Política de Seguridad de la Información en el Trabajo

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Diego González	03-01-2022	Versión inicial	INNOVATE DC	Pública
2.0	Diego González	22-03-2023	Se reestructuró el sistema de gestión de seguridad de la información y se consideraron nuevos riesgos.	INNOVATE DC	Pública
3.0	Diego González	18-04-2023	Precisiones del borrado irrecuperable	INNOVATE DC	Pública
4.0	Diego González	11-01-2024	Se reemplaza a la política Política de Teletrabajo, BYOD, dispositivos móviles y uso adecuado de activos por la Política de Seguridad de la Información en el Trabajo y se alinean los controles al estándar ISO 27001:2022	INNOVATE DC	Pública
5.0	Diego González	04-05-2024	Adaptación al ISO 27001:2022 y recodificación	INNOVATE DC	Pública
6.0	Diego González	02-07-2024	Remediaciones del procedimiento de mantenimiento de equipos	INNOVATE DC	Pública
7.0	Diego González	11-07-2024	Sección de identidades	RANKMI	Pública
8.0	Diego González	08-11-2024	Medios de transferencia oficiales	RANKMI	Pública
9.0	Diego González	20-06-2025	Borrado seguro de archivos	RANKMI	Pública
9.1	Diego González	26-06-2025	Especificaciones y fe de erratas ambigüedades	RANKMI	Pública
9.2	Diego González	02-07-2025	Sección de firewall	RANKMI	Pública
10.0	Diego A. González	08-09-2025	Cifrado de disco	RANKMI	Pública
10.1	Diego A. González	01-04-2026	Aclaraciones del Proceso Disciplinario	RANKMI	Pública

RANKMI

Chile

Responsable de actualizar y revisar el documento

Head of Security

Introducción

La Gestión de Seguridad en el Trabajo se refiere a la implementación de controles de seguridad para garantizar un entorno laboral seguro y saludable para todos los colaboradores. Establece medidas para prevenir lesiones y promover prácticas seguras en el lugar de trabajo, reafirmando nuestro compromiso inquebrantable con la protección de la salud y seguridad de todos los empleados.

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 respecto a la gestión de seguridad en el trabajo que se deben adoptar en Rankmi.

Alcance de la Política

Esta política es de cumplimiento obligatorio para todos los empleados, proveedores, contratistas y socios comerciales que participan en las operaciones de Rankmi y/o tienen acceso a sus activos de información.

Política

Todos los proyectos relativos a la implementación de servicios dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) deben utilizar los controles estipulados en la presente política.

Sección 1: Gestión de Activos de Información

- **Identificación y Clasificación.** Los activos de información de Rankmi se encuentran listados en el inventario de activos de información. Cada activo es asignado a un propietario, clasificado y etiquetado en función de sus necesidades de confidencialidad, integridad, disponibilidad y autenticidad. La clasificación de la información determinará las medidas de seguridad y los controles aplicables para su protección.
- **Protección Obligatoria.** Los empleados, proveedores y socios deben proteger la información de acuerdo con su clasificación y etiquetado. Los propietarios de los activos son responsables de velar por la protección de los accesos, la integridad y la disponibilidad de la información según sus necesidades. Los activos deben ser protegidos desde su adquisición, generación, desarrollo, prueba, puesta en producción, mantenimiento, transporte o eliminación.
- **Instrucciones de Protección.** La presente política provee instrucciones sobre cómo proteger los activos de información durante las actividades laborales.

Sección 2: Retorno y Eliminación Segura de Activos

Devolución de Activos. Al finalizar la relación contractual de un empleado, proveedor o socio comercial, o al ser trasladado a otros roles, el individuo debe devolver todos los activos de información (documentos, datos, imágenes, etc.), así como los activos físicos y electrónicos propiedad de Rankmi, al propietario del activo, al área contratante o al Head of Security.

Borrado Seguro en Dispositivos Personales/Adquiridos. En los casos en que el personal o terceros adquieran o utilicen sus propios equipos, toda la información relevante de la empresa debe ser transferida a Rankmi y posteriormente eliminada de forma segura del equipo personal.

Transferencia de Conocimiento. Si el personal o terceros poseen conocimientos importantes para las operaciones en curso, esta información debe ser documentada y transferida a la organización.

Eliminación o Reutilización Segura de Equipos. Los medios de almacenamiento que contengan información confidencial o protegida por derechos de autor deben ser destruidos físicamente, o la información debe ser eliminada o sobrescrita utilizando técnicas que impidan su recuperación, en lugar de la función de eliminación estándar.

- Se debe eliminar el etiquetado y referencias a la organización.
- En caso de equipos dañados con información no cifrada o protegida, el Head of Security realizará una evaluación de riesgos para determinar si deben destruirse físicamente.
- Se debe informar al Head of Security antes de desechar o enviar equipos a reparación.
- El cifrado de discos completos debe ser robusto y las claves criptográficas deben ser suficientemente largas, confidenciales y no almacenadas en el mismo disco.

Sección 3: Transferencia de Información y Medios

Medios de Almacenamiento Físico

- La transferencia de información en medios de almacenamiento físico (ej., memorias USB externas) requiere autorización por correo electrónico del jefe de área, propietario del activo o Head of Security, indicando el propósito.
- El uso de medios de almacenamiento extraíbles no está permitido, a menos que sea estipulado por los propietarios de la información, el área contratante o el Head of Security en el inventario de activos o el inventario del proyecto.
- Si se utilizan medios de almacenamiento físico que deban ser desechados o transferidos, la información confidencial contenida debe ser borrada de manera segura.

Dispositivos de Comunicación y Computación. Se permite ingresar y retirar dispositivos de comunicación y computación (tablets, laptops, celulares) de las oficinas, bajo la responsabilidad del empleado, proveedor o socio, siempre que se cumplan las disposiciones de seguridad de esta política. No se permite retirar otros equipos, salvo para roles encargados de mantenimiento.

Transferencia Verbal. No se deben tener conversaciones verbales sobre temas confidenciales de la empresa en lugares públicos o por canales de comunicación inseguros. Solo el personal o terceros autorizados pueden participar en dichas conversaciones. Los temas confidenciales son aquellos referidos al contenido de los activos de información clasificados como confidenciales.

Transferencia Electrónica.

- La transferencia electrónica de información confidencial debe realizarse sólo por canales cifrados y autenticados, previa verificación de la identidad del receptor y bajo autorización del propietario de la información o como parte de las obligaciones laborales.
- Se debe utilizar el correo electrónico empresarial para comunicaciones relacionadas con Rankmi.
- Todo mensaje recibido debe ser verificado contra malware.
- La transferencia de información confidencial debe ser realizada sólo a cuentas de correo verificadas.
- No se debe enviar información ni responder automáticamente o manualmente a correos electrónicos desconocidos.
- Se prohíbe la transferencia o carga de información de nuestros clientes a través de medios no oficiales. Los medios oficiales incluyen: Google Drive corporativo de Rankmi, Buckets S3 del producto, o cualquier plataforma segura aprobada por el equipo de Seguridad de Rankmi.

Sección 4: Información de Autenticación

Es responsabilidad de cada usuario:

- Proteger la información de la empresa a la que tenga acceso.
- Proteger la información de autenticación, como contraseñas personales o PIN.
- Cambiar contraseñas temporales asignadas por contraseñas seguras y no predecibles.
- Renovar periódicamente sus contraseñas.
- Activar la autenticación de dos factores (2FA) cuando esté disponible y sea requerido.
- Las identidades son de uso personal e intransferible. No se pueden usar credenciales de otro colaborador.
- Es de total responsabilidad del colaborador y del proveedor la protección de las credenciales e identidades entregadas, haciendo uso adecuado de esta política y de otras relacionadas a la seguridad de contraseñas y compartición de información.
- Notificar la terminación del uso de credenciales (por cambio de rol o término de periodo de uso) a su supervisor o al equipo responsable de la plataforma.

Sección 5: Escritorio y pantalla limpios

- Los empleados, proveedores y socios deben proteger los dispositivos terminales con cerraduras o medios de seguridad cuando no estén en uso o desatendidos.
- Se debe bloquear la pantalla y teclado o desconectar el equipo, protegido por un mecanismo de autenticación, cuando estén desatendidos.
- Todas las computadoras y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático después de 15 minutos de inactividad.
- Se debe mantener el escritorio físico libre de información sensible o confidencial cuando no se esté presente.

Sección 6: Seguridad de los activos fuera de las instalaciones

Cualquier dispositivo que se use fuera de las instalaciones y que almacene o procese información confidencial (organizacional o personal), incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad privada (BYOD) utilizados en nombre de la organización, deben utilizar protección antimalware o contra ataques de cibercrimen.

El uso de estos dispositivos para el procesamiento de información confidencial debe ser autorizado o estipulado en el inventario de activos por los propietarios de la información.

Dispositivos de Punto Final de Usuario

- La empresa puede restringir la instalación de software en los dispositivos del usuario, según la sensibilidad de la información.
- El empleado, contratista o proveedor es responsable de:
  - Cerrar sesiones activas y finalizar servicios no necesarios.
  - Proteger los dispositivos terminales con control físico (cerradura de llave) y lógico (acceso con contraseña) cuando no estén en uso.
  - No dejar desatendidos dispositivos con información importante (sensible o crítica).
  - Usar dispositivos con especial cuidado en lugares públicos o desprotegidos (evitar lectura por terceros, usar filtros de pantalla de privacidad).
  - Proteger físicamente los dispositivos contra robos (en vehículos, hoteles, conferencias).
  - Notificar a Recursos Humanos (empleados) o al área contratante (proveedores) en caso de pérdida o robo de dispositivos con información confidencial.
  - Utilizar conexiones inalámbricas seguras (WIFI) o protegidas con VPN o canales cifrados HTTPS.

Sección 7: Mantenimiento de Equipos

- Solo el personal o proveedores de mantenimiento autorizados pueden realizar reparaciones y mantenimiento de equipos de la empresa.
- La necesidad de mantenimiento debe ser notificada al responsable interno del país correspondiente o al responsable de la oficina central en Chile si no hay un responsable asignado.
- Durante el mantenimiento de dispositivos con información confidencial, se deben adoptar las siguientes medidas:
  - Supervisar al personal de mantenimiento.
  - Aplicar medidas de seguridad para activos fuera de las instalaciones si el equipo es retirado para mantenimiento.
  - Inspeccionar el equipo después del mantenimiento para asegurar que no ha sido manipulado y funciona correctamente.

Sección 8: Protección contra Malware y Software

- No se debe instalar software o sistemas operativos no licenciados o provenientes de fuentes no confiables.
- Mantener instalado un sistema o servicio antimalware, o una configuración del sistema operativo que detecte el uso de sitios web maliciosos o sospechosos.
- El sistema antimalware debe detectar y bloquear ataques que puedan explotar vulnerabilidades de seguridad.
- Escanear periódicamente los computadores y medios de almacenamiento electrónico.
- Escanear cualquier dato recibido a través de redes o medios de almacenamiento electrónico en busca de malware antes de su uso.
- Escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso.
- Escanear páginas web en busca de malware al acceder a ellas.

Sección 9: Uso de Dispositivos Personales (BYOD)

Los empleados y proveedores que usen sus propios equipos deben:

- Separar el uso personal y comercial en el sistema operativo, incluyendo software para respaldar dicha separación y proteger los datos comerciales.
- Crear una cuenta separada para acceder a su sesión de trabajo en Rankmi.
- Aceptar sus deberes estipulados en esta política (protección física, actualización de software, etc.), renunciando a la propiedad de los datos de la empresa.
- Permitir la eliminación remota de datos por parte de la organización en caso de robo.
- Permitir la eliminación remota de datos por parte de la organización en caso de salida de la empresa.
- Permitir el acceso al usuario dedicado para verificar la seguridad de la máquina o durante una investigación

Sección 10: Trabajo Remoto

En caso de trabajo remoto, el personal y los proveedores deben cumplir lo siguiente:

- Las conexiones de acceso remoto (ej., escritorio virtual) que soporten procesamiento y almacenamiento de información en equipos privados deben protegerse con criptografía, autenticación de entidades y, si es posible, de dispositivos. El dispositivo debe tener protección antimalware antes de conectarse.
- Es responsabilidad del usuario garantizar que no ocurra acceso no autorizado a información o recursos por parte de otras personas en los dispositivos utilizados para el trabajo remoto (ej., familia y amigos).
- Es responsable de garantizar que no ocurra acceso no autorizado a información o recursos por parte de otras personas en lugares públicos.
- En redes domiciliarias y públicas, se deben utilizar canales VPN SSL.
- Activar la configuración de firewalls, cifrado de datos y utilizar la herramienta de protección contra malware en los computadores.
- Utilizar solamente servicios y sistemas provistos por la empresa para implementar e inicializar sistemas de manera segura de forma remota.
- Utilizar mecanismos seguros de autenticación suficientemente fuertes según los privilegios de acceso, y usar más de un factor de autenticación cuando sea posible.
- Las actividades permitidas en trabajo remoto, el tipo de información a la que se puede acceder, la información bajo custodia y los sistemas internos autorizados deben ser estipulados o autorizados por los propietarios, líderes de proyecto o áreas contratantes.
- La información debe ser siempre almacenada o respaldada en los repositorios virtuales provistos por la empresa para garantizar la continuidad del negocio.
- Se debe permitir la auditoría y el seguimiento de la seguridad por parte del administrador autorizado por la empresa.
- Al finalizar las actividades, se revocarán la autorización y los derechos de acceso, y se deberán devolver los equipos.

Sección 11: Reporte de Eventos de Seguridad y Vulnerabilidades

Todo el personal y proveedores son responsables de informar los eventos de seguridad de la información tan pronto como sea posible para minimizar el efecto de los incidentes.
En caso de detección de eventos de seguridad, los empleados y proveedores deben reportarlos por correo electrónico a la cuenta de seguridad de la empresa (`seguridad@rankmi.com`) de forma inmediata, idealmente en un plazo no mayor a 1 hora. Para incidentes críticos que impidan el uso del correo, se debe utilizar el canal de comunicación alternativo designado por el Head of Security.

Situaciones que requieren reporte de seguridad:

- Control de seguridad de la información ineficaz.
- Incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información.
- Errores humanos.
- Incumplimiento de la política de seguridad de la información, políticas de tópico específico o normas aplicables.
- Incumplimientos de las medidas de seguridad física.
- Cambios del sistema que no han pasado por el proceso de gestión de cambios.
- Mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware.
- Infracciones de acceso.
- Vulnerabilidades.
- Sospecha de infección por malware.

El personal y los proveedores no deben probar vulnerabilidades de seguridad de la información sospechosas, ya que esto puede resultar en responsabilidad legal.

Sección 12: Borrado Seguro de Archivos y Datos Personales

Todo el personal que realice tratamiento de la información personal de nuestros clientes, y que descargue archivos con información personal, confidencial, privada y sensible de los clientes de Rankmi en sus máquinas y dispositivos, una vez que haya concluido con el uso de la información indicada, deberá obligatoriamente realizar el Borrado Seguro y Definitivo (Irrecuperable) de la información. Para esto deberá seguir los lineamientos establecidos en el procedimiento RKM-PRO-Borrado-Seguro-Archivos.

Sección 13: Capacitación y Concientización

El cumplimiento de esta política y la comprensión de sus principios son requisitos obligatorios para la continuidad de la relación laboral o contractual. La participación en los programas de concientización es vinculante, y su inobservancia será tratada como un incumplimiento administrativo de las obligaciones contractuales, integrándose formalmente en las métricas de desempeño y conducta del colaborador.

Sección 14: Monitoreo y Auditoría

Rankmi se reserva el derecho de monitorear y auditar el cumplimiento de esta política, incluyendo el uso de sistemas, redes y dispositivos, para garantizar la seguridad de la información y la integridad de los activos de la empresa. La aceptación de esta política implica el consentimiento a dichas actividades de monitoreo y auditoría.

Sección 15: Gestión de Incumplimientos y Proceso Disciplinario

El incumplimiento de las directrices establecidas en esta política, así como de cualquier norma de seguridad de la información de Rankmi, activará un proceso de gestión de infracciones coordinado entre las áreas de Seguridad, Recursos Humanos y Legal.

El Head of Security es el responsable de liderar la investigación técnica para determinar el alcance, la intencionalidad y el impacto del evento, mientras que el área de Recursos Humanos actuará como responsable administrativo para asegurar que cualquier medida se aplique conforme al reglamento interno y la legislación laboral vigente.

El área Legal brindará soporte en la calificación jurídica del incumplimiento, especialmente en casos que involucren la propiedad intelectual o datos sensibles de clientes, evaluando la procedencia de acciones civiles o penales adicionales.

Este proceso se integra directamente con el Código de Conducta de la organización, garantizando que todo colaborador o proveedor tenga derecho a ser escuchado antes de la determinación final de una sanción.

15.1. Clasificación de Infracciones y Medidas Aplicables

Las infracciones a la presente política se clasificaron en tres niveles de severidad según el riesgo generado para Rankmi.

- Se considerará una **Infracción Leve** aquel descuido operativo que no comprometa la integridad de los datos, como el incumplimiento de la política de escritorio limpio o el uso de bloqueos de pantalla, cuya sanción principal será una amonestación verbal o escrita con fines educativos.
- Se calificará como **Infracción Moderada** la reincidencia en faltas leves o acciones que expongan información interna sin autorización, tales como la instalación de software no licenciado o la omisión en el reporte de pérdida de activos, resultando en una amonestación formal en el expediente laboral.
- Finalmente, se considerará **Infracción Grave** cualquier acción dolosa o negligencia crítica que resulte en la fuga de información de clientes, el uso de canales no oficiales para transferencias sensibles, el préstamo de credenciales de acceso o la manipulación deliberada del cifrado de disco, lo cual facultará a Rankmi para proceder con la terminación del vínculo contractual y el inicio de las acciones legales pertinentes.

Sección 16: Gestión de Excepciones

Cualquier solicitud de excepción a los principios establecidos en esta política debe ser presentada por escrito al Head of Security, justificando la necesidad y proponiendo medidas compensatorias. Toda excepción debe ser aprobada formalmente por el Comité Directivo de Seguridad de Rankmi.

Sección 17: Firewall

La configuración de firewall en dispositivos móviles se basará en el principio de **mínimo privilegio** y se implementará a través de una solución MDM centralizada para dispositivos corporativos y/o configuraciones específicas para BYOD, según se detalle.

- **17.1. Reglas de Filtrado de Tráfico**
  - **Tráfico Saliente.** Se permitirá únicamente el tráfico necesario para el funcionamiento de aplicaciones corporativas autorizadas y servicios esenciales (ej. DNS, NTP, actualizaciones del sistema). Todo otro tráfico saliente no explícitamente permitido será denegado por defecto.
  - **Tráfico Entrante.** Se denegará por defecto todo el tráfico entrante no solicitado, con la excepción de respuestas a conexiones iniciadas por el dispositivo. No se permitirá la escucha de puertos para servicios externos a menos que sea estrictamente necesario y justificado por el negocio, y en cuyo caso, se aplicarán reglas de acceso estrictas.
- **17.2. Control de Aplicaciones**
  - Se establecerán políticas para restringir la instalación de aplicaciones no autorizadas o de fuentes no confiables.

Sección 18: Cifrado de Discos

Todo equipo de trabajo en Rankmi, que almacene información de nuestros clientes, deberá contar con cifrado de disco duro, esto con la finalidad de evitar que un equipo robado, descuidado o manipulado permita el acceso libre a la información almacenada en él. Todo colaborador deberá activar el cifrado en disco de su equipo sin excepción (y para todo sistema operativo), y no deberá manipular esta configuración posteriormente. Todo equipo entregado por Rankmi, además, tendrá activa esta opción por defecto, realizada con usuario administrador, y sin la posibilidad de desactivación de esta configuración.

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	04-05-2024
Felipe Mundaca, Fernanda Riffo, Felipe Cuadra	CTO, COO, CRH	01-04-2026
Diego González	Head of Security	26-06-2025

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.
Gestión de Incumplimientos	Head of Security / RRHH
Colaboradores y Proveedores	Cumplir la presente política.

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

Términos y Definiciones

Términos	Definiciones
Empleado	Toda persona que tenga un vínculo contractual de trabajo con Rankmi sea éste indefinido, a plazo fijo o a honorarios.
Dispositivo móvil	Aparatos portátiles con capacidades de procesamiento y almacenamiento de información, así como capacidades de conexión a una red y/o Internet. Esto incluye notebooks, laptops, tablets y smartphones.
Medio removible	Corresponde a dispositivos que se utilizan principalmente para almacenamiento, respaldo o transferencia de información, aún cuando pueden contar con capacidades de procesamiento y conectividad.
BYOD	Sigla que corresponde a la expresión en inglés “Bring Your Own Device”, que traducido al español significa “trae tu propio dispositivo”. El ejemplo más común es autorizar a un empleado a utilizar un notebook o un “smartphone” personal, para almacenar o comunicar información de la organización.