Política de Software Autorizado

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Diego González	04-05-2025	Creación del documento	Diego A. González	Público
1.1	Diego González	28-08-2025	Rustdesk	Diego A. González	Público
1.2	Felipe A. Mundaca	14-11-2025	Directriz sobre Navegadores con Integración de Inteligencia Artificial	Diego A. González	Público
1.3	Directiva seguridad	02-04-2026	Aplicaciones y Agentes de IA permitidos	Diego A. González	Público
1.4	Diego A. González	07-04-2026	Fe de erratas	Diego A. González	Público

RANKMI

Chile

Responsable de actualizar y revisar el documento

Head of Security, CTO

Introducción

Relevancia de la Gestión de Software Autorizado

La gestión y el control del software utilizado en Rankmi son fundamentales para mantener nuestra **postura de seguridad y garantizar la continuidad de nuestras operaciones**. Dada nuestra certificación ISO 27001:2022 e ISO 27701:2019, la implementación de un control estricto sobre el software nos permite:

- **Prevenir** la instalación de software malicioso o vulnerable que podría comprometer nuestros sistemas y datos.
- **Garantizar** el uso de licencias apropiadas, evitando sanciones y problemas legales.
- **Reducir** la exposición de nuestros datos al asegurar que solo se utilicen herramientas seguras y validadas.
- **Evitar** conflictos de software y problemas de rendimiento que podrían impactar la productividad.
- **Optimizar** nuestros esfuerzos de soporte y mantenimiento en un conjunto definido de aplicaciones.

Esta política es clave para nuestra estrategia de **seguridad de la información** y para mantener la confianza de nuestros clientes y colaboradores.

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

Esta política tiene como objetivo establecer las directrices y los requisitos para la **selección, adquisición, instalación y uso de software** en todos los activos de información de Rankmi. El propósito es asegurar la **integridad, confidencialidad y disponibilidad** de la información, reducir la superficie de ataque, garantizar el **licenciamiento adecuado** y cumplir con nuestras certificaciones ISO 27001:2022 e ISO 27701:2019.

Alcance de la Política

Esta política aplica a todos los colaboradores, contratistas y terceros que utilicen cualquier activo de información propiedad de Rankmi o que se conecten a la red corporativa de Rankmi, incluyendo, pero no limitado a, estaciones de trabajo, laptops, servidores y dispositivos móviles

Principios Generales

Software Autorizado. Sólo se permitirá la instalación y uso de software que haya sido **explícitamente autorizado** por el área de Tecnología de la Información (TI).

Mínimo Privilegio. Los usuarios sólo tendrán los permisos necesarios para instalar y ejecutar el software esencial para sus funciones laborales.

Licenciamiento. Todo el software utilizado debe contar con las licencias correspondientes y estar legalmente adquirido.

Seguridad. El software autorizado debe cumplir con los **estándares de seguridad** de Rankmi y someterse a revisiones periódicas.

Actualización. El software autorizado debe mantenerse **actualizado** con los últimos parches de seguridad y versiones estables.

Sección 1: Software Autorizado para Usuarios Generales

El siguiente software está **pre-aprobado para su instalación y uso** en los equipos de los colaboradores de Rankmi, siempre que se obtenga a través de los canales oficiales definidos por TI:

5.1 Seguridad

- **Firewall.** El firewall del sistema operativo (Windows Defender Firewall, macOS Firewall y el firewall manejado por el sistema Antimalware) debe estar **siempre activado y configurado** según las directrices de TI. No se permite la instalación de firewalls de terceros sin autorización explícita de TI.
- **Antivirus. Avast Business Antivirus o Bitdefender** son las soluciones de seguridad antivirus autorizadas y deben estar instaladas, activas y con las bases de datos de firmas actualizadas en todo momento.

5.2 Navegadores Seguros

Solo los siguientes navegadores web están autorizados y deben configurarse con las políticas de seguridad corporativas definidas por TI (por ejemplo, configuración de proxy, bloqueo de scripts maliciosos, gestión de cookies):

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**
- **Safari**
- **Brave**
- **DuckDuckGo**

5.3 Paquete de Oficina y Productividad

- **Microsoft Office Suite.** (Word, Excel, PowerPoint, Outlook) o suites compatibles autorizadas.
- **Google Workspace Applications.** (Docs, Sheets, Slides) para uso a través del navegador web.
- **Herramientas de Comunicación.** (Rankmi Chat, Google Meet, Zoom, Webex, MS Teams) autorizadas por Rankmi para comunicación interna y externa.
- **Odoo**. Plataforma ERP para uso a través del navegador web.
- **Gemini**. Plataforma de IA para todas las áreas.

5.4 Otros Software General

- **Adobe Acrobat Reader** (última versión).
- **7-Zip** o herramientas de compresión y descompresión similares autorizadas.
- **Rustdesk**. Herramienta de Control Remoto.

Sección 2: Software Autorizado para el Equipo de Tecnología de la Información (TI)

El equipo de TI, debido a sus funciones específicas de desarrollo, operaciones y soporte de infraestructura, tiene autorización para instalar y utilizar las siguientes herramientas adicionales, sujetas a la **revisión y aprobación** del Head of Security y la validación de su necesidad operativa. Estas herramientas deben ser utilizadas bajo los principios de **seguridad por diseño y mínimo privilegio**.

- **Docker Desktop.** Para el desarrollo, pruebas y orquestación de contenedores.
- **pgAdmin.** Para la administración y gestión de bases de datos PostgreSQL.
- **Visual Studio Code.** Como entorno de desarrollo integrado (IDE) principal para la codificación y depuración.
- **DBeaver.** Para la conexión y gestión de diversas bases de datos.
- **AWS CLI / SDKs.** Herramientas de línea de comandos y kits de desarrollo de software para la interacción con los servicios de AWS.
- **Kubectl.** Herramienta de línea de comandos para la gestión de clústeres de Kubernetes (especialmente para nuestra infraestructura EKS).
- **Git.** Para el control de versiones de código fuente.
- **Postman / Insomnia.** Para pruebas y desarrollo de APIs.
- **Terminales Seguras.** (ej. PuTTY, iTerm2, Windows Terminal, Mac Terminal, Linux Terminal) con configuraciones seguras (SSH keys, multi-factor authentication).
- **Doppler CLI.** Para la gestión segura de secretos y configuraciones.
- **Cloudflare CLI.** Para la administración de nuestra infraestructura de red y seguridad.
- **Cursor**. Asistente IA para tecnología.

Sección 3: Software y Agentes de IA Permitidos

En el siguiente documento anexo hemos establecido los lineamientos sobre el uso de Software y Agentes de Inteligencia Artificial y las herramientas que consideramos permitidas bajo términos de seguridad, como por ejemplo el uso con información corporativa (de la empresa) en las distintas versiones de cada una de las aplicaciones indicadas:

Mapeo Herramientas de IA - Guía Rankmi

La contravención en el uso de software y agentes de IA puede resultar en una potencial fuga de información la misma que podrá ser sancionada bajo los términos indicados en la Política de Seguridad de la Información en el Trabajo.

Sección 4: Proceso de Solicitud y Aprobación de Software No Listado

Cualquier software no especificado en las secciones 1 o 2 requiere una **solicitud formal y aprobación** del área de TI y/o el Head of Security antes de su instalación y uso. El proceso incluirá:

1. **Justificación.** El solicitante deberá proporcionar una justificación clara de la necesidad del software, su funcionalidad, costos, tipo de licencia, y de ser necesario, por qué el software autorizado existente no es suficiente.
2. **Evaluación de Riesgos.** TI y Seguridad realizarán una evaluación de riesgos del software propuesto, considerando su origen, vulnerabilidades conocidas, requisitos de licenciamiento, impacto en el rendimiento y compatibilidad con nuestros sistemas existentes.
3. **Aprobación.** La aprobación final será otorgada por el Head of Security, con el respaldo del Comité Operativo si es necesario.
4. **Adquisición y Despliegue.** Una vez aprobado, TI será responsable de la adquisición (si aplica) y la gestión del despliegue seguro del software.

Sección 5: Auditoría y Cumplimiento

- El área de TI realizará **auditorías periódicas** (al menos una vez al año) para asegurar el cumplimiento de esta política, incluyendo la revisión de software instalado, versiones y configuraciones.
- Se utilizarán herramientas de monitoreo (como **AWS Config, Amazon Inspector, Amazon GuardDuty**) para detectar software no autorizado o configuraciones inseguras.
- Cualquier incumplimiento de esta política puede resultar en **acciones disciplinarias** según las políticas internas de Rankmi, y la desinstalación inmediata del software no autorizado.

Sección 6: Actualizaciones y Gestión de Parches

La gestión oportuna de actualizaciones y parches es un pilar fundamental de nuestra estrategia de seguridad de la información, en línea con el **RKM-PRO-27 Procedimiento de gestión de parches**. Asegurar que todo el software autorizado esté actualizado es crucial para mitigar vulnerabilidades y proteger nuestros activos de información.

Sección 7: Directriz sobre Navegadores con Integración de Inteligencia Artificial (IA)

Prohibición de uso de Funcionalidades de IA.
Está **estrictamente prohibido** utilizar cualquier funcionalidad o asistente de Inteligencia Artificial (IA) integrado en los navegadores web (incluidos los autorizados en la Sección 1) cuando dicha funcionalidad requiera el envío de **datos o contenido** de la red corporativa o de los activos de Rankmi a un servicio de terceros (como resúmenes de páginas, *chatbots* conscientes del contexto de navegación, o funciones de escritura/análisis).

Control de la Configuración.
El área de TI tiene la responsabilidad y la autoridad de **deshabilitar** o **restringir** las funcionalidades de IA en todos los navegadores web corporativos a través de las políticas de seguridad.

Autorización Explícita.
El uso de cualquier navegador con capacidades de IA o de cualquier funcionalidad de IA en navegadores existentes no se considerará autorizado por defecto y requerirá una **solicitud formal y una Evaluación de Riesgos** completa a través del proceso descrito en la Sección 3, la cual debe ser aprobada por el Head of Security. La justificación deberá detallar cómo se garantiza la **confidencialidad** de los datos de Rankmi.

Sección 8: Excepciones

Cualquier excepción a esta política debe ser **justificada, documentada y aprobada** por el Head of Security y la Dirección, y revisada periódicamente.

Aprobación y Revisión

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

Nombre	Cargo	Fecha de Revisión
Diego González	Head of Security	02-04-2026
Felipe Cuadra	CRH	02-04-2026
Fernanda Riffo	COO	02-04-2026
Felipe Mundaca	CTO	02-04-2026

Roles y Responsabilidades

Responsabilidades respecto de la gestión de la seguridad:

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.
Equipo de TI	El equipo de TI es responsable de monitorear, evaluar, probar y desplegar las actualizaciones y parches de seguridad para todo el software autorizado en la infraestructura y equipos corporativos. Esto incluye, pero no se limita a, sistemas operativos, aplicaciones críticas, antivirus y navegadores web.
Colaboradores y Proveedores	Los colaboradores son responsables de instalar las actualizaciones que el equipo de TI les notifique, así como de asegurarse de que el software autorizado en sus equipos

	personales (si aplica) se mantenga actualizado, siguiendo las directrices proporcionadas.

RACI

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

Contactos

Lista de roles notables:

Sujetos	Contactos	Teléfono	Email
Consultas	Diego González	+593998981436	diego.gonzalez@rankmi.com