Política de Seguridad de la Información

I. OBJETIVO

- Establecer un marco de gobierno, operación y control para la protección de los activos y recursos tecnológicos que los soportan. Con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información.

- Establecer una cultura de gestión de Seguridad de la Información y Ciberseguridad en los procesos organizacionales con el respaldo de la alta dirección.

- Gestionar los riesgos de Seguridad de la Información y Ciberseguridad para minimizar su impacto de materialización, garantizando la confidencialidad, integridad y disponibilidad de la información de acuerdo con los objetivos estratégicos del negocio.

- Cumplir con los requisitos legales, regulatorios y de terceros que afecten a la organización en lo relacionado a Seguridad de la Información y Ciberseguridad.

II. ALCANCE

La presente política debe ser cumplida por todos los colaboradores de Rimac Seguros, Rimac EPS y terceros que intercambien en medio físico o digital los activos de información de la compañía.

La protección de los activos de información tiene aplicabilidad para todos los entornos donde la información es procesada, transmitida y almacenada. Esto incluye y no se limita a entornos de nube u on premise, teniendo como prioridad la protección de la infraestructura crítica de la organización

III. OTRAS REFERENCIAS

- Ley N° 29733 – Ley de Protección de Datos Personales
- Resolución SBS 504
- PCI DSS
- ISO 27001
- NIST V1.

IV. DESARROLLO DE LA POLÍTICA

1. Gestión de Riesgos Tecnológicos y de Información

Contamos con un proceso formal de identificación, análisis, evaluación y tratamiento de riesgos relacionados con la información. Los riesgos se analizan considerando criterios como impacto y probabilidad, lo que permite tomar decisiones con base en datos y priorizar los recursos de mitigación.

La documentación generada alimenta nuestros planes de continuidad, controles operativos y protocolos de respuesta ante incidentes, y es supervisada por las áreas responsables de

seguridad y auditoría interna.

2. Gestión de Riesgos en Proveedores

Conscientes de que la cadena de suministro representa un punto crítico en la seguridad, aplicamos controles específicos sobre terceros que acceden o gestionan información relevante para la organización.

Entre las medidas adoptadas se encuentran:

- Evaluaciones de riesgo antes de contratar a proveedores.
- Inclusión de cláusulas de confidencialidad, privacidad y seguridad en contratos.
- Revisión de controles aplicados por el proveedor, especialmente cuando se trata de servicios tecnológicos, cloud o procesamiento de datos personales.
- Monitoreo continuo y revisiones periódicas para proveedores clasificados como críticos.

Estas prácticas nos permiten asegurar que nuestros aliados cumplan con estándares equivalentes a los nuestros en términos de protección de la información.

3. Seguridad en los Procesos Organizacionales

La seguridad está integrada en los procesos operativos clave. Cada área de negocio cuenta con lineamientos y procedimientos que incluyen:

- Control de acceso basado en roles y principios de menor privilegio.
- Separación de ambientes y funciones (desarrollo, prueba y producción).
- Aprobación y validación de cambios tecnológicos a través de procedimientos formales.
- Registro y trazabilidad de acciones relevantes dentro de los sistemas.

Además, se aplican controles técnicos de monitoreo, registro de eventos y revisión de logs, permitiendo una visibilidad continua sobre la actividad operativa, detección de comportamientos anómalos y cumplimiento normativo.

4. Seguridad en Proyectos y Desarrollos Tecnológicos

Todos los nuevos desarrollos, integraciones o implementaciones de sistemas deben cumplir con los principios de seguridad desde el diseño, asegurando que la protección de la información esté incorporada desde las fases iniciales del proyecto. Nuestro enfoque se basa en la aplicación de buenas prácticas de desarrollo seguro a lo largo de todo el ciclo de vida, lo que incluye:

- Revisión de arquitectura y diseño técnico por parte del equipo de seguridad para garantizar que las soluciones cumplan con los estándares corporativos y regulatorios.
- Pruebas de vulnerabilidades y validaciones de seguridad, que incluyen análisis automatizados, revisiones manuales y pruebas de ethical hacking realizadas por especialistas internos o externos. Estas pruebas simulan escenarios de ataque controlados para identificar y corregir vulnerabilidades antes de la puesta en producción.
- Documentación formal de riesgos, dependencias y controles aplicados, asegurando trazabilidad y cumplimiento normativo.
- Formamos parte del flujo de control de cambios, lo que nos permite validar que cumplan con lo anteriormente mencionado.

Este enfoque integral nos permite reducir riesgos de seguridad, prevenir brechas y garantizar que las soluciones tecnológicas sean confiables y resilientes, contribuyendo a la continuidad del negocio y la protección de los datos.

5. Gestión del Riesgo Humano

Reconocemos que las personas pueden ser tanto la primera línea de defensa como un punto de vulnerabilidad. Por ello, trabajamos constantemente en la formación, concientización y gestión del comportamiento humano en seguridad.

Nuestras iniciativas incluyen:

- Capacitaciones obligatorias en temas de seguridad y privacidad para todos los colaboradores.
- Capacitaciones temáticas durante el año, enfocadas en riesgos actuales como phishing, inteligencia artificial y protección de dispositivos.
- Simulaciones de ataques de ingeniería social para medir la efectividad de las capacitaciones.
- Procedimientos de sanción en caso de incumplimientos de nuestra política de seguridad de la información.

Estas acciones no solo buscan cumplir con normativas, sino fortalecer la cultura de seguridad en toda la organización, promoviendo comportamientos responsables y proactivos frente a las amenazas. Creemos que la conciencia y el compromiso de cada colaborador son factores clave para reducir riesgos, proteger la información y garantizar la continuidad del negocio.

6. Protección de Infraestructura y Sistemas Críticos

Nuestra infraestructura tecnológica está protegida mediante un enfoque integral de seguridad, que combina controles físicos, lógicos y procesos de monitoreo continuo para garantizar la disponibilidad, integridad y confidencialidad de la información.

Entre las principales medidas implementadas se incluyen:

- Segmentación de redes y monitoreo perimetral, para reducir riesgos y controlar el tráfico entre entornos críticos.
- Controles avanzados de detección y prevención de amenazas, que permiten identificar y responder oportunamente a incidentes.
- Protección de aplicaciones y datos, mediante mecanismos que previenen accesos no autorizados y fugas de información.
- Autenticación reforzada y gestión segura de accesos, asegurando que solo usuarios y dispositivos autorizados interactúen con los sistemas.
- Monitoreo centralizado y análisis de eventos, para anticipar riesgos y actuar de manera proactiva.
- Planes de continuidad y recuperación ante desastres, probados periódicamente para garantizar la resiliencia operativa.

Adicionalmente, contamos con un Plan de Respuesta ante Incidentes, que establece procedimientos claros para la detección, contención, erradicación y recuperación frente a eventos de seguridad. Este plan incluye la notificación oportuna a las áreas responsables, la coordinación con equipos especializados y la ejecución de acciones correctivas y preventivas, asegurando que cada incidente sea gestionado de manera eficiente y que se incorporen aprendizajes para fortalecer la postura de seguridad.

Este conjunto de medidas nos permite mantener la operación segura y confiable, incluso frente a escenarios adversos, alineándonos con estándares internacionales y regulaciones locales.

7. Controles de Acceso

Gestionamos los accesos a la información y a los sistemas críticos bajo el principio de mínimo privilegio, asegurando que cada usuario cuente únicamente con los permisos necesarios para desempeñar sus funciones.

Entre las principales prácticas implementadas se incluyen:

- Autenticación reforzada, que incorpora mecanismos adicionales para validar la identidad de los usuarios en accesos sensibles.
- Gestión centralizada de identidades y roles, para garantizar la asignación y revocación oportuna de permisos.
- Monitoreo y trazabilidad de accesos, lo que permite detectar comportamientos inusuales y responder de manera proactiva.

Este enfoque integral nos permite proteger la confidencialidad y la integridad de la información, reduciendo el riesgo de accesos no autorizados y fortaleciendo la seguridad en toda la organización.

V. RESPONSABLES DEL FLUJO DE APROBACIÓN

Nuestra política de Seguridad de la Información fue aprobada en el año 2024 bajo el siguiente proceso:

Etapa	Área	Cargo	Nombre
Dueño	SEGURIDAD DE LA INFORMACION	GERENTE SEGURIDAD DE LA INFORMACION	Karla Mariella Parra Bocanegra
Editor	RIESGOS SEGURIDAD DE LA INFORMACION	RISK ENGINEER PROFESSIONAL	Edu Denilson Acosta Bejarano
Revisor	RIESGOS SEGURIDAD DE LA INFORMACION	RISK ENGINEER PROFESSIONAL	Edu Denilson Acosta Bejarano
Revisor	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo
Aprobador	SEGURIDAD DE LA INFORMACION	GERENTE SEGURIDAD DE LA INFORMACION	Karla Mariella Parra Bocanegra
Aprobador	DIVISION TI Y DATA	VICEPRESIDENTE EJECUTIVO	CARLOS ALBERTO HERRERA
Aprobador	BUSINESS PROCESS ENGINEERING	BUSINESS PROCESS ENGINEER SPECIALIST	Leslie Valverde Montalvo
Aprobador	RIESGOS OPERACIONALES Y CONTINUIDAD	GERENTE RIESGO OPERACIONAL Y CONTINUIDAD	Renato Bedoya Chirinos