P16 Procedimiento de respuesta a incidentes

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Felipe Mundaca	05-05-2024	Creación del documento	INNOVATE DC	Privado
2.0	Felipe Mundaca	26-02-2025	Mejoras	INNOVATE DC	Privado
3.0	Felipe Mundaca	20-06-2025	Conservación de evidencia y consideraciones legales, CSIRT Chile	Diego A. González	Privado

3.1	Felipe Mundaca	27-06-2025	Se pasan tiempos de respuesta a SLA's	Diego A. González	Privado

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 las directivas generales y máximas en la gestión de la respuesta a incidentes de seguridad 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 P07 Alcance del SGSI. Pero sobre todo está enfocado en el **equipo de respuesta a incidentes y el equipo de análisis forense** de Rankmi.

Matriz Legal

País	Ley/Regulación	Obligación de Notificación de Incidentes	Autoridad Competente / Contacto Relevante

Chile	**Ley 21.663 - Ley Marco de Ciberseguridad** (Publicada en 2024)	**Alerta Temprana:** Máx. **3 horas** al CSIRT Nacional para incidentes con efectos significativos (Operadores de Importancia Vital). **Reporte Final:** Máx. **24 horas**.	**CSIRT Nacional de Chile** (Servicio Público)
Chile	**Nueva Ley de Protección de Datos Personales** (Pendiente de promulgación final, reemplazará la Ley 19.628)	Notificación obligatoria al **titular** en caso de tratamiento de datos que le afecte.	**Consejo para la Transparencia** (Transitorio, en espera del nuevo órgano de control)
Perú	**Ley N° 29733 - Ley de Protección de Datos Personales (LPDP) y D.U. 007-2020**	Notificación a la **ANPD** de incidentes de seguridad de datos personales de forma **inmediata**, conforme a los plazos regulatorios. Notificación al **titular** (persona afectada) de la brecha.	**Autoridad Nacional de Protección de Datos Personales (ANPD)**
Perú	**Regulación de Ciberseguridad** (Directrices y Recomendaciones)	Reporte a **CSIRT Perú** (Para incidentes de ciberseguridad no	**CSIRT Perú**

		específicos de datos).	
México	**Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**	Notificación al **titular** de la información tan pronto como se detecte la vulneración si afecta su patrimonio o integridad, siguiendo las guías y recomendaciones del INAI.	**Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**
General	**GDPR (Reglamento General de Protección de Datos - UE)**	Notificación a la autoridad de control en máx. **72 horas** desde que se tiene conocimiento de la brecha. Notificación al interesado sin demora indebida si el riesgo es alto.	**Autoridades de Control de la UE** (Relevante para clientes con operaciones en la UE)

Responsabilidades

1. Asignar responsabilidades de respuesta a los incidentes a personas con las competencias necesarias. Ver documento de SLA's de Seguridad para validar los tiempos de respuesta. El contacto principal y único para reportar un incidente de seguridad para clientes y proveedores será: **seguridad@rankmi.com**.

Categorización	Priorización	Responsable de resolución
Denegación de servicio.	Alta	Head de Infraestructura CTO, Head de Seguridad en la nube
Fuga de información personal de los clientes por robo en los sistemas	Alta	Head de Operaciones CTO Head de Datos CISO
Fuga de información por parte del personal	Alta	CISO Head Finanzas Head de People & Culture
Ataques internos de malware por parte de equipos del personal	Muy crítica	CTO Head de Infraestructura CISO, Head de Seguridad en la nube, Head Finanzas Head de People & Culture
Extorsiones	Alta	CTO, CEO CISO
Suplantación de identidad de clientes	Alta	CISO, Head Finanzas, COO
Suplantación de identidad de administradores	Muy crítica	Head Finanzas Head de People & Culture, CISO, CTO
Ransomware	Muy crítica	CISO, CTO, Head de Infraestructura
Phishing	Media	Head Finanzas Head de People & Culture

		CISO, CTO
Robo de contraseñas de administradores, propietarios	Muy crítica	Head Finanzas Head de People & Culture CISO, CTO, Head de Infraestructura
Robo de contraseñas de personal	Alta	Head de People & Culture CISO, Head de Infraestructura

2. Contenido de la respuesta

Tipo de respuesta	**Detalle**
Contener	Si las consecuencias del incidente pueden extenderse, los sistemas afectados por el incidente. Recolectar evidencia tan pronto como sea posible después de la ocurrencia.

Recolectar evidencia	➔ Desarrollar y seguir procedimientos internos al tratar con evidencia relacionada con eventos de seguridad de la información con el propósito de acciones disciplinarias y legales. Se deberían considerar los requisitos de las diferentes jurisdicciones para maximizar las posibilidades de admisión en las jurisdicciones relevantes. ➔ **En Chile, según la Ley 21663.** Es importante seguir las indicaciones del marco normativo Chileno y posteriormente contrastar con las leyes de Perú y Chile. Para esto se debe contemplar lo siguiente: ◆ **Minimizar alteraciones.** Actuar rápidamente para preservar la evidencia digital sin modificarla. Esto incluye crear imágenes forenses de discos duros, memoria RAM y otros medios de almacenamiento. ◆ **Documentación exhaustiva.** Registrar cada paso tomado durante la respuesta al incidente y la recolección de evidencia, incluyendo fechas, horas, personas involucradas y herramientas utilizadas. ◆ **Aislamiento de sistemas.** Separar los sistemas o redes

	comprometidas para evitar una mayor propagación del incidente y para preservar el estado actual de la evidencia. ◆ **Uso de herramientas forenses.** Emplear software y hardware específicos para la adquisición y análisis de evidencia digital que aseguren la no alteración de los datos originales. ◆ **Resguardo seguro.** Almacenar la evidencia recolectada en un lugar seguro y controlado para evitar accesos no autorizados o daños. ➔ **En Perú, según Recomendaciones LPDP** Además de la investigación interna para comprender cómo ocurrió el incidente, se debe realizar una evaluación de impacto para identificar y mitigar riesgos futuros, como parte de los pasos a seguir frente a un incidente de seguridad de datos personales. ➔ Elementos a conservar y recolectar. Se debe crear un directorio en drive del caso compartido únicamente con los miembros del equipo legal y el equipo de gestión de incidentes. En este directorio conseguiremos:

	Registros (Logs) de sistemas: ● Logs de servidores (web, bases de datos, aplicaciones. Cloudtrail, NewReliq, GlitchTip, Rankmi Audit). ● Logs de sistemas operativos (event logs de Windows, syslog de Linux/Unix). ● Logs de dispositivos de red (firewalls, routers, switches, IDS/IPS). ● Logs de sistemas de gestión de identidades y accesos (Audits y Rankmi Audit) **Imágenes forenses:** ● Imágenes de discos duros de equipos comprometidos (servidores, estaciones de trabajo). ● Volcados de memoria RAM. ● Copias bit a bit de dispositivos móviles o de almacenamiento externo. ● Es muy **IMPORTANTE** sacar copias de los equipos y elementos comprometidos antes de realizar ninguna acción sobre ellos. Clonar nodos, servidores, bdds, etc. Al menos dos copias. Esto nos

	permitirá realizar el análisis forense posterior. **Archivos relevantes:** ● Malware (muestras de virus, ransomware, troyanos). ● Archivos de configuración modificados o sospechosos. ● Documentos y datos exfiltrados (si aplica). ● Backups del sistema afectado (antes y después del incidente). **Información de red:** ● Capturas de tráfico de red (PCAP). ● Registros de conexiones de red. **Información de usuario y autenticación:** ● Credenciales comprometidas. ● Registros de actividad de usuarios. **Documentación interna:** ● Políticas y procedimientos de seguridad de la información. ● Planes de respuesta a incidentes. ● Registros de vulnerabilidades y evaluaciones de riesgo.

	➔ Los registros están completos y no han sido manipulados de ninguna manera. Nadie debe tener acceso a modificar la información de Rankmi Audit ni de las tablas Audits. ➔ Las copias de las pruebas electrónicas probablemente sean idénticas a las originales. Totalmente comparable vs respaldos de AWS RDS. ➔ Cualquier sistema de información del que se hayan obtenido pruebas funcionaba correctamente en el momento en que se registró la prueba.
Escalada	Según sea necesario, incluidas las actividades de gestión de crisis y posiblemente invocando planes de continuidad del negocio. Se debe generar una reunión de carácter urgente con los responsables del incidente (Ver tabla arriba).
Supervisión	Garantizar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis. El encargado de seguridad hará seguimiento oportuno.
Comunicaciones a partes interesadas	Comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a todas las partes interesadas internas y externas pertinentes **(esto incluye al cliente)** siguiendo el principio de necesidad de saber. Se realiza la comunicación en

	este punto, durante las primeras horas de la detección del incidente, y luego del análisis del postmortem. Adicionalmente: **Chile**. ➔ **Reporte y Comunicación CSIRT Nacional (Ley 21663).** Es importante seguir las indicaciones del marco normativo Chileno y posteriormente contrastar con las leyes de Perú y Chile. Si la afectación es general, debemos revisar todas las regulaciones. Para esto revisar aquí a donde debemos dirigir nuestra comunicación: https://csirt.lacnic.net/csirts-de-la-region **Para Incidentes críticos.** Para incidentes de ciberseguridad con **efectos significativos** (ej. interrupción de servicio esencial, afectación a la integridad física/salud), se debe enviar una **alerta temprana** al CSIRT Nacional en un plazo máximo de **tres (3) horas** desde que se tomó conocimiento del incidente. El reporte final o la actualización de información para un "Operador de Importancia Vital" debe entregarse en un plazo máximo de

	veinticuatro (24) horas. El reporte debe omitir datos personales. ➔ **Reporte de Informe al CSIRT** Se debe generar un reporte con los detalles iniciales del incidente, este mismo debe contener, esto durante las primeras 24 horas: ● Fecha y hora del incidente. ● Descripción general del incidente y sistemas afectados. ● Acciones iniciales tomadas para contener el incidente. Posteriormente, en un plazo **máximo de 72 horas,** debe entregarse un informe completo con: ● Análisis detallado del incidente. ● Evaluación del impacto real. ● Medidas correctivas aplicadas. ● Estrategias preventivas para evitar futuras vulnerabilidades. **Perú** Reporte a la Autoridad Nacional de Protección de Datos Personales (ANPD - Perú): Si el incidente involucra datos personales, la notificación a la ANPD debe realizarse de manera inmediata y no más allá de los plazos establecidos por la normativa específica. El informe debe incluir detalles sobre lo ocurrido, los datos afectados y las medidas

	correctivas tomadas. Además, se debe informar a los afectados (clientes, empleados) lo antes posible, explicando qué datos se vieron comprometidos y qué pueden hacer para protegerse. **México** **Notificación de Vulneraciones de Datos Personales (México).** En caso de **vulneraciones** a la seguridad que afecten de forma significativa la información personal de un titular (confidencialidad, integridad o disponibilidad), se debe notificar al **titular** de la información tan pronto como sea posible, siguiendo las guías y recomendaciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Esta notificación debe permitir al titular tomar las medidas correspondientes.
Coordinación con grupos de seguridad y proveedores	Coordinar con partes internas y externas como autoridades, grupos y foros de interés externos, proveedores y clientes para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones. **IMPORTANTE**: Una vez comprendido el problema, y sobre todo en caso de violación de la privacidad, contactar a nuestro equipo legal para solicitar su

	apoyo y manejar als comunicaciones: **rgsabogados.cl**
Cierre	Una vez solucionado satisfactoriamente el incidente, cerrarlo formalmente y registrarlo;
Análisis post mortem	Realizar análisis forenses de seguridad de la información, según se requiera. Esto sobre las copias generadas en pasos anteriores.
Causa raíz	Realizar un análisis posterior al incidente para identificar la causa raíz. Asegúrese de que esté documentado y comunicado de acuerdo con los procedimientos definidos.
Identificar y tratar vulnerabilidades relacionadas	Identificar y gestionar las vulnerabilidades y debilidades de la seguridad de la información, incluidas aquellas relacionadas con los controles que han causado, contribuido o fallado en prevenir el incidente. Importante dejar una sección de las lecciones aprendidas en el informe final.

3. Definir personal capacitado y con documentación para gestionar los incidentes

Categorización	**Responsable de resolución**	**Documentación**

Denegación de servicio.	Head de Infraestructura: Franco Quijano, Head de Seguridad en la nube: Max Zeballos	https://aws.amazon.com/es/developer/application-security-performance/articles/ddos-protection/
Fuga de información personal de los clientes por robo en los sistemas	CISO: Diego Gonzalez Head People & Finance: Según el país que corresponda, Responsable Finanzas: Jesymar Capella	
Fuga de información por parte del personal	CISO: Diego Gonzalez Head People & Finance: Según el país que corresponda, Responsable Finanzas: Jesymar Capella	
Ataques internos de malware por parte de equipos del personal	CISO: Diego Gonzalez Head de Infraestructura: Franco Quijano, Head de Seguridad en la nube: Max Zeballos	https://www.avast.com/c-malware

Extorsiones	CEO: Enrique Besa, CTO: Felipe Mundaca, CISO: Diego González	
Suplantación de identidad de clientes	CISO: Diego Gonzalez, COO: Fernanda Riffo, Responsable Finanzas: Jesymar Capella	
Suplantación de identidad de administradores	CISO: Diego Gonzalez, CTO: Felipe Mundaca, Head de Infraestructura: Franco Quijano	
Ransomware	Head de Infraestructura: Franco Quijano, Head de Seguridad en la nube: Max Zeballos	https://aws.amazon.com/es/security/protecting-against-ransomware/
Phishing	CISO: Diego Gonzalez Head People & Finance: Según el país que corresponda,	

	Responsable Finanzas: Jesymar Capella	
Robo de contraseñas de administradores, propietarios	CISO: Diego Gonzalez CTO: Felipe Mundaca, Head Infraestructura: Franco Quijano	
Robo de contraseñas de personal	CISO: Diego Gonzalez Head People & Finance: Según el país que corresponda, Responsable Finanzas: Jesymar Capella	

4. Establecer un proceso para desarrollar competencias para enfrentar los incidentes

Capacitaciones sobre principales amenazas.

Categorización	**Responsable de resolución**	**Curso**
Denegación de servicio.	Head de seguridad en la nube	
Fuga de información personal de los clientes	CISO: Diego A. Gonzalez	Privacidad de la Información.

por robo en los sistemas		Taller de Ciberseguridad.
Fuga de información por parte del personal	CISO: Diego A. Gonzalez	Privacidad de la Información. Taller de Ciberseguridad.
Ataques internos de malware por parte de equipos del personal	CISO: Diego A. Gonzalez	Privacidad de la Información. Taller de Ciberseguridad.
Extorsiones		Pendiente: Manejo de Extorsiones y Suplantación
Suplantación de identidad de clientes		Pendiente: Manejo de Extorsiones y Suplantación
Suplantación de identidad de administradores		Pendiente: Manejo de Extorsiones, Robo y Suplantación
Ransomware	CISO: Diego A. Gonzalez, Head de seguridad en la nube	Taller de Ciberseguridad.
Phishing	CISO: Diego A. Gonzalez	Taller de Ciberseguridad.
Robo de contraseñas de administradores, propietarios	CISO: Diego A. Gonzalez	Pendiente: Manejo de Extorsiones, Robo y Suplantación
Robo de contraseñas de personal	CISO: Diego A. Gonzalez	Pendiente: Manejo de Extorsiones, Robo y Suplantación

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	CTO	26-02-2025
Felipe Mundaca Fernanda Rifo	CTO COO	23-06-2025

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				☑

Contactos

Lista de roles notables:

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

Términos y Definiciones

Términos	Definiciones
Autenticación multifactor	Mecanismo que permite tener más de un factor de autenticación antes de dar acceso a los sistemas
Biometría Facial	La biometría facial es una tecnología que emplea características únicas del rostro de una persona, como rasgos faciales y patrones de expresión, para identificar y verificar su identidad.

Orquestación	La orquestación en la identidad digital se refiere al proceso de coordinar y gestionar de forma centralizada diferentes servicios y tecnologías de verificación de identidad para ofrecer una experiencia fluida y segura.
Verificación de documentos de identidad	La verificación de documentos de identidad implica el análisis de documentos, como pasaportes o licencias de conducir, para verificar su autenticidad y determinar si pertenecen a la persona que los presenta.
Verificación de identidad	La verificación de identidad es el proceso de confirmar la autenticidad de la identidad de una persona. La verificación de identidad utiliza diversos métodos, como el análisis de documentos, la biometría y la autenticación multifactor, para confirmar la identidad de una persona.


rankmi