Política de seguridad de la información

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Felipe Mundaca	05-02-2022	Creación del documento	Diego González	Pública
2.0	Felipe Mundaca	22-03-2023	Se reestructuró el sistema de gestión de seguridad de la información y se consideraron nuevos riesgos	Diego González	Pública
3.0	Felipe Mundaca	10-01-2024	Se agregaron nuevos objetivos de seguridad para mejorar el control	Diego González	Pública
4.0	Felipe Mundaca	22-05-2024	Adaptación al ISO 27001: 2022 y recodificación	INNOVATE DC	Pública
4.1	Fernanda Riffo Felipe Cuadra Felipe Mundaca	12-03-2026	Aclaraciones sobre Independencia de la Función de Seguridad	Diego González	Pública

RANKMI

Chile

Responsable de actualizar y revisar el documento

CISO, CTO, COO

Introducción

El Sistema de Gestión de Seguridad de la Información es un sistema cíclico que busca la mejora continua en las actividades que protegen la información que es valiosa para la operación de la empresa.

Modelo de negocio

Rankmi es una empresa que brinda un software como servicio (SaaS) enfocado a la Gestión del Talento Humano a través de módulos cómo Beneficios, Payroll, Evaluaciones de Desempeño, Clima Laboral, Reconocimiento, LMS, ATS, Genius (módulo de IA), Hub Social, entre otros, dirigidos especialmente a medianas y grandes empresas de Latinoamérica.

Propósito del documento

Este documento tiene como objetivo establecer las directivas generales y máximas en la gestión de la seguridad de la información de Rankmi.

Alcance de la Política

Esta norma es relevante para el personal, proveedores y terceras partes interesadas de los servicios del Sistema de Gestión de Seguridad de la Información conforme al alcance del SGSI definido en el documento RKM-POL-P07_Alcance del SGSI.

Política

La Alta Dirección de Rankmi ratifica su compromiso estratégico con la protección de los activos de información y la privacidad de los datos de nuestros clientes mediante la operación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la mejora continua. Este compromiso se traduce en las siguientes directrices obligatorias:

Gobernanza e Independencia de Seguridad.

Se establece la función del **Head of Security (CISO)** como un rol con autonomía técnica y operativa. Para garantizar la imparcialidad en la gestión de riesgos, el CISO posee independencia jerárquica de las áreas de desarrollo y tecnología, manteniendo una línea de reporte directa y funcional ante el Comité Directivo para la toma de decisiones estratégicas y la gestión de crisis.

Seguridad en el Ciclo de Vida y AI.

El desarrollo de nuestra plataforma SaaS, incluyendo el módulo Genius AI, integra la seguridad desde el diseño (Privacy by Design). El procesamiento mediante Inteligencia Artificial está estrictamente regulado para asegurar la segregación de datos y la monitorización constante, garantizando que el uso de estas tecnologías no comprometa la confidencialidad de la información del cliente.

Seguridad Operativa y Remota.

Nuestra infraestructura en AWS se protege mediante una arquitectura de defensa en profundidad. Dado nuestro modelo de trabajo remoto, es obligatorio el uso de cuentas corporativas dedicadas, autenticación multifactor (MFA), y estaciones de trabajo controladas con antivirus y bloqueo de medios removibles (USB) gestionado centralmente.

Ecosistema de Terceros

Extendemos nuestra postura de seguridad a toda la cadena de suministro. Las integraciones con socios estratégicos (Firma, Antecedentes, Pagos) y proveedores de servicio deben regirse por cláusulas estrictas de seguridad y privacidad, sujetas a verificación y auditoría.

Resiliencia y Cumplimiento

Rankmi mantiene su resiliencia mediante auditorías anuales, procesos constantes de hacking ético y una gestión proactiva de vulnerabilidades, asegurando el cumplimiento con los estándares **ISO 27001:2022**.

El incumplimiento de esta política por parte de empleados o proveedores será sujeto a medidas disciplinarias según la normativa interna y legal vigente.

Objetivos de Seguridad de la Información

1. Proteger la información de los clientes que es gestionada en la Plataforma de Gestión de Recursos Humanos de RANKMI.
2. Asegurar que los riesgos de seguridad sean controlados.
3. Garantizar la sostenibilidad y mejora continua capacitando al personal.
4. Prepararse para prevenir ataques cibernéticos.

Compromiso

La Dirección se compromete en satisfacer los requisitos de seguridad; confidencialidad, integridad, disponibilidad que sean aplicables y necesarios según los tipos de información que se utilicen dentro de la ejecución de los procesos que forman parte del alcance del SGSI.

Mejora continua

La Dirección se compromete a gestionar la seguridad siguiendo el modelo cíclico de mejora continua Planear-Hacer-Verificar y Actuar.

Independencia de la Función de Seguridad

Para garantizar la objetividad y evitar conflictos de interés, la función del Head of Security (CISO) posee independencia operativa de las áreas de desarrollo y tecnología. El CISO tiene autoridad directa para supervisar el cumplimiento de los controles de seguridad y reporta de manera funcional al Comité Directivo, poseyendo la facultad de escalar riesgos críticos y vetar prácticas que comprometan la integridad del SGSI sin interferencia de las metas operativas de producción.

Roles y Responsabilidades

Responsabilidades respecto de la gestión de la seguridad:

Rol	Responsabilidad
Dirección (comité directivo)	Revisar y aprobar las actualizaciones de la presente política al menos de manera semestral y cada vez que haya un cambio importante. Recibe informes del head de seguridad.
Comité Operativo	Realizar actividades y supervisar a colaboradores y proveedores a su cargo, para garantizar el cumplimiento de la presente política.
Head of Security (CISO)	Revisar el cumplimiento, revisar la eficiencia y actualizar la presente política al menos una vez al año. Entrega informe al comité directivo.
Colaboradores y Proveedores	Cumplir la presente política.

Aprobación y Revisión

Los miembros del Comité Directivo que aprueban la versión vigente de la presente política es:

Name	Title	Date of Review
Felipe Cuadra	CRH	12-03-2026
Fernanda Riffo	COO	12-03-2026
Felipe Mundaca	CTO	12-03-2026

RACI

Roles	Responsable	Aprobador	Consultado	Informado
Comité Directivo		■		
Comité Operativo	■			
Head of Security	■			
Colaboradores				■
Proveedores				■
Consultores SGSI			■	
Autoridades				■
Clientes				■
Público en general				■

Términos y Definiciones

Términos	Definiciones
Autenticidad	Que proviene de una fuente original y cierta, que puede ser verificada.
Confidencialidad	Propiedad de la información de mantenerse no público o accesible frente a personas o sistemas no autorizados.
Disponibilidad	Propiedad de la información de mantenerse accesible para poder ser utilizado por los usuarios que lo requieran.
Integridad	Propiedad de un activo de información de mantenerse exacto, sin modificaciones o alteración no autorizada.
Seguridad de la información	Preservación de las necesidades de seguridad de la información, como, por ejemplo; la confidencialidad, la integridad, disponibilidad y autenticidad de la información.
Sistema de Gestión de la Seguridad de la Información - SGSI:	Conjunto de elementos de una organización interrelacionados que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos, en el marco de mantener controlados los riesgos de la seguridad de la información.