P16 Procedimiento de respuesta a incidentes

Versión 4.0 - Chile, Perú, México, Argentina y Uruguay

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
4.0	Felipe Mundaca	20-07-2026	Incorporación del marco legal de Argentina (Ley 25.326) y Uruguay (Ley 18.331 / Ley 20.212); actualización de la Matriz Legal, del proceso de recolección de evidencia y del procedimiento de notificación por país; se agrega tabla de Contactos de Emergencia para notificación de incidentes	Diego A. González	Privado

RANKMI

Chile, Perú, México, Argentina, Uruguay

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

A continuación se detalla el marco normativo de ciberseguridad y protección de datos personales aplicable en cada país donde Rankmi opera y/o presta servicios, incluyendo las obligaciones de notificación de incidentes y la autoridad competente.

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 (Agencia Nacional de Ciberseguridad)
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 (D.U. N° 007-2020 y directrices del Centro Nacional de Seguridad Digital)	Reporte a PECERT / CSIRT Perú para incidentes de ciberseguridad no específicos de datos.	PECERT - Centro Nacional de Seguridad Digital
México	Ley Federal de Protección de Datos Personales	Notificación al titular de la información tan pronto como se detecte la vulneración si afecta su patrimonio	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

País	Ley/Regulación	Obligación de Notificación de Incidentes	Autoridad Competente / Contacto Relevante
	en Posesión de los Particulares (LFPDPPP)	o integridad, siguiendo las guías y recomendaciones del INAI.	
Argentina	Ley N° 25.326 - Ley de Protección de Datos Personales ("Ley de Habeas Data") y Decreto Reglamentario N° 1558/2001	La Ley 25.326 no establece hoy un plazo legal expreso de notificación de brechas de datos personales (a diferencia de Chile/Perú/México). No obstante, en virtud del principio de responsabilidad proactiva, la AAIP recomienda notificar sin dilación indebida cuando el incidente pueda afectar significativamente los derechos de los titulares, y puede iniciar investigaciones de oficio ante filtraciones conocidas públicamente. El proyecto de actualización de la Ley 25.326 (en discusión desde 2022) incorporaría una obligación expresa de notificación.	Agencia de Acceso a la Información Pública (AAIP) - Dirección Nacional de Protección de Datos Personales
Argentina	Ciberseguridad del Sector Público Nacional (Disposición DNC N° 01/2021) y CSIRTs provinciales (ej. CSIRT-PBA)	Notificación obligatoria al CERT.ar dentro de las 48 horas de detectado el incidente para organismos del Sector Público Nacional. Para el sector privado el reporte es voluntario, pero recomendado especialmente si el incidente involucra infraestructura crítica de información.	CERT.ar - Dirección Nacional de Ciberseguridad (Jefatura de Gabinete de Ministros)
Uruguay	Ley N° 18.331 - Protección de Datos Personales y Acción de "Habeas Data", Decreto N° 414/009 y Decreto N° 64/020	Notificación obligatoria a la URCDP dentro de un plazo de 72 horas desde que se toma conocimiento de una vulneración que afecte o se sospeche que afecte datos personales (art. 4° Decreto N° 64/020), además de notificación a los titulares afectados.	Unidad Reguladora y de Control de Datos Personales (URCDP - AGESIC)
Uruguay	Ley N° 20.212, art. 78, reglamentada por el Decreto N° 66/025, art. 10	Reporte obligatorio al CERTuy dentro de las 24 horas siguientes de detectado el incidente, para entidades públicas y privadas vinculadas a servicios o sectores críticos. El resto de las organizaciones puede reportar de forma voluntaria.	CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática (AGESIC)
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
Robo de contraseñas de administradores, propietarios	Muy crítica	CISO, CTO, Head Finanzas, Head de People & Culture, Head de Infraestructura
Robo de contraseñas de personal	Alta	Head de People & Culture, CISO, Head de Infraestructura

2. Contenido de la respuesta

Contener: Si las consecuencias del incidente pueden extenderse, contener 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 (Chile, Perú, México, Argentina, Uruguay) para maximizar las posibilidades de admisión en las jurisdicciones relevantes.
- **En Chile, según la Ley 21.663.** Es importante seguir las indicaciones del marco normativo chileno y posteriormente contrastar con las leyes de los demás países donde el incidente tenga efecto. 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.
- **En Argentina, conforme a la Ley N° 25.326 y a los criterios de la AAIP.** Si bien la ley no fija un procedimiento forense específico, se recomienda mantener una cadena de custodia documentada (registro de quién accedió a la evidencia, cuándo y con qué propósito) dado que la evidencia digital puede ser utilizada en un proceso de habeas data o en una causa penal bajo el Código Procesal Penal Federal. Ante una eventual denuncia ante la AAIP o el CERT.ar, la evidencia debe permitir reconstruir la cronología del incidente y el alcance de los datos comprometidos.
- **En Uruguay, conforme a la Ley N° 18.331 y el Decreto N° 64/020.** Dado que la URCDP exige notificación dentro de 72 horas cuando se vean afectados datos personales, es crítico iniciar la recolección de evidencia (logs, imágenes forenses, alcance de los datos comprometidos) de forma inmediata, para poder cumplir con dicho plazo. Asimismo, si Rankmi calificara como entidad vinculada a un sector crítico, el reporte a CERTuy debe realizarse dentro de las 24 horas de detectado el incidente (Ley N° 20.212, art. 78 y Decreto N° 66/025, art. 10), por lo que la evidencia inicial debe estar disponible en ese mismo plazo.
- **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, NewRelic, 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 de Responsabilidades).

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, según el país afectado:

Chile

- **Reporte y Comunicación CSIRT Nacional (Ley 21.663).** Es importante seguir las indicaciones del marco normativo chileno y posteriormente contrastar con las leyes de los demás países donde el incidente tenga efecto. Si la afectación es general, debemos revisar todas las regulaciones. Directorio regional de CSIRTs: 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 (fecha y hora, descripción general y sistemas afectados, acciones iniciales tomadas) durante las primeras 24 horas. Posteriormente, en un plazo máximo de 72 horas, debe entregarse un informe completo con análisis detallado, evaluación del impacto real, medidas correctivas aplicadas y estrategias preventivas.

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 INAI. Esta notificación debe permitir al titular tomar las medidas correspondientes.

Argentina

- **Reporte y Comunicación AAIP (Ley N° 25.326).** Si bien la ley vigente no establece un plazo legal explícito de notificación de brechas, se debe notificar sin dilación indebida a la Dirección Nacional de Protección de Datos Personales de la AAIP cuando el incidente pueda afectar significativamente los derechos de los titulares de los datos, indicando la naturaleza del incidente, los datos comprometidos y las medidas correctivas adoptadas. Contacto: datospersonales@aaip.gob.ar.
- **Reporte a CERT.ar.** Para organismos del Sector Público Nacional, la notificación es obligatoria dentro de las 48 horas de detectado el incidente, indicando nivel de criticidad, clasificación del incidente y sistemas afectados, a través de reportes@cert.ar. Para el sector privado (caso de Rankmi frente a clientes argentinos), el reporte es voluntario pero recomendado, especialmente si el incidente involucra infraestructura crítica de información o afecta a múltiples organizaciones.

Uruguay

- **Reporte y Comunicación CERTuy (Ley N° 20.212, art. 78 y Decreto N° 66/025, art. 10).** Las entidades públicas y privadas vinculadas a servicios o sectores críticos deben reportar al CERTuy dentro de las 24 horas siguientes de detectado el incidente. El resto de las organizaciones puede reportar de forma voluntaria. Vías de reporte: formulario web en gub.uy, correo a cert@cert.uy, o línea de urgencia (+598) 150 2378 (atención 24/7). El reporte debe enviarse sin alterar la evidencia y conservando el sistema en las condiciones en que se encontraba al detectar el incidente, salvo que sea necesario tomar medidas urgentes de contención.
- **Reporte a la URCDP (Decreto N° 64/020, art. 4°).** En los incidentes en que se identifique o se sospeche la afectación de datos personales, se debe denunciar ante la URCDP dentro de un plazo de 72 horas desde que se toma conocimiento de la vulneración, además de notificar a los titulares de datos afectados.
- **Dirección General de Cibercrimen (Policía Nacional).** Ante la identificación de un posible delito informático, corresponde presentar una denuncia para iniciar la investigación judicial correspondiente. Contacto: dipn-cibercrimen@minterior.gub.uy / (+598) 2030 4625.

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 las 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.

Tabla de Contactos de Emergencia para Notificación de Incidentes

Directorio de contactos oficiales (autoridades de ciberseguridad y de protección de datos personales) y de apoyo interno de Rankmi, a utilizar para cumplir con las obligaciones de notificación en cada jurisdicción descritas en la Matriz Legal.

País	Organismo	Tipo	Canal de contacto	Plazo de notificación
Chile	CSIRT Nacional (Agencia Nacional de Ciberseguridad, ANCI)	Ciberseguridad	Portal: csirt.gob.cl/reportar | Tel: 1510 / +56 44 77 111 31	3 h (alerta temprana) / 24 h (reporte final) - OIV
Chile	Consejo para la Transparencia (transitorio, protección de datos)	Datos personales	www.consejotransparencia.cl	Notificación sin demora indebida al titular
Perú	PECERT - Centro Nacional de Seguridad Digital	Ciberseguridad	www.gob.pe/14084 (reporte digital)	Inmediato / según criticidad
Perú	Autoridad Nacional de Protección de Datos Personales (ANPD - MINJUSDH)	Datos personales	protegetusdatos@minjus.gob.pe	Inmediato, conforme normativa específica
México	INAI - Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	Datos personales	www.inai.org.mx	Tan pronto se detecte la vulneración
Argentina	AAIP - Agencia de Acceso a la Información Pública	Datos personales	datospersonales@aaip.gob.ar | www.argentina.gob.ar/aaip	Sin dilación indebida (buena práctica; sin plazo legal expreso vigente)
Argentina	CERT.ar - Dirección Nacional de Ciberseguridad	Ciberseguridad	reportes@cert.ar | www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/centro-nacional-de-ciberseguridad/certar	48 h (obligatorio Sector Público Nacional; voluntario privados)
Uruguay	CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática (AGESIC)	Ciberseguridad	cert@cert.uy | Tel: (+598) 150 2378 (24/7) | Formulario: gub.uy/certuy	24 h - entidades vinculadas a servicios/sectores críticos
Uruguay	URCDP - Unidad Reguladora y de Control de Datos Personales	Datos personales	Trámite vía gub.uy - denuncias URCDP	72 h desde conocimiento de la vulneración (Decreto 64/020, art. 4°)
Uruguay	Dirección General de Cibercrimen (Policía Nacional)	Denuncia penal	dipn-cibercrimen@minterior.gub.uy | Tel: (+598) 2030 4625	Ante identificación de delito informático
Regional / LACNIC	Directorio de CSIRTs de la región	Ciberseguridad	https://csirt.lacnic.net/csirts-de-la-region	Según el país de afectación
Rankmi (interno)	Equipo de Seguridad de la Información	Canal único cliente/proveedor	seguridad@rankmi.com	Según SLA's de Seguridad vigentes
Rankmi (interno)	Asesoría legal externa	Apoyo legal / comunicaciones	rgsabogados.cl	Al identificar afectación de privacidad

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.	
Fuga de información por parte del personal	CISO: Diego Gonzalez, Head People & Finance: según el país que corresponda, Responsable Finanzas.	
Ataques internos de malware por parte de equipos del personal	CISO: Diego Gonzalez, Head de Infraestructura: Franco Quijano, Head de Seguridad en la nube.	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.	
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.	https://aws.amazon.com/es/security/protecting-against-ransomware/
Phishing	CISO: Diego Gonzalez, Head People & Finance: según el país que corresponda, Responsable Finanzas.	
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.	

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 por robo en los sistemas	CISO: Diego A. Gonzalez	Privacidad de la Información. 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

Categorización	Responsable de resolución	Curso
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 son:

Nombre	Cargo	Fecha de Revisión
Felipe Mundaca	CTO	26-02-2025
Felipe Mundaca / Fernanda Riffo	CTO / COO	23-06-2025
Felipe Mundaca / Fernanda Riffo	CTO / COO	20-07-2026

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.
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.

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	Tecnología que emplea características únicas del rostro de una persona, como rasgos faciales y patrones de expresión, para identificar y verificar su identidad.
Orquestación	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	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	Proceso de confirmar la autenticidad de la identidad de una persona, utilizando métodos como el análisis de documentos, la biometría y la autenticación multifactor.
AAIP	Agencia de Acceso a la Información Pública. Autoridad de control de la Ley N° 25.326 de Protección de Datos Personales de Argentina.
CERT.ar	Equipo de Respuesta ante Emergencias Informáticas del Sector Público Nacional de Argentina.
URCDP	Unidad Reguladora y de Control de Datos Personales de Uruguay, autoridad de control de la Ley N° 18.331.
CERTuy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (AGESIC).