infrastructure.

III. OTHER REFERENCES

• Law No. 29733 – Personal Data Protection Law

• SBS Resolution No. 504

• PCI DSS

• ISO 27001

• NIST V2

IV. POLICY DEVELOPMENT

1. Technology and Information Risk Management

We maintain a formal process for the identification, analysis, assessment, and treatment of information-related risks. Risks are analyzed considering criteria such as impact and frequency, enabling data-driven decision-making and the prioritization of mitigation resources.

The documentation generated supports our business continuity plans, operational controls, and incident response protocols, and is overseen by the areas responsible for security and internal audit.

2. Third-Party Risk Management

Recognizing that the supply chain represents a critical point in security, we apply specific controls to third parties that access or manage information relevant to the organization.

The measures adopted include:

• Risk assessments prior to engaging suppliers.

• Inclusion of confidentiality, privacy, and security clauses in contracts.

• Review of controls implemented by suppliers, particularly when technological services, cloud services, or personal data processing are involved.

• Continuous monitoring and periodic reviews of suppliers classified as critical.

These practices enable us to ensure that our partners comply with protection standards equivalent to our own regarding information security.

3. Security in Organizational Processes

Security is integrated into key operational processes. Each business area has guidelines and procedures that include:

• Role-based access control and the principle of least privilege.

• Segregation of environments and functions (development, testing, and production).

• Approval and validation of technological changes through formal procedures.

• Logging and traceability of relevant actions within systems.

Additionally, technical controls for monitoring, event logging, and log reviews are implemented, providing continuous visibility into operational activities, enabling the detection of anomalous behavior, and supporting regulatory compliance.

4. Security in Projects and Technology Developments

All new developments, integrations, or system implementations shall comply with security-by-design principles, ensuring that information protection is incorporated from the earliest stages of the project. Our approach is based on applying secure development best practices throughout the entire lifecycle, including:

• Architecture and technical design reviews by the security team to ensure that solutions comply with corporate and regulatory standards.

• Vulnerability assessments and security validations, including automated analyses, manual reviews, and ethical hacking tests conducted by internal or external specialists. These tests simulate controlled attack scenarios to identify and remediate vulnerabilities before production deployment.

• Formal documentation of risks, dependencies, and implemented controls, ensuring traceability and regulatory compliance.

• Change management controls are administered including an information security perspective, allowing validation that the aforementioned requirements are met.

This comprehensive approach enables us to reduce security risks, prevent breaches, and ensure that technological solutions are reliable and resilient, contributing to business continuity and data protection.

5. Human Risk Management

We recognize that people can be both the first line of defense and a point of vulnerability. Therefore, we continuously work on training, awareness, and the management of human behavior in security matters.

Our initiatives include:

• Mandatory security and privacy training for all employees.

• Thematic training sessions throughout the year focused on current risks such as phishing, artificial intelligence, and device protection.

• Social engineering attack simulations to measure the effectiveness of training activities.

• Disciplinary procedures in the event of non-compliance with our Information Security Policy.

• Monitoring of security behavior indicators aimed at strengthening a preventive and proactive culture.

These actions not only seek regulatory compliance but also strengthen an organizational culture of security by promoting secure behaviors and responsible decision-making in the face of threats. We believe that the awareness and commitment of each employee are essential to reducing risks, protecting information, and ensuring business continuity.

6. Protection of Critical Infrastructure and Systems

Our technological infrastructure is protected through a comprehensive security approach that combines physical and logical controls with continuous monitoring processes to ensure the availability, integrity, and confidentiality of information. This approach also extends to the secure adoption of emerging technologies, such as artificial intelligence, ensuring that their use is aligned with security, privacy, and risk management principles.

The primary measures implemented include:

• Network segmentation and perimeter monitoring to reduce risks and control traffic between critical environments.

• Advanced threat detection and prevention controls that enable the timely identification of and response to incidents.

• Application and data protection mechanisms designed to prevent unauthorized access and information leakage.

• Enhanced authentication and secure access management, ensuring that only authorized users and devices interact with systems.

• Centralized monitoring and event analysis to anticipate risks and act proactively.

• Business continuity and disaster recovery plans, periodically tested to ensure operational resilience.

Additionally, we maintain an Incident Response Plan that establishes clear procedures for detection, containment, eradication, and recovery in response to security events. This plan includes timely notification of responsible areas, coordination with specialized teams, and the execution of corrective and preventive actions, ensuring that each incident is managed efficiently and that lessons learned are incorporated to strengthen the security posture.

This set of measures enables us to maintain secure and reliable operations even under adverse circumstances, aligning with international standards and local regulations.

7. Access Controls

Define controls for access to information and the critical systems that support it, ensuring that each user is granted only the access necessary to perform their functions.

The primary practices implemented include:

• Multi-factor authentication in applications federated with Entra ID.

• Access monitoring, enabling the detection of deviations and proactive response.

• Development of role matrices for critical applications, which are used as the basis for access management.

This approach enables the protection of information and resources, reduces the risk of unauthorized access, and strengthens security throughout the organization.

V. APPROVAL WORKFLOW RESPONSIBILITIES

Our Information Security Policy was approved in 2026 under the following process:

Stage	Area	Position	Name
Owner	INFORMATION SECURITY	INFORMATION SECURITY MANAGER	Karla Mariella Parra Bocanegra
Editor	INFORMATION SECURITY RISK MANAGEMENT	RISK ENGINEER PROFESSIONAL	Alexandra Alicia García Abanto
Reviewer	INFORMATION SECURITY RISK MANAGEMENT	RISK ENGINEER PROFESSIONAL	Edu Denilson Acosta Bejarano
Reviewer	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo

Approver	INFORMATION SECURITY	INFORMATION SECURITY MANAGER	Karla Mariella Parra Bocanegra
Approver	IT AND DATA DIVISION	EXECUTIVE VICE PRESIDENT	Carlos Herrera Cornejo
Approver	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo
Approver	OPERATIONAL RISK AND CONTINUITY	OPERATIONAL RISK AND CONTINUITY MANAGER	Renato Bedoya Chirinos