Information Security Policy

I. OBJECTIVES

- To establish a governance, operation, and control framework for the protection of the assets and technological resources that support them, in order to ensure the confidentiality, integrity, and availability of information.
- To establish a culture of Information Security and Cybersecurity management in organizational processes with the support of senior management.
- To manage Information Security and Cybersecurity risks to minimize their materialization impact, guaranteeing the confidentiality, integrity and availability of information in accordance with the strategic objectives of the business.
- To comply with legal, regulatory and third-party requirements that affect the organization in relation to Information Security and Cybersecurity.

II. SCOPE

This policy must be complied by all employees of Rimac Seguros, Rimac EPS and third parties who exchange the company's information assets in physical or digital media.

The protection of information assets has applicability to all environments where information is processed, transmitted and stored. This includes and is not limited to cloud or on-premise environments, with the protection of the organization's critical infrastructure as a priority.

III. OTHER REFERENCES

- Law No. 29733 – Personal Data Protection Law
- SBS 504 Resolution
- PCI DSS
- ISO 27001
- NIST V1.

IV. POLICY GUIDELINES

1. Technology and Information Risk Management

We have a formal process for identifying, analyzing, evaluating, and dealing with information-related risks. Risks are analyzed considering criteria such as impact and probability, which allows decisions to be made based on data and prioritize mitigation resources.

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

2. Risk Management in Suppliers

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

Among the measures adopted are:

- Risk assessments before hiring suppliers.
- Inclusion of confidentiality, privacy and security clauses in contracts.
- Review of controls applied by the provider, especially when it comes to technological services, cloud or personal data processing.
- Continuous monitoring and periodic reviews for suppliers classified as critical.

These practices allow us to ensure that our partners meet equivalent standards to ours in terms of information protection.

3. Security in Organizational Processes

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

- Access control based on roles and principles of least privilege.
- Separation of environments and functions (development, testing and production).
- Approval and validation of technological changes through formal procedures.
- Recording and traceability of relevant actions within the systems.

In addition to this, technical controls are applied for monitoring, event logging and log review, allowing continuous visibility on operational activity, detection of anomalous behavior and regulatory compliance.

4. Safety in Projects and Technological Developments

All new system developments, integrations or implementations must comply with security principles by design, ensuring that information protection is incorporated from the initial phases of the project. Our approach is based on the application of good secure development practices throughout the entire lifecycle, including:

- Architecture and technical design review by the security team to ensure solutions meet corporate and regulatory standards.
- Vulnerability testing and security validations, including automated scans, manual reviews, and ethical hacking tests performed by internal or external specialists. These tests simulate controlled attack scenarios to identify and remediate vulnerabilities before they go into production.
- Formal documentation of risks, dependencies and controls applied, ensuring traceability and regulatory compliance.
- We are part of the change control flow, which allows us to validate that they comply with the above.

This integral approach allows us to reduce security risks, prevent breaches, and ensure that technology 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. For this reason, we are constantly working on training, awareness and management of human behavior in safety.

Our initiatives include:

- Mandatory training on security and privacy issues for all employees.
- Thematic trainings during the year, focused on current risks such as phishing, artificial intelligence and device protection.
- Simulations of social engineering attacks to measure the effectiveness of training.
- Sanction procedures in case of breaches of our information security policy.

These actions not only seek to comply with regulations, but also to strengthen the security culture throughout the organization, promoting responsible and proactive behaviors in the face of threats. We believe that the awareness and commitment of each employee are key factors to reduce risks, protect information and ensure business continuity.

6. Protection of Critical Infrastructure and Systems

Our technological infrastructure is protected by a comprehensive approach to security, which combines physical and logical controls and continuous monitoring processes to ensure the availability, integrity and confidentiality of information.

Key measures implemented include:

- Network segmentation and perimeter monitoring, to reduce risks and control traffic between critical environments.
- Advanced threat detection and prevention controls, which allows to identify and respond to incidents in a timely manner.
- Protection of applications and data, through mechanisms that prevent unauthorized access and information leaks.
- Strong authentication and secure access management, ensuring that only authorized users and devices interact with the systems.
- Centralized monitoring and event analysis, to anticipate risks and act proactively.
- Continuity and disaster recovery plans, regularly tested to ensure operational resilience.

In addition, we have an Incident Response Plan, which establishes clear procedures for the detection, containment, eradication and recovery from security events. This plan includes timely notification to the responsible areas, coordination with specialized teams and the execution of corrective and preventive actions, ensuring that each incident is managed efficiently and that learnings are incorporated to strengthen the security posture.

This set of measures allows us to maintain safe and reliable operation, even in the face of adverse scenarios, aligning ourselves with international standards and local regulations.

7. Access Controls

We manage access to critical information and systems under the principle of least privilege, ensuring that each user has only the necessary permissions to perform their functions.

Key practices implemented include:

- Strong authentication, which incorporates additional mechanisms to validate the identity of users in sensitive accesses.
- Centralized management of identities and roles, to ensure timely assignment and revocation of permissions.
- Access monitoring and traceability, allowing unusual behavior to be detected and proactively responded.

This integral approach allows us to protect the confidentiality and integrity of information, reducing the risk of unauthorized access and strengthening security throughout the organization.

V. APPROVAL FLOW

Our Information Security policy was approved in 2024 under the following process:

Etapa	Área	Cargo	Nombre
Owner	INFORMATION SECURITY	INFORMATION SECURITY MANAGER	Karla Mariella Parra Bocanegra
Editor	INFORMATION SECURITY RISKS	RISK ENGINEER PROFESSIONAL	Edu Denilson Acosta Bejarano
Proofreader	INFORMATION SECURITY RISKS	RISK ENGINEER PROFESSIONAL	Edu Denilson Acosta Bejarano
Proofreader	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo
Approver	INFORMATION SECURITY	INFORMATION SECURITY MANAGER	Karla Mariella Parra Bocanegra
Approver	IT & DATA DIVISION	EXECUTIVE VICEPRESIDENT	Carlos Alberto Herrera Cornejo
Approver	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo
Approver	OPERATIONAL RISKS AND CONTINUITY	OPERATIONAL RISKS AND CONTINUITY MANAGER	Renato Bedoya Chirinos