SLA’s Seguridad

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Felipe Mundaca	20-05-2025	Creación del documento	Diego González	Público
1.1	Felipe Mundaca	04-06-2025	Borrados seguro	Diego González	Público

RANKMI

Chile

Responsable de actualizar y revisar el documento

Information Security Manager

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 los Service Level Agreement (SLA) de los procedimientos relacionados al área de seguridad de Rankmi

Tiempos de Respuesta y Resolución de Incidentes de Seguridad

La rapidez es clave en la gestión de incidentes. Clasificaremos los incidentes por severidad para asignar los tiempos de respuesta y resolución adecuados, alineados con el **Procedimiento de Gestión de Incidentes de seguridad**

Severidad del Incidente	**Definición**	**Impacto en el Negocio**	**Tiempo Máximo de Respuesta (Primera Acción/Notificación)**	**Tiempo Objetivo de Resolución (Contención/ Mitigación)**	**Consideraciones**
Crítico (P1)	Violación de datos, interrupción total del servicio, acceso no autorizado a sistemas críticos.	Impacto Severo, pérdida financiera, daño reputacional, incumplimiento legal.	**30 minutos** (24/7)	**2 horas** (Contención inicial); **4 horas** (Mitigación significativa); **24 horas** (Resolución completa)	Activación inmediata del BCP/DRP (**RKM-PRO-D0 Business Contituity Plan V1.0.docx**). Involucramiento del Comité de Seguridad.

Alto (P2)	Exposición de datos sensibles, degradación significativa del servicio, vulnerabilidad crítica explotada.	Impacto Moderado, afectación a procesos clave, posible multa regulatoria.	**1 hora** (24/7)	**4 horas** (Contención inicial); **8 horas** (Mitigación significativa); **48 horas** (Resolución completa)	Evaluación de impacto y escalamiento según procedimiento.
Medio (P3)	Acceso no autorizado a sistemas no críticos, actividad sospechosa, vulnerabilidad de seguridad detectada.	Impacto Leve, interrupción menor, necesidad de investigación.	**4 horas** (Horario Laboral)	**48 horas** (Contención); **5 días hábiles** (Resolución)	Evaluación de impacto y escalamiento según procedimiento.
Bajo (P4)	Políticas de seguridad no conformes, reporte de falso positivo,	Impacto Mínimo, no afecta la operación.	**8 horas** (Horario Laboral)	**15 días hábiles** (Resolución)	Registro y seguimiento de la solicitud.

	solicitudes de información de seguridad.				

Gestión y Eliminación de Información del Cliente

Considerando la sensibilidad de la información y la necesidad de cumplir con normativas de privacidad (ISO 27701:2019), estableceremos un SLA robusto para la eliminación de datos.

- **SLA 1: Tiempo de Eliminación Total de Información de un Cliente (Solicitud de Baja)**
  - **Definición.** Plazo máximo para la eliminación completa e irreversible de todos los datos personales y de la cuenta de un cliente, incluyendo backups y logs, una vez recibida una solicitud formal y verificada.
  - **Categoría de Datos.** Aplica a datos almacenados en RDS (Postgres) y AuroraDB (Rankmi Audit), así como cualquier dato asociado en sistemas de almacenamiento de archivos (S3) o caché.
  - **Tiempo de Eliminación:**
    - **Datos en Producción: 15 días hábiles** desde la confirmación de la solicitud.
    - **Datos en Backups y Logs: 45 días calendario** desde la confirmación de la solicitud (garantizando que la rotación de backups y la política de retención permitan esta eliminación).

- **Verificación.** Se proporcionará un certificado de eliminación o un informe de auditoría que confirme la baja total de la información.
- **Consideraciones.** Se tendrá en cuenta el procedimiento de firma del documento “Solicitud de Borrado Total de Información" y las responsabilidades como "Encargado del Tratamiento" para asegurar la correcta comunicación y cumplimiento con el responsable del tratamiento.

Gestión de Vulnerabilidades

En Rankmi, nos comprometemos a mantener la seguridad de nuestra plataforma y proteger la información de nuestros clientes. Por eso, implementamos un proceso claro para manejar y resolver las vulnerabilidades de seguridad que identificamos, incluyendo las reportadas en informes de hacking ético.

Una vez que detectamos una vulnerabilidad, la clasificamos según su severidad (Crítica, Alta, Media, Baja, Informativa) y su impacto potencial. Esto nos permite priorizar y actuar rápidamente:

Vulnerabilidades Críticas y Altas. Son nuestra máxima prioridad. Nos comprometemos a resolverlas en un plazo máximo de dos (2) sprints de desarrollo desde su confirmación. Esto asegura que abordamos las amenazas más importantes de inmediato, alineados con nuestra validación de seguridad OWASP Top 10.

Vulnerabilidades Medias. Buscamos resolverlas en un plazo de hasta dos (2) meses. Si la complejidad de la solución es mayor y requiere más tiempo, se comunicará y planificará adecuadamente.

Vulnerabilidades Bajas. Las abordaremos en un plazo de hasta seis (6) meses, siempre que sea factible y eficiente. Revisamos estas vulnerabilidades para ver si su resolución aporta un valor significativo o si pueden ser postergadas sin riesgo.

Vulnerabilidades Informativas. Estas se documentan, pero generalmente no requieren acción inmediata. Podrían descartarse si no representan un riesgo real o si su impacto es nulo.

Después de implementar cualquier solución, siempre realizamos pruebas para asegurarnos de que la vulnerabilidad esté corregida y que no se hayan introducido nuevos problemas.

SLAs de Seguridad Críticos

Para garantizar la **seguridad del código** (OWASP Top 10) y la **infraestructura** (Procedimientos Infraestructura Segura), así como la eficiencia operativa con un equipo reducido, se proponen los siguientes SLAs:

- **SLA 2: Aplicación de Parches de Seguridad Críticos (CVEs con CVSS >= 9.0)**
  - **Definición.** Plazo máximo para la aplicación de parches de seguridad para vulnerabilidades críticas en la infraestructura y aplicaciones que afecten directamente la operatividad del servicio o la confidencialidad/integridad de los datos.
  - **Tiempo de Aplicación: 72 horas laborables** desde la disponibilidad del parche o la notificación de la vulnerabilidad.
  - **Consideraciones.** Se seguirá el **Procedimiento de gestión de parches.docx**, priorizando la continuidad y estabilidad del servicio. Se considerarán ventanas de mantenimiento coordinadas con el equipo de Desarrollo y Operaciones.
- **SLA 3: Resolución de Vulnerabilidades OWASP Top 10 (Detectadas en Pruebas de Seguridad)**
  - **Definición.** Plazo máximo para la resolución de vulnerabilidades de seguridad identificadas en el código fuente o en la aplicación, priorizando aquellas que estén dentro del OWASP Top 10.

    - **Tiempo de Resolución (para vulnerabilidades Críticas/Altas del OWASP Top 10):**
        - **Críticas: 15 días hábiles** desde su identificación.
        - **Altas: 30 días hábiles** desde su identificación.
    - **Consideraciones.** El equipo de desarrollo priorizará estas correcciones como parte de sus sprints, siguiendo el **Procedimiento de Revisión de productos y servicios de desarrollo**. Se implementarán controles en el CI/CD para prevenir la introducción de nuevas vulnerabilidades.
- **SLA 4: Disponibilidad de Backups Críticos (RPO/RTO)**
    - **Definición:** Garantía de que los backups están disponibles y son recuperables para asegurar la continuidad del negocio.
    - **Objetivo de Punto de Recuperación (RPO):**
        - **Bases de Datos Críticas (BDD PostgresSQL): 1 hora** (máxima pérdida de datos).
        - **Bases de Datos Críticas (BDD AuroraDB): 2 horas** (máxima pérdida de datos).
        - **Otras Bases de Datos y Datos de Archivos: 24 horas**.
    - **Objetivo de Tiempo de Recuperación (RTO):**
        - **Restauración Completa de Servicio Crítico: 8 horas** (desde la declaración de desastre).
        - **Restauración Parcial de Servicio o Datos Específicos: 4 horas**.
    - **Consideraciones.** Se aplicarán los **Procedimientos de Recuperación de Desastres**. Se realizarán pruebas periódicas de restauración de backups para asegurar su validez.
- **SLA 5: Revisiones de Línea Base de Seguridad de Infraestructura**
    - **Definición.** Frecuencia con la que se revisan y validan las configuraciones de seguridad de la infraestructura clave (servidores críticos en AWS EC2/EKS, equipos de red, etc.) contra las líneas base establecidas.
    - **Frecuencia: Trimestral** (al menos).

- **Consideraciones.** Se utilizará el **Línea Base Servidores y Equipos** y **Procedimientos Infraestructura Segura**. Las auditorías internas y externas validarán este cumplimiento.

Aprobación y Revisión

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

Name	**Title**	**Date of Review**
Felipe Mundaca Fernanda Rifo	CTO COO	25-06-2025
Equipo de TI	Arquitectos, Gerentes de Producto, TI Leads	27-06-2025

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.
Oficial de Seguridad	Revisar el cumplimiento, revisar la eficiencia y actualizar la presente política al menos una vez al año.
Colaboradores y Proveedores	Cumplir la presente política.

RACI

Roles	Responsable	Aprobador	Consultado	Informado
Comité Directivo		☑		
Comité Operativo	☑			
Oficial de Seguridad	☑			
Colaboradores				☑
Proveedores				☑
Consultores SGSI			☑	

Autoridades				☑
Clientes				☑
Público en general				☑

Contacts

Lista de roles notables:

Sujetos	**Contactos**	**Teléfono**	**Email**
Consultas	Diego González	+593 998981436	diego.gonzalez@rankmi.com