## 1. OBJETIVO

### Objetivo general

- 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.

### Objetivos específicos

- 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.

## 2. 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.

## 3. DEFINICIONES

- **Seguridad de la información:** Es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas, con el objetivo de minimizar el daño, garantizar la continuidad operacional y maximizar el retorno sobre las inversiones y las oportunidades de los negocios de la compañía.
- **Ciberseguridad:** Es la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados
- **Sistema de Gestión de Seguridad de la Información:** Sistema orientado implementar, operar, monitorear, revisar, mantener y mejorar la Seguridad de la Información de la compañía a fin de conseguir sus objetivos. Se basa en la evaluación del riesgo y de los niveles de aceptación del riesgo establecidos para tratar y gestionar los riesgos de manera eficaz.
- **Comité de Seguridad de la Información:** Es el máximo órgano al que compete la Seguridad de la Información en la organización. En este sentido, identifica objetivos y estrategias relacionados con la seguridad de la información y dirige y controla los procesos relacionados con la seguridad.

- **Activo de información:** Componente tecnológico, documentos, aplicaciones, personas y conocimiento o datos que tienen valor para la compañía, por lo tanto deben ser protegidos.

- **Tecnología de la Información**: Hardware y software operados por la organización o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- **Confidencialidad:** Característica de la información que permita que sea accesible sólo a aquellas personas autorizadas.

- **Disponibilidad:** Característica de la información que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

- **Integridad:** Características de la información que permite salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

- **Servicios en la nube:** La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

## 4. AREAS / CARGO/ ROLES Y RESPONSABILIDADES

- **ALTA DIRECCIÓN:**
  - Brindar los recursos necesarios y cooperar con el cumplimiento del sistema de gestión de seguridad de la información. Con la finalidad de implementar controles que apoyen a los requerimientos del negocio.

- **COLABORADORES Y TERCEROS:**
  - Aceptar, adoptar y cumplir la presente política y los procedimientos que de esta deriven adoptándolas dentro de las actividades relacionadas con su trabajo.

- **VICEPRESIDENTES EJECUTIVOS / VICEPRESIDENCIAS:**
  - Apoyar con la difusión de la presente política y garantizar que todo el personal a su cargo cumpla la presente política y los documentos que de esta deriven adoptándolas dentro de sus actividades laborales.
  - Asignar la responsabilidad de la seguridad de la información formalmente a un director de seguridad de la información o a otro miembro de la dirección ejecutiva con conocimientos de seguridad de la información.

- **Seguridad de la Información:**
  - Revisar la presente política por lo menos 1 vez al año de acuerdo a los objetivos estratégicos del negocio, legislación y actualizarla en base a la normativa vigente, o cuando ocurran cambios significativos en los procesos internos o en la normativa externa.
  - Gestionar la implementación de los controles de seguridad aprobados en coordinación con las áreas de negocio y tecnología de información.

- Revisar periódicamente la efectividad de los controles de seguridad adoptados en la presente política mediante métricas y coordinar acciones de mejora en caso de desviaciones.

- Difundir la presente política a todo el personal de la organización independiente del cargo que desempeñe y de su situación contractual.

## 5. DESARROLLO DE LA POLÍTICA

### Generalidades

- La política debe ser revisada por lo menos 1 vez al año y actualizada cuando ocurran cambios significativos en los procesos internos o en la normativa externa. Cada actualización del documento deberá ser acompañado de la respectiva notificación y capacitación a los obligados de cumplirla y de conocerla.

- Las infracciones sobre la presente política o documentos asociados serán considerados como un incidente de seguridad de la información por incumplimiento y será sancionado de acuerdo a lo especificado en la política de sanciones por incumplimiento de las políticas de seguridad de la información. Además, de las reglas, políticas y/o normas de RIMAC.

### Política de seguridad de la información y ciberseguridad

1. RIMAC ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C), soportado con lineamientos claros acorde a las necesidades del negocio y requerimientos regulatorios.

2. Todos los colaboradores y terceros; independientemente de su cargo; son responsables por la custodia y protección de los activos y tecnologías de información (on premise, nube, físicos y digitales) que manejan en el desempeño de sus funciones. Por lo tanto, se debe desarrollar y promover una cultura organizacional orientada al cuidado de la información en todos sus niveles. Además, son responsables de informar cualquier incumplimiento de esta política o las que deriven.

3. Todos los colaboradores y terceros que utilizan los activos tecnológicos e información de RIMAC deben ser conscientes que pueden ser sancionados por el incumplimiento de la presente política. La sanción será determinada teniendo en cuenta la naturaleza, gravedad, incumplimientos anteriores, legislación aplicable y toda otra información pertinente. La sanción será tomada de acuerdo con las reglas, políticas y/o normas de RIMAC.

4. Se deben implementar mecanismos de control para la protección de la información contenida en los activos físicos y lógicos que se puedan almacenar on premise o nube. Considerando el cumplimiento con la Ley de Protección de Datos Personales y otras que apliquen a la organización.

5. Los riesgos de Seguridad de la Información serán gestionados adoptando medidas y/o planes para su debida atención cuando estos se encuentren dentro de los niveles de riesgo no aceptables.

6. Las responsabilidades frente a la Seguridad de la Información serán definidas, compartidas, publicadas y aceptadas por los empleados, proveedores, socios de negocio y terceros.

7. Se establece una coordinación integrada mediante un proceso de gestión de eventos y/o incidentes fortaleciendo las capacidades de respuesta oportuna y eficaz frente a amenazas y/o incidentes con la finalidad de asegurar la disponibilidad y continuidad de la operación.

8. Se establecen condiciones, procedimientos y plazos para la recuperación o eliminación de activos de información ubicados o almacenados en la nube u on premise al finalizar un servicio con un tercero.

9. Se implementa controles de acceso a la información, sistemas y recursos de red.

10. Se deben implementar los requisitos de Seguridad de la Información dentro del ciclo de vida de desarrollo y adquisición de sistemas de información.

11. Se controla la operación y las comunicaciones de los procesos de negocio garantizando la confidencialidad, integridad y disponibilidad de los recursos tecnológicos y las redes de datos.

12. Se protege los activos y tecnologías de información de la compañía frente a las amenazas, internas o externas, deliberadas o accidentales.

13. Se monitorea y trabaja en el cumplimiento de los requisitos legales, regulatorios y contractuales que afectan a la compañía en lo relacionado a la Seguridad de la Información.

14. Se incluye la evaluación de aspectos de Seguridad de la Información y gestión de riesgos en los proyectos bajo lineamientos establecidos.

15. Se deben implementar medidas de protección sobre los activos de información en base a lo establecido en la política de clasificación, uso y tratamiento de información.

16. Se deben de implementar mecanismos de control para la gestión de proveedores durante la prestación del servicio, garantizando que se cuenten con términos de seguridad de la información y una adecuada gestión de accesos.

17. Toda desviación de cumplimiento a esta política o los documentos que deriven de esta, serán evaluadas para la identificación de riesgos e informadas a la Vicepresidencia responsable para su atención en plazos prudentes.

18. El sistema de gestión de seguridad de la información de RIMAC, sus políticas y procedimientos asociados se basan en las mejores prácticas y lineamientos establecidos por marcos de trabajo internacionales tales como ISO/IEC 27000, NIST, entre otros.

Algunos puntos descritos en la política se relacionan con políticas que proporcionan principios y guía en aspectos específicos de Seguridad de la Información y Ciberseguridad.

| Punto | Descripción |
|---|---|
| 4 | Política de protección de datos personales |
| 7 | Política de Gestión de Incidentes de Seguridad de la información. |

| | |
|---|---|
| 6 | Política de Seguridad en Recursos Humanos. |
| 1,13 | Política de Cumplimiento. |
| 9 | Política de Gestión de Accesos. |
| 2,3,8,12 | Política de Gestión de Activos Tecnológicos |
| 11,8 | Política de Gestión de aspectos de Seguridad de la Información para dar continuidad del negocio |
| 11 | Política de Seguridad en Infraestructura y Operaciones de TI. |
| 10 | Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento |
| 5,14 | Manual de Gestión de Riesgos de Seguridad de la Información. |
| 3 | Política de sanciones por incumplimiento de la política de seguridad. |
| 15 | Política de Clasificación, Uso y tratamiento de Información |
| 2 | Política de uso Aceptable de Información, Equipos y Servicios Informáticos |
| 16 | Política de Seguridad de la Información para proveedores |

## 6. DOCUMENTOS RELACIONADOS

| Código | Nombre |
|---|---|
| MAN-4699 | Manual de Gestión de Riesgos de Seguridad de la Información_actual |
| POL-6011 | Política de Clasificación, Uso y Tratamiento de la Información |
| POL-4322 | Política de Gestión de Activos Tecnológicos |
| POL-5009 | Política de Gestión de Cumplimiento en Seguridad de la Información |
| POL-6005 | Política de Gestión de Incidentes de Seguridad de la Información |

| | |
|---|---|
| POL-6006 | Política de Gestión de Seguridad de la Información para dar Continuidad al Negocio |
| POL-5008 | Política de Gestión de Seguridad de los Recursos Humanos |
| POL-5007 | Política de Seguridad de la Información para Proveedores |
| POL-6015 | Política de Seguridad en Infraestructura, Operaciones y Comunicaciones de TI |
| POL-6014 | Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento |
| POL-6013 | Política de Uso Aceptable de Información, Equipos y Servicios Informáticos |
| PRO-4519 | Continuidad operativa del monitoreo de base de datos |
| No Aplica | Gestión de monitoreo de líneas base |
| PRO-6334 | Modelo operativo de monitoreo de seguridad en base de datos |
| PRO-4539 | Procedimiento de reporte de operaciones |

## 7. ANEXOS

Control de Cambios anterior

| CREACIÓN DEL DOCUMENTO |
|---|

| FECHA DE ELABORACIÓN | DESCRIPCIÓN | V | ELABORADOR |
|---|---|---|---|
| 03/05/2019 | Documento Inicial | 01 | Richard Saldaña |

**REGISTRO DE ACTUALIZACIÓN DEL DOCUMENTO**

| REEMPLAZA DOCUMENTO PUBLICADO | | DESCRIPCIÓN DE LA ACTUALIZACIÓN | V | ELABORADOR / ACTUALIZADOR |
|---|---|---|---|---|
| **FECHA PUBLICACIÓN** | **CÓDIGO** | · Se realizó la actualización de las responsabilidades<br>· Se añadieron los puntos 15, 16 y 17.<br>· Actualización de la sección responsables del flujo de aprobación. | 02 | Diego Cárdenas |
| 03/05/2019 | POL-3679 | | | |
| **FECHA PUBLICACIÓN** | **CÓDIGO** | · Se realizó la actualización del punto 4.<br>· Se añadió el puntos 17. | 03 | Diego Cárdenas |
| 17/01/2021 | POL-4155 | | | |
| **FECHA PUBLICACIÓN** | **CÓDIGO** | · Se incluyó aspectos de ciberseguridad de acuerdo a lo establecido por la resolución SBS-504. | 04 | Diego Cárdenas |
| 09/04/2021 | POL-4320 | | | |
| **FECHA PUBLICACIÓN** | **CÓDIGO** | · Actualización de la sección responsabilidades, generalidades, punto 13 y responsables del flujo de aprobación. | 05 | Diego Cárdenas |
| 02/04/2021 | POL-4383 | | | |

## 8. RESPONSABLES DEL FLUJO DE APROBACIÓN

| Etapa | Area | 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 |

## 9. CONTROL DE CAMBIOS

| Fecha | Versión | Cambios Efectuados |
|---|---|---|
| 23/11/2023 | 06 | Se realizó la rectificación del documento |
| 24/12/2024 | 07 | Se detalla y agrega punto correspondiente; para la certificación PCI 2024. Punto detalla que el Vicepresidente ejecutivo a cargo de la responsabilidad de Seguridad de la Información, debe tener conocimientos sobre ello. |