POLÍTICA DE RETENCIÓN Y BORRADO SEGURO DE DATOS DE CLIENTES AL FIN DE CONTRATO

Código del Documento	RKM-PRO-Borrado_Datos_Clientes
Versión	1.0
Fecha de Emisión	Mayo 2026
Clasificación	Público
Autor	Diego González
Aprobado por	Felipe Mundaca

Information Security Manager — Rankmi SAS

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor
1.0	Felipe Mundaca	Mayo 2026	Creación del documento	Diego González

Responsable de actualizar y revisar el documento	Information Security Manager (CISO)

1. Introducción

Rankmi es una plataforma SaaS de Gestión del Talento Humano, certificada bajo las normas **ISO 27001, ISO 27701 e ISO 37001**, que presta servicios a medianas y grandes empresas en Chile, México, Colombia y Perú. En su rol de **Encargado del Tratamiento de Datos Personales** (conforme a la Ley N°21.719 de Chile, GDPR/UE y legislaciones equivalentes de LATAM), Rankmi procesa datos de los trabajadores de sus empresas clientes en nombre de dichas empresas, quienes actúan como Responsables del Tratamiento.

El presente documento establece la postura oficial de Rankmi respecto a la retención, inactivación y borrado seguro de los datos personales e información de las empresas cliente una vez que la relación contractual finaliza. Asimismo, define el protocolo detallado para gestionar la Solicitud de Borrado Total de Información, adaptado expresamente a los requerimientos de la nueva Ley de Protección de Datos Personales de Chile (Ley N°21.719, vigente 2026) y a la Ley Marco de Ciberseguridad (Ley N°21.663, vigente 2024).

2. Marco Legal Aplicable

Esta política da cumplimiento al siguiente marco normativo:

Normativa	Descripción y Relevancia
Ley N°21.719 (Chile, 2026)	Nueva Ley de Protección de Datos Personales. Reconoce el derecho de supresión de datos, establece plazos de respuesta, obliga al borrado efectivo y documentado, y define sanciones por incumplimiento.
Ley N°21.663 (Chile, 2024)	Ley Marco de Ciberseguridad. Exige a los operadores de servicios esenciales y prestadores de TI implementar controles de seguridad para la protección y eliminación segura de datos.
Ley N°19.628 (Chile)	Ley de Protección de la Vida Privada (vigente en tanto no sea derogada). Base legal preexistente para el tratamiento de datos personales.
GDPR / UE	Reglamento General de Protección de Datos. Aplica a clientes con operaciones en el Espacio Económico Europeo o que manejen datos de ciudadanos europeos.
LFPDPPP (México)	Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Aplica a clientes en México.
Ley 1581 (Colombia)	Ley de Protección de Datos Personales. Aplica a clientes en Colombia.
Ley N°29733 (Perú)	Ley de Protección de Datos Personales. Aplica a clientes en Perú.
ISO 27001 / ISO 27701	Normas internacionales de seguridad de la información y privacidad. Rankmi mantiene certificación activa bajo ambas normas.

3. Alcance y Partes Involucradas

Esta política aplica a:

- **Empresas cliente (Responsables del Tratamiento):** Organizaciones que contratan los servicios SaaS de Rankmi y cuyos trabajadores son los titulares de los datos personales procesados en la plataforma.
- **Rankmi (Encargado del Tratamiento):** Actúa exclusivamente bajo instrucción del cliente. No toma decisiones autónomas sobre los datos personales de los trabajadores del cliente.
- **Titulares de Datos (Trabajadores):** Para el ejercicio de derechos ARCO (Acceso, Rectificación, Cancelación, Oposición/Supresión), los trabajadores deben dirigirse en primera instancia al administrador de la plataforma designado por su empleador (empresa cliente). Rankmi atenderá solicitudes directas solo si el contrato con el cliente así lo prevé expresamente.

Importante: Rankmi opera bajo el modelo de responsabilidad compartida. La empresa cliente es responsable de la correcta administración de accesos y del ejercicio de derechos de sus trabajadores dentro de la plataforma mientras el contrato esté vigente.

4. Política de Retención de Datos Post-Contractual

4.1 Período de Retención en Modo Inactivo

Una vez finalizada la relación contractual entre Rankmi y la empresa cliente (por vencimiento de contrato, no renovación, resolución anticipada u otra causa), los datos del cliente —incluyendo datos personales de sus trabajadores, configuraciones, resultados de evaluaciones, registros de nómina y cualquier otro dato vinculado— serán:

- **Inactivados de forma inmediata:** Los datos dejarán de ser accesibles desde la interfaz de la plataforma y estarán en estado no operativo.
- **Retenidos en bases de datos inactivas:** Se conservarán por un período máximo de **7 años calendario** desde la fecha de terminación del contrato.

Fundamento Legal: El plazo de 7 años se justifica por las obligaciones legales de retención documental aplicables en Chile (Código del Trabajo, legislación tributaria, Ley N°21.719 Art. 17 que reconoce excepciones al borrado por obligación legal), así como por requerimientos similares en las demás jurisdicciones LATAM donde opera Rankmi. Este plazo permite atender eventuales requerimientos regulatorios, fiscales, laborales o judiciales.

4.2 Tipos de Datos Retenidos

Categoría de Datos	Descripción	Período de Retención
Datos de identificación de trabajadores	Nombres, RUT/cédula, correo electrónico, datos demográficos	7 años (modo inactivo)
Datos de nómina y remuneraciones	Liquidaciones de sueldo, bonos, descuentos, contratos	7 años (obligación legal Código del Trabajo/normativa tributaria)
Datos de desempeño	Evaluaciones, objetivos, feedbacks, calibraciones	7 años (modo inactivo)

Categoría de Datos	Descripción	Período de Retención
Datos de selección (ATS)	CVs, resultados de pruebas, entrevistas grabadas	7 años (modo inactivo)
Logs de auditoría y seguridad	Registros de acceso, cambios, eventos de seguridad (pgAudit, Teleport)	7 años (requisito ISO 27001 / Ley Ciberseguridad)
Archivos adjuntos (S3)	Documentos de contratos, certificados, evidencias	7 años (modo inactivo)
Datos de caché y sesiones	Tokens, sesiones, caché operacional	Eliminados inmediatamente al cierre del contrato

5. Solicitud de Borrado Total de Información

5.1 Descripción del Derecho

La empresa cliente, en su calidad de Responsable del Tratamiento, tiene derecho a solicitar el **borrado total, definitivo e irreversible** de todos los datos asociados a su organización y a los trabajadores de esta, en cualquier momento. Este derecho se enmarca en el **Artículo 17 de la Ley N°21.719** (derecho de supresión), así como en el Artículo 17 del GDPR y normativas equivalentes.

Rankmi reconoce este derecho sin restricciones salvo en los casos contemplados por la ley, como: (a) existencia de obligación legal de retención vigente; (b) necesidad de establecer, ejercer o defender una acción legal; o (c) interés público que exija la conservación. En dichos casos, Rankmi comunicará por escrito al solicitante el motivo de la imposibilidad o restricción parcial del borrado.

5.2 Procedimiento de Solicitud

El proceso para solicitar el Borrado Total de Información es el siguiente:

Paso	Responsable	Actividad	Plazo
1	Empresa Cliente	Descarga y completa el formulario «Solicitud de Borrado Total de Información» (RKM-FORM-Borrado_Total_v1.0). Debe completar las secciones 1 a 5 del formulario: identificación, representación legal, motivo de supresión, alcance de datos y declaración.	—
2	Empresa Cliente	Adjunta prueba de identidad del representante legal (pasaporte, cédula de identidad, o documento equivalente) y, si corresponde, prueba de identidad empresarial (RUT, RUC, RFC, CUIT).	—
3	Empresa Cliente	Envía el formulario firmado (firma electrónica avanzada o firma manuscrita escaneada) a: seguridad@rankmi.com con asunto «Solicitud Borrado Total – [Nombre Empresa]».	—
4	Rankmi – CISO	Acusa recibo de la solicitud y verifica la identidad del solicitante. Si faltan antecedentes, notifica al	24 horas hábiles

Paso	Responsable	Actividad	Plazo
		cliente para que los subsane dentro de 5 días hábiles. El plazo SLA comienza a correr desde la recepción completa y verificada.	
5	Rankmi – Ops / DBAs	Ejecuta el borrado físico (DELETE) en las bases de datos de producción (RDS PostgreSQL / AuroraDB) y en los servicios de almacenamiento de archivos (S3). Emite evidencia técnica del borrado (logs de ejecución firmados digitalmente).	15 días hábiles
6	Rankmi – Ops / DBAs	Invalida y purga los backups que contengan datos del cliente. Los ciclos de rotación de backups garantizan la eliminación completa dentro del plazo definido.	20 días calendario adicionales (35 días calendario totales desde confirmación)
7	Rankmi – CISO	Emite y entrega al cliente un «Certificado de Borrado Total» que incluye: fecha de ejecución, hash de los registros eliminados, sistemas afectados y nombre del responsable técnico que ejecutó el borrado.	Al término del paso 6

5.3 SLAs del Borrado Total

Etapa del Borrado	Plazo Máximo	Observaciones
Acuse de recibo y verificación de identidad	24 horas hábiles desde recepción	Si faltan documentos, el plazo se suspende hasta recibir la información completa (máx. 5 días hábiles para subsanar).
Borrado en bases de datos de producción (RDS/AuroraDB/S3)	15 días hábiles desde confirmación de solicitud completa	Aplica a datos de producción: PostgreSQL (RDS), AuroraDB, S3. Se emite evidencia técnica al finalizar.
Borrado en backups y logs archivados	20 días calendario adicionales	Los backups son eliminados conforme a los ciclos de rotación programados. Plazo máximo total: 35 días calendario.
Emisión del Certificado de Borrado Total	Al término del borrado en backups	Documento firmado digitalmente por el CISO de Rankmi que certifica el borrado irreversible.

Alineamiento con Ley N°21.719: El plazo total de 35 días calendario para el borrado completo (incluyendo backups) es compatible con el plazo de 30 días establecido en la Ley N°21.719 para dar respuesta a solicitudes de supresión, dado que la Ley reconoce que el borrado en sistemas de respaldo puede requerir un tiempo técnico adicional, siempre que el responsable/encargado acredite la ejecución iniciada dentro del plazo legal y notifique al solicitante.

6. Postura de Rankmi frente a la Ley N°21.719 y la Ley N°21.663

6.1 Rankmi como Encargado del Tratamiento

Rankmi actúa en todo momento como Encargado del Tratamiento (Processor), no como Responsable (Controller) de los datos de los trabajadores de sus clientes. En consecuencia:

- Rankmi no utiliza los datos de los trabajadores para fines propios, salvo los expresamente autorizados en el contrato de servicio y en la Política de Privacidad (e.g., mejora del servicio con datos anonimizados, análisis estadísticos disociados).
- Rankmi no cede ni vende datos de trabajadores a terceros con fines comerciales.
- Rankmi implementa medidas técnicas y organizativas certificadas bajo ISO 27001 e ISO 27701 para garantizar la confidencialidad, integridad y disponibilidad de los datos.
- Rankmi asiste al cliente (Responsable) en el cumplimiento de sus obligaciones frente a los titulares de datos, incluyendo el ejercicio de derechos ARCO.

6.2 Cumplimiento con la Ley N°21.719 de Chile

La nueva Ley de Protección de Datos Personales de Chile (N°21.719, vigente en 2026) introduce cambios significativos respecto de la Ley N°19.628. A continuación se detalla cómo el protocolo de Rankmi cumple con sus exigencias:

Exigencia Ley N°21.719	Cómo Rankmi da cumplimiento
Derecho de supresión (Art. 17): el titular puede exigir borrado al término de la relación contractual.	El protocolo de Borrado Total de Rankmi permite el borrado definitivo de todos los datos al término del contrato, previa solicitud formal.
Plazo de respuesta: máximo 30 días corridos para atender solicitudes.	Rankmi acusa recibo en 24 horas hábiles e inicia el borrado en producción en 15 días hábiles. Entrega el certificado antes de los 35 días calendario totales.
Excepciones al borrado: obligaciones legales de retención.	Rankmi informa al cliente si aplica alguna excepción y los datos no pueden ser borrados en su totalidad (e.g., obligaciones laborales o tributarias).
Consentimiento informado y base de legitimación.	La firma del contrato de servicio constituye la base de legitimación para el tratamiento de datos. Rankmi no trata datos sin instrucción del Responsable.
Transferencias internacionales de datos.	Documentadas en el Análisis de Impacto de Transferencia (TIA) con uso de AWS Oregon/Virginia y Cláusulas Contractuales Tipo (SCCs). Ver Centro de Confianza.
Obligación de notificar brechas.	Rankmi cuenta con procedimiento de gestión de incidentes de seguridad (RKM-PRO-Incidentes) con SLA de notificación alineado a la Ley N°21.663 (72 horas a la ANCI).
Registro de Tratamientos.	Rankmi mantiene un Registro de Actividades de Tratamiento (RAT) actualizado conforme a ISO 27701, disponible para auditoría.

6.3 Cumplimiento con la Ley Marco de Ciberseguridad (N°21.663)

La Ley N°21.663 establece obligaciones para operadores de servicios esenciales y prestadores de servicios de TI. Rankmi, como plataforma SaaS que procesa datos de talento humano de grandes empresas, se sujeta a las siguientes disposiciones:

- **Medidas de seguridad activas:** Rankmi implementa controles técnicos de cifrado (AES-256 en reposo, TLS 1.3+ en tránsito), segmentación de redes en AWS, monitoreo continuo con alertas, gestión de vulnerabilidades y pruebas de penetración anuales.
- **Borrado seguro en el ciclo de vida del dato:** El borrado físico (DELETE) con evidencia técnica es parte del proceso estándar de baja de cliente, cumpliendo el principio de minimización y destrucción segura de datos establecido por la Ley.
- **Notificación de incidentes:** El proceso de respuesta a incidentes de Rankmi (RKM-PRO-Incidentes) incluye la notificación a la Agencia Nacional de Ciberseguridad (ANCI) dentro de las 72 horas de confirmado un incidente que afecte datos de clientes.
- **Auditoría y trazabilidad:** Rankmi mantiene logs de auditoría con pgAudit y Teleport, garantizando la trazabilidad de todas las operaciones sobre datos, incluidas las de borrado.

7. Exportación y Descarga de Datos por el Cliente

Antes de la terminación del contrato y del proceso de borrado, Rankmi recomienda y facilita al cliente la exportación de su información mediante:

- **Panel de administración (autogestión):** El administrador del cliente puede descargar reportes, exportar datos en formato CSV/Excel y generar copias de seguridad de su información desde el panel de administración de la plataforma.
- **Asistencia del equipo Rankmi:** Previa coordinación con el PM asignado, el equipo de Rankmi puede facilitar la exportación de datos en formatos estructurados para su migración a otro sistema.
- **Plazo sugerido para descarga:** Se recomienda que el cliente realice la exportación de sus datos durante los **30 días previos** a la fecha de baja o antes de presentar la solicitud de Borrado Total.

Nota: Una vez ejecutado el Borrado Total de Información, la acción es irreversible. Rankmi no podrá recuperar ningún dato eliminado ni emitir reportes sobre información ya borrada. Es responsabilidad del cliente asegurarse de haber descargado toda la información que necesite con anterioridad.

8. Excepciones al Borrado Total

Rankmi podrá retener ciertos datos, de forma parcial o total, incluso ante una Solicitud de Borrado Total, en los siguientes casos contemplados por la ley:

- **Obligación legal vigente:** Cuando la normativa laboral, tributaria, de seguridad social o regulatoria del país del cliente exija la conservación de ciertos datos por un período determinado (e.g., liquidaciones de sueldo por 5 años en Chile según el Código del Trabajo).
- **Procedimiento judicial o administrativo activo:** Cuando los datos sean necesarios para la defensa de derechos en un procedimiento judicial, arbitral o administrativo vigente en que Rankmi sea parte.
- **Requerimiento de autoridad competente:** Cuando una autoridad regulatoria, judicial o de ciberseguridad requiera la preservación de datos como evidencia en el marco de una investigación.
- **Logs de seguridad con valor forense:** Los registros de auditoría de seguridad (pgAudit, Teleport) podrán conservarse durante el plazo de retención estándar aun cuando se ejecute

el borrado de datos de negocio, dado su valor como evidencia ante posibles incidentes de seguridad.

En todos los casos de excepción, Rankmi notificará por escrito al cliente dentro de los 5 días hábiles siguientes a la recepción de la solicitud, indicando: el fundamento legal de la excepción, el alcance de los datos retenidos y el plazo estimado de retención.

9. Evidencia y Certificación del Borrado

Al término del proceso de Borrado Total, Rankmi emitirá un Certificado de Borrado Total que contendrá:

- Identificación del cliente y número de solicitud.
- Fecha de inicio y término de la ejecución del borrado.
- Sistemas y bases de datos afectados (producción y backups).
- Metodología de borrado aplicada (DELETE físico en RDBMS, purga de ciclos de backup, eliminación de objetos S3).
- Hash o resumen criptográfico de los registros de ejecución como evidencia de integridad.
- Nombre y firma del responsable técnico (DBA / DevOps) que ejecutó el borrado.
- Nombre y firma del CISO de Rankmi en carácter de certificante.
- Declaración de que el borrado es completo, definitivo e irreversible.

Este certificado tiene valor probatorio ante la Agencia de Protección de Datos Personales (APDP) de Chile y ante las autoridades regulatorias de las demás jurisdicciones LATAM en que opera Rankmi.

10. Roles y Responsabilidades

Rol	Responsabilidades
CISO (Information Security Manager)	Gestionar, aprobar y supervisar el proceso de Borrado Total. Emitir el Certificado de Borrado. Actualizar esta política anualmente o ante cambios legales.
Equipo de Operaciones / DBAs	Ejecutar técnicamente el borrado en producción y backups. Generar evidencia técnica de ejecución.
PM / Customer Success	Recibir la notificación de baja del cliente y coordinar con el cliente la descarga previa de datos. Derivar la solicitud de borrado al CISO.
Legal / Compliance	Verificar si aplica alguna excepción legal al borrado. Notificar al cliente en caso de excepción.
Empresa Cliente (Responsable)	Completar y firmar el formulario de Solicitud de Borrado Total. Asegurarse de haber descargado previamente la información necesaria.

11. Matriz RACI

Actividad	Responsable	Aprobador	Consultado	Informado
Recepción y verificación de solicitud	CISO	CISO	Legal	PM / CS
Ejecución borrado en producción	DBAs / Ops	CISO	—	PM / CS
Purga de backups	DBAs / Ops	CISO	—	—
Aplicación de excepción legal	Legal	CISO	Comité Directivo	Cliente
Emisión Certificado de Borrado	CISO	CISO	DBAs / Ops	Cliente
Revisión anual de política	CISO	Comité Directivo	Legal / Compliance	Comité Operativo

12. Contacto

Rol	Nombre	Teléfono	Email
CISO / Information Security Manager	Diego González	+593 998 981 436	seguridad@rankmi.com
Consultas Privacidad / DPA	Área de Seguridad Rankmi	—	seguridad@rankmi.com

13. Aprobación y Revisión

Nombre	Cargo	Fecha de Revisión
Felipe Mundaca	CTO	Mayo 2026
Fernanda Rifo	COO	Mayo 2026
Diego González	CISO / Information Security Manager	Mayo 2026

Este documento es revisado anualmente o ante cambios en la legislación aplicable. La versión vigente se encuentra disponible en el **Centro de Confianza y Cumplimiento de Rankmi** en: rankmi.com/es/centro-de-confianza-y-cumplimiento-de-rankmi