Data Security and Privacy Management 2025

RIMAC

Information Security Management Programs

RIMAC

Information Security Policy

RIMAC establishes a governance, operational, and control framework to protect information assets and the technological resources that support them, ensuring the confidentiality, integrity, and availability of information.

01. Governance and Risk Management

A formal process is in place to identify, analyze, evaluate, and address information security risks based on impact and likelihood criteria.

02. Security in Processes and Technology

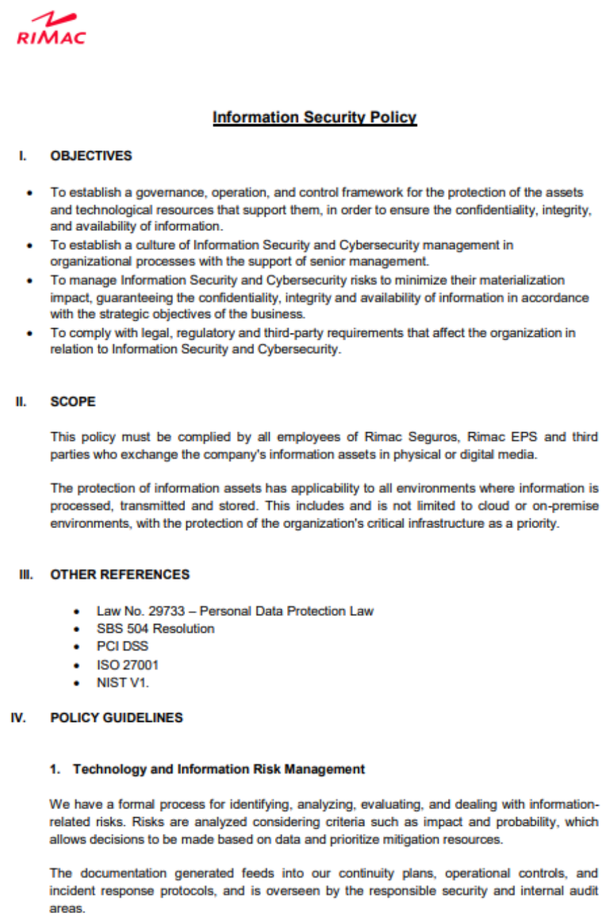
Role-based access controls, the principle of least privilege, segregation of environments, change validation, monitoring, and log reviews.

03. People and Suppliers

Mandatory training, topic-specific sessions, social engineering simulations, and controls for critical third parties.

04. Incident Response and Resilience

Business continuity and disaster recovery plans are regularly tested, together with an Incident Response Plan.



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

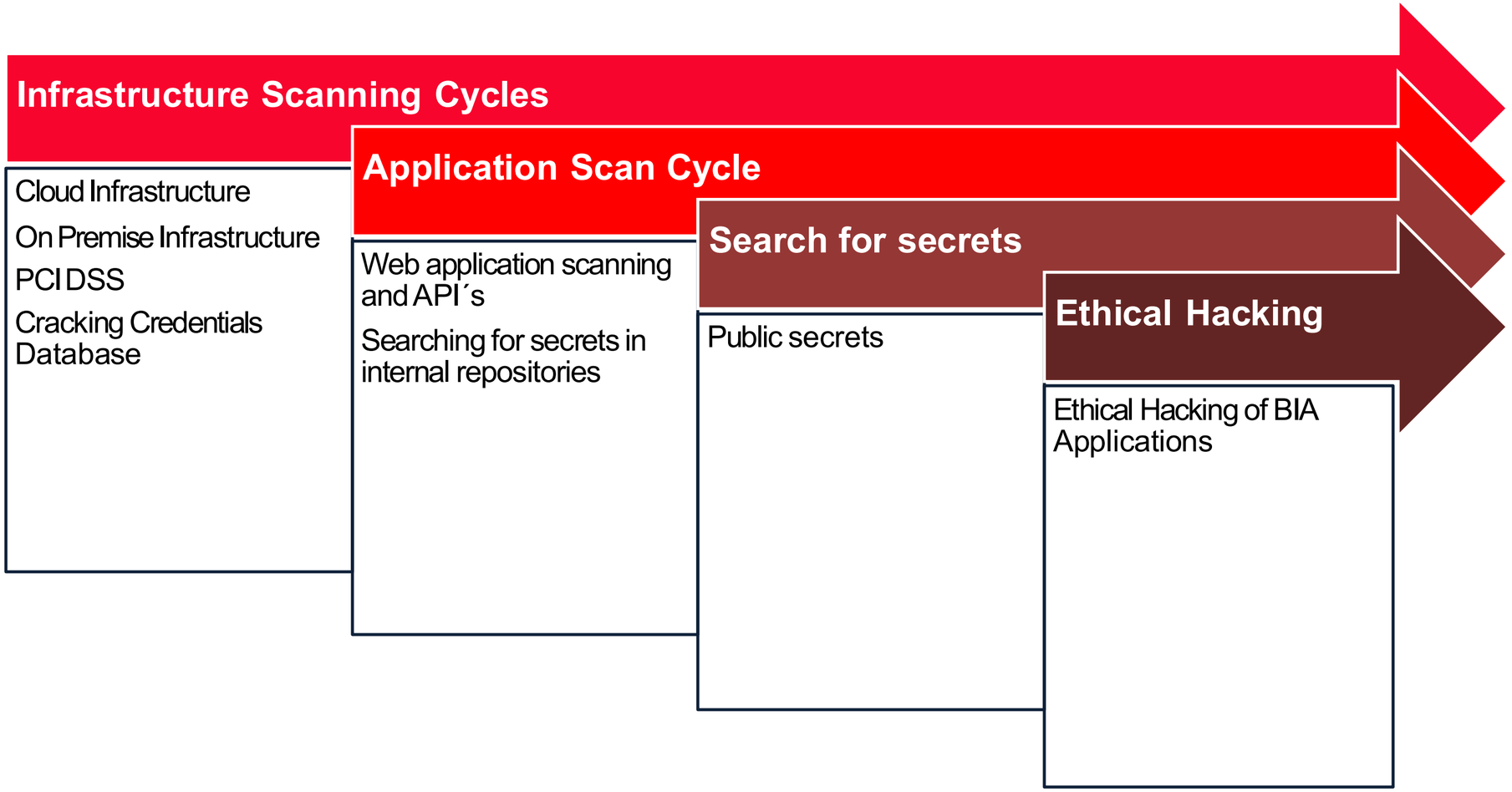
1. Technology and Information Risk Management

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.

Click here to view our Information Security Policy.

Vulnerability Management Roadmap 2025



Baseline Monitoring Management Roadmap 2025

Monitoring of cybersecurity baselines and vulnerabilities across systems hosted within RIMAC's internal infrastructure.

Onpremise

Cloud

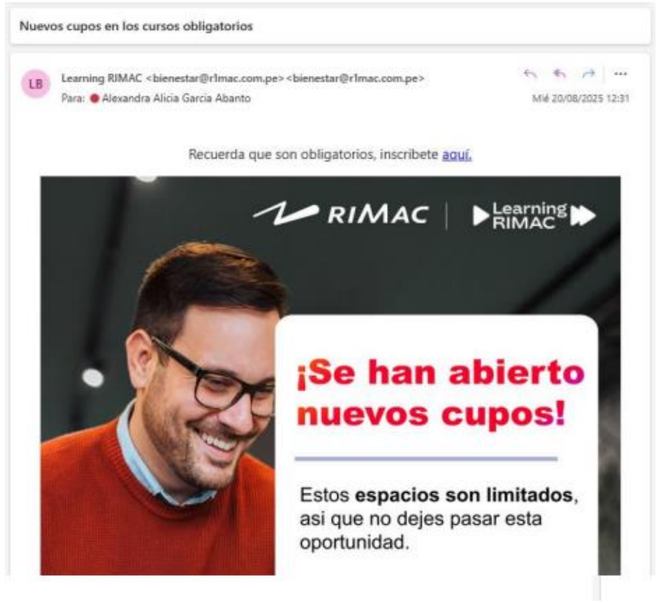
Monitoring of cybersecurity baselines and vulnerabilities across systems and services hosted in cloud environments.

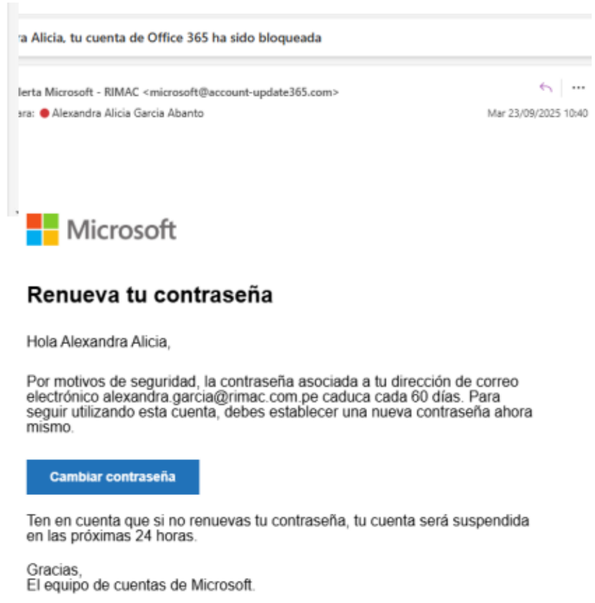
The Baseline Monitoring and Vulnerability Management Plan helps us identify, assess, and track cybersecurity gaps to prevent potential threats and attacks.

Cibersecurity drills

We also carry out cybersecurity drills to keep our employees alert and ensure that they can correctly identify different threats.

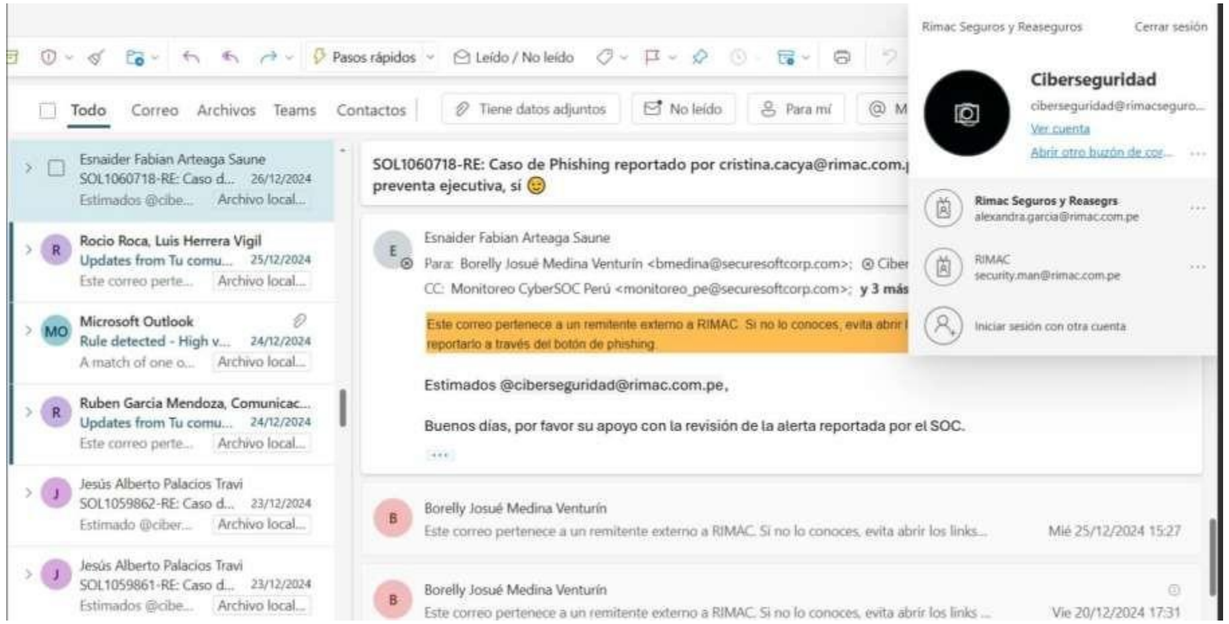
As presented in the example, a mass email is sent to all employees with a phishing simulation and those who cannot correctly identify it are sent an explanation email after that.





Cybersecurity Mailbox

At RIMAC we have an email that works as a mailbox to receive concerns and reports of cybersecurity cases in the organization. This email is **ciberseguridad@rimac.com.pe**



Cybersecurity Incidents Report

Upon receiving a report about a cybersecurity incident through the mailbox, the cybersecurity area conducts an investigation of the case. For example, in the case of phishing presented below, an analysis of the email is carried out to determine if it does indeed present a risk and at what level, as well as the actions to be taken.

De: Borelly Josué Medina Venturín <bmedina@securesoftcorp.com>
Enviado: miércoles, 25 de diciembre de 2024 15:27
Para: ciberseguridad@rimac.com.pe <ciberseguridad@rimac.com.pe>; CyberSOC RIMAC <cybersoc_rimac@securesoftcorp.com>
Cc: Monitoreo CyberSOC Perú <monitoreo_pe@securesoftcorp.com>; Soporte Secure Soft Perú <soporte@securesoftcorp.com>; Soporte Onsite Rimac <soporte_onsite_rimac@securesoftcorp.com>; SMARTFENSE <preport@livefense.com>
Asunto: RE: SOL1060718-RE: Caso de Phishing reportado por cristina.cacya@rimac.com.pe: Santa no te traerá un ascenso...la preventa ejecutiva, sí 😀

Estimado @CyberSOC RIMAC buen día,

Se realizó el análisis del correo en un ambiente seguro **Sandbox**

Conclusión del Análisis:

Posible campaña de spam publicitario: El correo parece ser parte de una campaña de spam publicitario que ofrece programas educativos de desarrollo profesional. El tono de detallada sobre la oferta hacen que este correo se asemeje más a un mensaje de marketing masivo que a una oferta legítima.

Acciones a Tomar - Securesoft	Realizar el bloqueo proactivo de las **IOC´s** maliciosa/sospechosa en todas las plataformas (Soporte) (previa confirmación)
Acciones a Tomar - Cliente	Revisar si los **IOC´s** pertenece a un proveedor o servicio, de ser el caso solicitar el bloqueo. (Cliente) Indicar a los usuarios finales que No deben ingresar credenciales y/o información personal en páginas no autorizadas. Evite hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas o sospechosas. Eliminar el correo del buzón de las personas que recibieron dicho correo. Evitar el uso de las cuentas corporativas en páginas que no estén asociadas a las funciones de la empresa. NO hacer clic en hipervínculos de correos electrónicos de remitentes desconocidos. NO abrir correos si se desconoce el sender e inmediatamente remitirlo al área de ciber-seguridad para su posterior revisión.

Supplier Cybersecurity Homologation

Through the homologation document, suppliers commit to RIMAC's General Information Security Terms when they store, process, transfer, or access RIMAC information.

Supplier responsibilities

Safeguards • Training • Assessments • Incident response

01

Safeguards & access

- Administrative, technical, and physical controls
- Secure authentication and access by legitimate need
- Logs retained for at least 90 days
- Malware controls, security patches, and credential protection

02

Training & human risk

- Annual training and continuous supervision for personnel with access to RIMAC information
- Phishing tests, secure password practices, and cyberattack prevention
- Competency evaluations and reinforcement plans

03

Assessments & audits

- RIMAC may request control assessments, on-site evidence, and vulnerability reports
- Suppliers self-assess safeguards at least annually
- Audit reports, penetration tests, or certifications may be provided, including ISO 27001, SOC1, SOC2, or PCI

04

Incident response

- Maintain a security incident response program
- Notify RIMAC within no more than 24 hours after discovering a security incident
- Correct critical, high, and medium findings within 30, 60, and 90 days

To view the full policy, click here.

Privacy protection

RIMAC

Privacy Policy: Scope and Management

We manage personal data through a defined privacy and information protection framework.

At RIMAC, we take the protection and privacy of personal data seriously. Our Privacy Policy establishes how we handle personal data in accordance with Peru's Personal Data Protection Act and its applicable regulations.

Scope across RIMAC

Our Privacy Policy covers RIMAC Seguros y Reaseguros and RIMAC S.A. Entidad Prestadora de Salud (EPS), and governs the handling of personal data within our business relationships.

Personal data as confidential information

We classify personal data as confidential information and require security measures in the information systems and platforms that contain or support such data.

Lifecycle and data subject rights

We define retention periods and provide mechanisms for individuals to exercise access, information, updating, correction, cancellation, portability and suppression rights, as well as to challenge use or disclosure or withdraw consent.

Third-party protection

Our information classification policy applies to employees and third parties providing services to us. Third parties with access to company information are subject to confidentiality, personal data protection and contractual security requirements.

To view the full policy, click here.

Privacy Governance and Responsibilities

We assign defined accountability for personal data protection, information security and information governance.

Personal Data Protection Officer

We have designated Karen Mora Gutiérrez as our Personal Data Protection Officer, providing a specific point of accountability and contact for personal data protection matters.

pdpcumplimiento@rimac.com.pe

Information Security

We advise on information classification and security controls, monitor their effectiveness through metrics, coordinate improvements and verify regulatory changes.

Data Governance & Owners

We identify Data Owners, who define access levels and ensure information is appropriately classified and safeguarded.

Risk-based governance

Senior Management provides resources for the Information Security Management System, while the Risk Committee (GIR) approves policies, procedures, guidelines and directives related to information classification.

Approval and oversight

The policy approval and publication flow involves Information Security, Operational Risk Management, the Integral Risk Management Committee and the Board of Directors.

Monitoring, review and audit

We periodically assess the effectiveness of our security controls, review our policy at least annually, and may conduct special audits of electronic information and information assets, within an information security framework aligned with ISO 27001 and NIST (National Institute of Standards and Technology) (Annual Report 2025, page 71)


RIMAC