POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACÍÓN

Documento N°: RSM-ISMS-P-A-CHI-00-SIF
Versión V1.1

Información del Documento

Título:	Política General de Seguridad de la Información
Versión:	1.1
Fecha:	20-02-2025
Documento N°:	RSM-ISMS-P-A-CHI-00-SIF
Clasificación:	Publico
Elaborado por:	Franco Godoy
Propietario del documento:	CISO

Historial de revisión:

N° de serie	Fecha	N° de versión	Actualizado por	Revisado por	Aprobado por
1	31-10-2024	V1.0	Franco Godoy	CISO	Comité de Seguridad de la Información, Ciberseguridad y Tecnología
2	20-02-2025	V1.1	Franco Godoy	CISO	Comité de Seguridad de la Información, Ciberseguridad y Tecnología

CONTENIDO

1. INTRODUCCIÓN

En RSM Chile, la seguridad de la información constituye un compromiso estratégico que respalda la misión organizacional y garantiza la continuidad de las operaciones en todas las entidades del grupo. Nuestro Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para proteger la confidencialidad, integridad y disponibilidad de los activos de información, proporcionando un marco integral de políticas, procedimientos y controles alineados con los estándares internacionales y las mejores prácticas.

Esta política, como pilar fundamental del SGSI, define los principios rectores para gestionar de manera efectiva los riesgos asociados a la seguridad de la información. Asimismo, promueve un enfoque consistente que permite a todas las filiales y áreas operativas de RSM Chile afrontar desafíos emergentes y adaptarse a un entorno dinámico de riesgos y oportunidades.

En un contexto de amenazas en constante evolución, RSM Chile reafirma su compromiso con la mejora continua del SGSI, integrando prácticas proactivas y resilientes para mitigar riesgos y garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables. Este enfoque holístico asegura que las necesidades de todas las partes interesadas, internas y externas se gestionen de manera eficaz y contribuyan al logro de los objetivos organizacionales.

2. OBJETIVO

La Política General de Seguridad de la Información tiene como objetivo principal establecer las directrices que permiten gestionar los riesgos asociados a los activos de información. A través de esta política, RSM Chile busca:

- Proteger la información en todas sus formas y fases, garantizando su confidencialidad, integridad y disponibilidad.
- Gestionar los riesgos asociados a la información mediante controles efectivos y evaluaciones periódicas.
- Asegurar la continuidad operativa, reduciendo el impacto de incidentes de seguridad.
- Cumplir con las normativas legales, regulatorias y contractuales aplicables.
- Promover una cultura de seguridad entre todos los colaboradores y partes interesadas.
- Fomentar la mejora continua, alineando las prácticas de seguridad con los cambios en el entorno.

Esta política define un enfoque integral que garantiza la implementación de medidas consistentes de seguridad en toda la organización, alineándose con los objetivos estratégicos de RSM Chile.

3. ALCANCE

Esta política aplica a todas las entidades del grupo RSM Chile y a sus colaboradores, prestadores de servicios y proveedores. Su alcance abarca toda la información gestionada por RSM Chile, independientemente de su formato, medio de almacenamiento, ubicación o quién la procese, ya sea en formato impreso o digital.

Adicionalmente, esta política incluye:

- **Información generada, procesada o almacenada por terceros externos y entidades asociadas:** Garantizando que los socios y proveedores cumplan con los principios y controles establecidos.
- **Infraestructuras tecnológicas y físicas:** Incluyendo sistemas de información, redes, dispositivos y cualquier medio relacionado con la gestión de datos.
- **Procesos de negocio:** Asegurando que todos los procesos internos y externos se alineen con los estándares de seguridad de la información.

Esta política debe ser conocida, comprendida y cumplida por todos los colaboradores y partes interesadas. Para garantizar su disponibilidad, estará publicada en la intranet corporativa y en un repositorio común accesible a todos los involucrados. Además, se fomentará su difusión mediante programas de sensibilización y formación periódicos. Esta política aplica a:

- Todas las empresas del grupo RSM Chile.
- Todos los colaboradores, prestadores de servicios, proveedores y terceros que gestionen o accedan a información de RSM Chile.
- Todos los procesos, sistemas, servicios y activos de información, independientemente de su formato (físico o digital) o ubicación.

Incluye la información generada, procesada, almacenada y transmitida dentro y fuera de la organización, garantizando que todos los involucrados cumplan con los principios y controles establecidos en esta política.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de RSM Chile reafirma su compromiso con la seguridad de la información como un elemento estratégico esencial para garantizar la continuidad de las operaciones y la protección de los activos de información. Este compromiso se manifiesta en los siguientes puntos clave:

- **Liderazgo estratégico:** La Alta Dirección asume la responsabilidad de integrar la seguridad de la información en los objetivos organizacionales, promoviendo una cultura de protección y responsabilidad en todos los niveles de la organización.
- **Asignación de recursos:** Se asegurarán los recursos necesarios, tanto humanos como tecnológicos y financieros, para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y eficaz.
- **Cumplimiento normativo:** La Alta Dirección garantiza que todas las actividades de RSM Chile cumplen con las leyes, regulaciones y requisitos contractuales aplicables, monitoreando constantemente su cumplimiento.
- **Revisión periódica:** El SGSI será revisado de forma regular para asegurar que los controles implementados sean efectivos y adecuados frente a los riesgos identificados y los cambios internos o externos.
- **Promoción de la cultura de seguridad:** La Alta Dirección liderará iniciativas de formación y sensibilización para todos los empleados y partes interesadas, fomentando un entorno donde la seguridad de la información sea prioridad.
- **Mejora continua:** Se impulsará la innovación y la adopción de mejores prácticas para fortalecer la resiliencia frente a amenazas emergentes y garantizar la protección de la información.

Estos compromisos demuestran el liderazgo y responsabilidad de la Alta Dirección en la protección de los activos de información, alineando las operaciones con estándares internacionales, mejores prácticas y la misión de RSM Chile.

5. ROLES Y RESPONSABILIDADES

5.1 ALTA DIRECCIÓN

La Alta Dirección desempeña un rol estratégico en la seguridad de la información, asegurando que esté alineada con los objetivos generales de la organización. Entre sus principales responsabilidades están:

- **Liderazgo visible:** Demostrar compromiso con la seguridad mediante la participación activa en revisiones del SGSI, aprobación de políticas y toma de decisiones clave.
- **Asignación de recursos:** Garantizar la disponibilidad de recursos necesarios, incluyendo tecnología, personal capacitado y presupuesto adecuado.
- **Supervisión y monitoreo:** Revisar periódicamente los informes de auditorías y las revisiones del SGSI para evaluar su efectividad y adecuación a los cambios organizacionales o del entorno.
- **Promoción de la cultura de seguridad:** Impulsar la concienciación y la capacitación en seguridad de la información en toda la organización.

5.2 CHIEF INFORMATION SECURITY OFFICER (CISO)

El CISO es responsable de liderar y gestionar el SGSI, asegurando su implementación efectiva en toda la organización. Sus responsabilidades incluyen:

- **Diseño e implementación del SGSI:** Establecer y mantener el marco de gestión de la seguridad de la información, alineado con las mejores prácticas y normativas aplicables.
- **Evaluación de riesgos:** Identificar, analizar y gestionar los riesgos relacionados con la información, implementando controles adecuados para mitigar los riesgos identificados.
- **Supervisión de controles de seguridad:** Garantizar que los controles implementados sean efectivos y proporcionales a los riesgos.
- **Coordinación de auditorías:** Planificar y supervisar las auditorías internas y externas, asegurando que los hallazgos sean abordados oportunamente.
- **Capacitación y sensibilización:** Promover programas de formación en seguridad para todos los empleados y contratistas.
- **Gestíon de incidentes:** Supervisar la gestión de incidentes de seguridad, asegurando respuestas rápidas y efectivas.

5.3 GERENTES DE ÁREA

Los gerentes de área son responsables de implementar y supervisar las políticas y controles de seguridad dentro de sus respectivas áreas. Entre sus funciones están:

- **Cumplimiento de políticas:** Asegurar que todos los procesos bajo su gestión cumplan con las políticas de seguridad establecidas.
- **Supervisión de equipos:** Monitorear que los miembros de su equipo apliquen las medidas de seguridad requeridas.
- **Gestión de riesgos:** Identificar riesgos específicos de su área y trabajar con el CISO para implementar controles adecuados.
- **Reportes de incidentes:** Escalar incidentes de seguridad detectados en su área de manera oportuna.

5.4 COLABORADORES Y PRESTADORES DE SERVICIOS

Todos los colaboradores y prestadores de servicio tienen la responsabilidad de actuar de manera conforme a las políticas de seguridad de la organización. Sus responsabilidades incluyen:

- **Cumplimiento de políticas:** Seguir todas las normativas y procedimientos relacionados con la seguridad de la información.
- **Reporte de incidentes:** Informar cualquier evento que comprometa la seguridad de la información, utilizando los canales establecidos.
- **Participación en formación:** Asistir a las capacitaciones y actividades de concienciación organizadas por la organización.
- **Protección de la información:** Manejar la información de forma responsable, asegurando su confidencialidad y evitando accesos no autorizados.

6. GESTIÓN DE RIESGOS

La gestión de riesgos es un pilar fundamental para garantizar la seguridad de la información y proteger los activos de RSM Chile frente a amenazas y vulnerabilidades. A través de un enfoque estructurado y continuo, se busca identificar, analizar y mitigar los riesgos, asegurando que las operaciones de la organización se mantengan resilientes y alineadas con los objetivos de seguridad establecidos.

La gestión de riesgos es fundamental para la seguridad de la información. RSM Chile se compromete a:

- **Identificar riesgos:** Realizar evaluaciones periódicas para identificar amenazas, vulnerabilidades y riesgos asociados a los activos de información.
- **Evaluar el impacto:** Priorizar los riesgos en función de su probabilidad y gravedad.
- **Mitigar riesgos:** Implementar controles adecuados para reducir la exposición a los riesgos.
- **Monitorear y revisar:** Evaluar la efectividad de los controles mediante auditorías regulares.

7. GESTIÓN DE LA SEGURIDAD DE LOS RECURSOS HUMANOS

El Departamento de Recursos Humanos de RSM Chile deberá gestionar los aspectos de seguridad de la información en todas las fases del ciclo de vida de los colaboradores, desde la contratación hasta la desvinculación. Esto incluye:

- **Formación y Concienciación: RSM Chile** garantizará que todos los colaboradores reciban la formación y concienciación adecuadas en materia de seguridad de la información, de acuerdo con las normativas vigentes, poniendo especial énfasis en la confidencialidad y la prevención de fugas de información. Los colaboradores también serán informados sobre cualquier actualización de las políticas y procedimientos de seguridad.
- **Política de Escritorio Limpio:** Los colaboradores deberán asegurar que sus áreas de trabajo están libres de documentos o dispositivos que contengan información sensible al finalizar la jornada laboral. Los dispositivos deberán bloquearse al dejar el puesto de trabajo, tanto manualmente como de forma automatizada.

8. GESTIÓN DE ACTIVOS

RSM Chile deberá identificar e inventariar todos los activos de información necesarios para la operación de los procesos de negocio. El inventario de activos se mantendrá actualizado de manera continua.

- **Clasificación de Activos:** Los activos serán clasificados de acuerdo con el tipo de información que contienen, según lo dispuesto en la sección de clasificación de la información.
- **Responsabilidad de Activos:** Cada activo o elemento de información deberá tener un responsable que garantice su correcta clasificación, protección e inventariado. Este responsable deberá mantener un registro formal de los usuarios autorizados a acceder al activo.
- **Gestión de Dispositivos BYOD:** RSM Chile permite el uso de dispositivos personales (BYOD) para acceder a recursos corporativos, siempre que estos dispositivos cumplan con las mismas medidas y configuraciones de seguridad que los dispositivos corporativos. Los usuarios de dispositivos BYOD serán responsables de su seguridad y deberán mantenerlos actualizados con el software de gestión de dispositivos móviles (MDM) proporcionado por el departamento de TI.

9. GESTIÓN DEL CICLO DE VIDA DE LA INFORMACIÓN

RSM Chile gestionará adecuadamente el ciclo de vida de la información para evitar su uso incorrecto en cualquiera de las fases:

1. **Creación o Recolección:** Registra y almacena información desde su origen, ya sea creada internamente o recibida de fuentes externas.
2. **Distribución:** Gestiona la información creada o recibida, tanto internamente como externamente.
3. **Uso o Acceso:** Regula el acceso autorizado a la información, asegurando que solo personas autorizadas puedan acceder a ella.
4. **Almacenamiento:** Organiza y gestiona la información para garantizar su accesibilidad y seguridad.
5. **Destrucción:** Implementa prácticas para eliminar la información que ha cumplido su período de retención, garantizando su confidencialidad durante el proceso de destrucción.

RSM Chile deberá identificar y aplicar las medidas de seguridad necesarias para asegurar la correcta gestión del ciclo de vida de los activos de información.

10. GESTIÓN DE COPIAS DE SEGURIDAD

RSM Chile deberá realizar copias de seguridad periódicas de la información, el software y los sistemas, verificándolas regularmente:

- Las copias de seguridad deberán realizarse al menos semanalmente, y con mayor frecuencia si la información es de alta criticidad.
- Las copias de seguridad deben recibir las mismas protecciones que los datos originales y, siempre que sea posible, deberán estar cifradas.
- Se realizarán pruebas periódicas de restauración de copias de seguridad para asegurar su funcionamiento adecuado. Estas pruebas serán documentadas.

Las copias de seguridad deberán almacenarse en ubicaciones seguras y preferiblemente en centros diferentes a donde se generaron, garantizando la integridad de la información ante posibles incidentes de seguridad, como ataques de ransomware.

11. CLASIFICACIÓN DE LA INFORMACIÓN

RSM Chile establecerá un modelo de clasificación de la información que defina las medidas técnicas y organizativas necesarias para proteger la información en función de su sensibilidad:

- **Tipos de Información:** La información se clasificará en soportes lógicos (digitales) y físicos (documentos impresos y otros medios de almacenamiento).
- **Niveles de Clasificación:** La información se categorizará en niveles como Uso Público, Interno y Confidencial.

12. CONTROL DE ACCESO

RSM Chile implementará controles de acceso que aseguren que solo usuarios autorizados puedan acceder a la información y sistemas:

- **Requisitos de Negocio:** Los usuarios serán únicos, sin posibilidad de compartir cuentas, y deberán utilizar autenticación de doble factor (MFA) cuando sea posible.
- **Derechos de Acceso:** Los permisos se basarán en la necesidad de saber y el principio de privilegios mínimos, asegurando una adecuada segregación de funciones.

13. SEGURIDAD FÍSICA Y DEL ENTORNO

Las instalaciones de RSM Chile donde se ubiquen los sistemas de información deberán estar protegidas mediante controles de acceso físico, sistemas de vigilancia y medidas preventivas para mitigar riesgos como accesos no autorizados, robos, sabotajes y desastres ambientales.

14. SEGURIDAD EN EL TRABAJO EN LA NUBE

RSM Chile reconoce la importancia de garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y procesada en la nube. Para ello, se han establecido las siguientes acciones para abordar la seguridad en la nube:

- **Infraestructura:** Asegurar que el proveedor de servicios en la nube monitoriza el entorno y establece controles de acceso robustos.
- **Plataforma y Software:** Seguir las mejores prácticas de seguridad, incluyendo las guías de OWASP y/o SANS25 para la seguridad de aplicaciones.

15. SEGURIDAD EN LA OPERATIVA

Todos los sistemas de información de RSM Chile deberán contar con medidas de seguridad adecuadas que optimicen su nivel de madurez. Las redes se gestionarán y monitorearán adecuadamente para proteger los sistemas y aplicaciones de amenazas.

16. SEGURIDAD EN LAS TELECOMUNICACIONES

RSM Chile asegurará que su arquitectura de red cuenta con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se implementarán controles adicionales para los datos sensibles que circulen por redes públicas.

17. SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

RSM Chile garantizará que todos los procesos de adquisición, desarrollo y mantenimiento de sistemas incorporen requisitos mínimos de seguridad. Se gestionarán las pruebas, los cambios y el inventario de software conforme a las mejores prácticas del sector.

18. SEGURIDAD EN LOS PROVEEDORES

Se evaluará la criticidad de los servicios subcontratados para asegurar que los proveedores cumplen con los requisitos de seguridad establecidos por RSM Chile. Los procesos de selección, los acuerdos contractuales y la monitorización de los servicios deberán garantizar la seguridad de la información subcontratada.

19. GESTIÓN DE INCIDENTES

Todos los colaboradores de RSM Chile son responsables de identificar y notificar cualquier incidente que pueda comprometer la seguridad de la información. RSM Chile implementará procedimientos de gestión de incidentes que incluyan la categorización, análisis de impacto y escalado de incidentes.

20. CONTINUIDAD DE NEGOCIO

RSM Chile dispondrá de un Plan de Continuidad de Negocio que garantice la continuidad de los servicios esenciales en caso de crisis. Este plan será revisado y probado periódicamente, e incluirá un Plan de Recuperación ante Desastres para las tecnologías de la información.

21. CUMPLIMIENTO REGULATORIO

RSM Chile se compromete a cumplir con toda la legislación y normativa aplicable en materia de seguridad de la información. La responsabilidad de este cumplimiento recae en todos los miembros de la organización.

22. AUDITORÍAS DE SEGURIDAD Y GESTIÓN DE VULNERABILIDADES

RSM Chile realizará auditorías periódicas para identificar vulnerabilidades técnicas en sus sistemas y aplicaciones. Una vez identificadas, se implementarán las medidas correctivas necesarias con un enfoque basado en riesgos.

23. GESTIÓN DE EXCEPCIONES

Cualquier excepción a esta Política deberá ser registrada e informada al responsable de Seguridad de la Información de RSM Chile. Las excepciones se analizarán para evaluar los riesgos y serán aprobadas por los responsables del negocio en conjunto con el peticionario.

24. SANCIONES DISCIPLINARIAS

El incumplimiento de las obligaciones establecidas en esta Política, así como de las Políticas específicas del Sistema de Gestión de Seguridad de la Información, Procedimientos u otros documentos derivados de estas, será sancionado conforme a las leyes vigentes y aplicables, así como al reglamento interno de orden para los funcionarios de RSM Chile.

Para los colaboradores de RSM Chile, el incumplimiento podrá resultar en sanciones disciplinarias que van desde amonestaciones hasta la terminación del contrato laboral, dependiendo de la gravedad de la infracción. Estas sanciones se aplicarán de acuerdo con lo estipulado en el reglamento interno de la organización y en conformidad con la normativa legal vigente.

En el caso de personas que no tengan responsabilidades administrativas dentro de RSM Chile, como prestadores de servicios, contratistas o proveedores, y que se encuentren dentro del alcance de esta Política, cualquier incumplimiento podrá resultar en la terminación anticipada del contrato, por incumplimiento de obligaciones contractuales. Esto será sin perjuicio de las responsabilidades civiles y penales que pudieran derivarse de dichas infracciones, las cuales serán perseguidas conforme a la ley.

RSM Chile se reserva el derecho de actuar legalmente contra cualquier individuo o entidad que incumpla con las obligaciones establecidas en esta Política, asegurando así la protección de la información y los activos de la organización.

25. REVISIÓN DE LA POLÍTICA

Esta Política será revisada y aprobada anualmente por el Comité de Seguridad de la Información, Ciberseguridad y Tecnología de RSM Chile. En caso de cambios significativos en el entorno operativo o en los riesgos, la Política se revisará cuando sea necesario para asegurar que sigue siendo adecuada a la realidad de la organización.

26. EXENCIÓN DE RESPONSABILIDAD

RSM Chile Auditores Ltda.

Cruz del Sur 133, 4° Piso
Las Condes
Santiago.
T: + (56) 232 539 050

El Bosque Norte 500, Oficina 1002
Las Condes
Santiago.
T: + (56) 232 539 050

THE POWER OF UNDERSTANDING
ASSURANCE | TAX | CONSULTING