RKM-POL-D13

Política de gestión de vulnerabilidades

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Diego González	04-05-2024	Creación del documento	INNOVATE DC	Público
2.0	Diego González	22-05-2024	Simplificación de actividades	INNOVATE	Público
2.1	Diego González	30-04-2025	Revisión y aclaración del proceso de gestión	Diego A. González	Público
2.2	Diego González	17-09-2025	Referencia a Identificación de vulnerabilidades, se clasifica como privada.	Diego A. González	Privada
2.3	Felipe Mundaca	02-07-2026	Incorporación del Rankmi Pentest Framework (RPF), cadencia mínima de hacking ético (1 auspiciado por Rankmi al año + auspiciados por clientes + escaneos adicionales) y referencia al nuevo Procedimiento RKM-PRO-D13	Diego A. González	Privada

RANKMI · Chile

Responsable de actualizar y revisar el documento: Head of Security

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 vulnerabilidades de Rankmi.

Alcance de la Política

Esta política es de cumplimiento obligatorio para los empleados y proveedores que participan en la gestión de vulnerabilidades de Rankmi.

Sección 1: Identificación de vulnerabilidades técnicas

Refiérase al documento RKM-PRO-D13 Procedimiento de Gestión de Vulnerabilidades, que detalla las fuentes de identificación, el flujo de gestión, los SLA de remediación y la cadencia mínima de actividades.

Las fuentes de identificación de vulnerabilidades técnicas de Rankmi son:

- Rankmi Pentest Framework (RPF): scanner de seguridad automatizado de ejecución interna, orientado a APIs multi-tenant (IDOR/BAC, JWT, headers, CORS, SQLi, exposición de datos sensibles, rate limiting, versionado de API, lógica de negocio).
- Hacking Ético auspiciado por Rankmi: al menos un (1) ejercicio anual, contratado con un proveedor externo, con alcance amplio sobre la plataforma.
- Hacking Ético auspiciado por clientes: múltiples ejercicios a lo largo del año, con alcance definido por cada cliente conforme a la Sección 7.
- Escaneos adicionales: monitoreo de vulnerabilidades de infraestructura (AWS Inspector, GuardDuty, Patch Manager), análisis de dependencias (SCA) y escaneos internos gray-box (ej. OWASP ZAP).

Sección 2: Responsabilidades

- Las áreas de infraestructura y desarrollo se encargan de la gestión técnica de las vulnerabilidades, incluido el seguimiento de la vulnerabilidad, la evaluación del riesgo, la actualización, el seguimiento de los activos y las responsabilidades de coordinación necesarias.
- El responsable de seguridad da seguimiento a la ejecución de los procesos de Pentest (RPF, hacking ético propio y de clientes) y a la gestión de las vulnerabilidades de cada informe.
- El equipo de TI debe actuar de forma diligente según la criticidad de las vulnerabilidades localizadas en los distintos procesos de pentest.

Sección 3: Evaluación de vulnerabilidades técnicas

Se debe analizar y verificar cada informe o hallazgo para determinar qué respuesta y actividad de remediación se necesita, siguiendo la metodología de clasificación de severidad y triage definida en RKM-PRO-D13.

Sección 4: Gestión de parches

- Se deben administrar las actualizaciones de software para garantizar que se instalen los parches aprobados más actualizados y las actualizaciones de aplicaciones para todo el software autorizado.
- Se pueden usar las entradas o hallazgos localizados en el servicio de Patch Manager.
- Se debe tomar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas, definiendo un cronograma para reaccionar a las notificaciones relevantes.

Sección 5: Abordar vulnerabilidades técnicas

- En este proceso se debe generar una tarea de Youtrack con el detalle exacto de la vulnerabilidad y un enlace hacia el informe o reporte original (RPF, hacking ético, u otro) donde se encuentra el detalle completo.
- Las vulnerabilidades se dividen en críticas, altas, medias, bajas e informativas; el equipo debe priorizar la resolución según los siguientes plazos:

Severidad	Plazo de remediación
Críticas	1-2 Sprints
Altas	2-4 Sprints
Medias	2-6 Meses

Bajas	6-12 Meses (se puede asumir el riesgo según sea el caso)

Si se reciben más de un informe con vulnerabilidades en un mismo periodo (por ejemplo, RPF y hacking ético en paralelo), se deben integrar todos los issues en un solo informe consolidado, agregando una columna que indique el origen (RPF, proveedor de hacking ético propio, hacking ético de cliente, u otro).

Sección 6: Supervisión

Se debe mantener un registro de auditoría de todos los pasos realizados en la gestión de vulnerabilidades técnicas. El proceso debe supervisarse y evaluarse periódicamente para garantizar su eficacia y eficiencia, incluyendo el cumplimiento de la cadencia mínima definida en RKM-PRO-D13 (mínimo un hacking ético auspiciado por Rankmi al año, ejecución periódica de RPF y revisión mensual de parches).

Sección 7: Regulaciones a los Pentests

Para la realización de procesos de Hacking Ético (propios o de clientes) se deben contemplar las siguientes indicaciones:

- Antes de iniciar cualquier prueba de penetración, se debe firmar un acuerdo de confidencialidad con el proveedor de Hacking Ético.
- El contrato de servicio con el proveedor debe establecer un alcance claro y limitado para las pruebas, especificando qué sistemas y datos son objeto de la prueba y cuáles están estrictamente prohibidos.
- Siempre que sea posible, las pruebas deben realizarse en entornos de staging o en empresas ficticias dentro del entorno de producción.
- Los hallazgos, especialmente aquellos relacionados con información confidencial, deben comunicarse de manera segura y directa a un canal designado. Los informes pueden compartirse con clientes, y solamente informes posteriores a las remediaciones pueden compartirse con potenciales clientes.
- Rankmi mantiene, como mínimo, un (1) ejercicio de hacking ético anual auspiciado por la compañía, además de los ejercicios auspiciados por clientes que se ejecuten a lo largo del año conforme a demanda contractual, y del escaneo continuo/periódico mediante el Rankmi Pentest Framework (RPF).

Aprobación y Revisión

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

Nombre	Cargo	Fecha de Revisión
Diego González	Head of Security	17-09-2025
Felipe Mundaca	CTO	02-07-2026

Roles y Responsabilidades

Rol	Responsabilidad
Comité Directivo	Revisar y aprobar las actualizaciones de la presente política al menos una vez al año.
Comité Operativo	Realizar actividades y supervisar a colaboradores y proveedores a su cargo, para garantizar el cumplimiento de la presente política.
Head of Security	Revisar el cumplimiento, revisar la eficiencia y actualizar la presente política al menos una vez al año.
Colaboradores y Proveedores	Cumplir la presente política.

Contactos

Sujetos	Contactos	Teléfono	Email

Head of Security	Diego González	+593 998981436	diego.gonzalez@rankmi.com / seguridad@rankmi.com

Términos y Definiciones

Términos	Definiciones
Parches	Cambios de software aplicados a un programa para corregir errores, añadir o cambiar funcionalidades, actualizarlo para asegurar compatibilidad, o mejorar su rendimiento.
Prueba de penetración	Prueba de seguridad que lanza un ciberataque simulado para encontrar vulnerabilidades en un sistema informático.
RPF	Rankmi Pentest Framework: scanner de seguridad automatizado desarrollado internamente para pruebas de caja gris sobre APIs de Rankmi. Repositorio: github.com/Rankmi/rankmi-pentest-framework.
SCA	Software Composition Analysis: análisis automatizado de dependencias de terceros para identificar vulnerabilidades conocidas.