# Mapeo de Datos y Creación del RAT bajo la Ley 21.719: Guía Práctica Avanzada para el DPO

## Introducción: El Registro de Actividades de Tratamiento como Piedra Angular de la Responsabilidad Proactiva

El Registro de Actividades de Tratamiento (RAT), más que una simple obligación documental impuesta por la Ley N° 21.719, constituye la piedra angular de todo el sistema de cumplimiento.1 Es la materialización del principio de responsabilidad proactiva o

*accountability*, un pilar fundamental de la nueva normativa chilena que exige a las organizaciones no solo cumplir con la ley, sino también ser capaces de demostrar dicho cumplimiento en todo momento.2 Sin un conocimiento claro, granular y actualizado de qué datos personales se tratan, dónde residen, por qué se tratan, cómo fluyen y cuándo deben ser eliminados, es logísticamente imposible garantizar el respeto a los demás principios rectores como la licitud, finalidad y proporcionalidad.1

Este curso posiciona al RAT no como una carga administrativa, sino como un activo estratégico de gobernanza de datos. Un RAT bien construido trasciende el cumplimiento legal para convertirse en una herramienta que permite a la organización comprender sus activos de información, gestionar riesgos de manera proactiva, optimizar procesos de negocio y, fundamentalmente, construir una relación de confianza con sus clientes, lo cual representa una ventaja competitiva tangible en la economía digital.3

En este contexto, el Delegado de Protección de Datos (DPO) asume un rol de liderazgo y orquestación. El DPO no es quien crea el RAT en solitario desde su escritorio; es el director de un equipo multidisciplinario que, a través de una metodología rigurosa, levanta, documenta y mantiene este inventario.1 Esta labor exige una combinación única de conocimiento legal, entendimiento de procesos de negocio, habilidades de comunicación y competencia técnica.

La perspectiva fundamental que guiará este curso es que el RAT debe ser concebido como la "única fuente de verdad" (*Single Source of Truth*) para todas las operaciones de privacidad de la organización. Obligaciones críticas como responder a las solicitudes de derechos de los titulares en los plazos estipulados 9, notificar violaciones de seguridad a la autoridad y a los afectados 12, o realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) 5, dependen de un conocimiento rápido y preciso del universo de datos de la empresa. Sin un registro centralizado y fiable, cada una de estas tareas se convierte en un ejercicio de investigación

*ad-hoc*, lento, propenso a errores y costoso. Por lo tanto, el RAT no es solo un registro *para* la autoridad fiscalizadora, sino un sistema de información crítico *para* la propia organización, transformando una obligación de cumplimiento en una inversión estratégica en resiliencia y eficiencia operativa.

## Módulo 1: Planificación y Metodología del Mapeo de Datos (Data Discovery)

El éxito de un proyecto de mapeo de datos reside en una planificación meticulosa y en la adopción de una metodología que vaya más allá de lo superficial. Este módulo sienta las bases para un levantamiento de información eficaz y exhaustivo.

### Fase 1: Conformación del Equipo de Trabajo Multidisciplinario

El primer paso, liderado por el DPO, es la conformación de un equipo de trabajo que represente a todas las áreas clave de la organización que tratan datos personales. Este equipo debe incluir, como mínimo, a representantes de Recursos Humanos, Finanzas, Marketing, Ventas, Operaciones, Tecnologías de la Información (TI) y Legal.1 La inclusión de estos actores es crucial no solo porque son la fuente primaria de información sobre los tratamientos de datos, sino porque su participación temprana fomenta la aceptación del programa de privacidad en toda la empresa y los convierte en agentes de cambio en sus respectivas áreas.3

### Fase 2: El Cambio de Paradigma Metodológico

La metodología de levantamiento es el factor más determinante para la calidad del RAT. El enfoque tradicional, centrado en la tecnología, consiste en preguntar a los departamentos "¿qué bases de datos tienen?". Este enfoque es inherentemente limitado y está destinado al fracaso. La Ley 21.719 regula el "tratamiento" de datos, no solo las bases de datos. Por ello, el curso adopta el cambio de paradigma propuesto en la documentación base: el foco debe estar en los procesos de negocio.1 La pregunta clave debe ser:

**"¿qué actividades o procesos realizan que involucren información de personas?"**.

Este enfoque centrado en procesos es superior porque permite descubrir tratamientos de datos que ocurren fuera de los sistemas corporativos tradicionales. Permite identificar:

* **Datos no estructurados**: Información personal contenida en hojas de cálculo de Excel, documentos de Word, presentaciones y correos electrónicos.
* **Shadow IT**: Aplicaciones en la nube (SaaS) contratadas directamente por un departamento sin la supervisión de TI, que pueden estar almacenando grandes volúmenes de datos personales.
* **Procesos manuales**: Actividades que involucran papel, como la recepción de currículums impresos o formularios de inscripción en eventos.
* **Flujos de datos implícitos**: Transferencias de información entre sistemas o hacia terceros que no están formalmente documentadas en la arquitectura de TI.

### Fase 3: Diseño de la Estrategia de Entrevistas

Con el equipo conformado y la metodología definida, el siguiente paso es planificar la ejecución:

1. **Inventario de Procesos**: Crear un listado inicial de los procesos de negocio clave de la organización (ej. "Reclutamiento y Selección", "Gestión de Nómina", "Facturación y Cobranza", "Marketing Digital", "Atención al Cliente").
2. **Identificación de Dueños de Proceso**: Para cada proceso, identificar al "dueño del proceso" (*Process Owner*), que es la persona con el conocimiento más profundo sobre cómo funciona esa actividad en el día a día.
3. **Plan de Comunicación**: Preparar un paquete de comunicación claro y conciso para los dueños de proceso. Este debe explicar el propósito del proyecto de mapeo, su obligatoriedad bajo la Ley 21.719, los beneficios para su área (como la identificación de ineficiencias o riesgos) y qué se espera de ellos durante la entrevista.

#### Herramienta Práctica 1: Plantilla de Plan de Proyecto de Mapeo de Datos

Se proporciona un documento editable (formato Word o Project) que sirve como hoja de ruta para el DPO. Incluye secciones para definir objetivos, alcance, conformación del equipo del proyecto con roles y responsabilidades detallados, un cronograma de entrevistas, el plan de comunicación y métricas de éxito (ej. porcentaje de procesos mapeados).

#### Herramienta Práctica 2: Modelo de Cuestionario Pre-Entrevista

Para optimizar el tiempo de las reuniones, se entrega una plantilla de formulario online (ej. Microsoft Forms, Google Forms). Este cuestionario se envía a los dueños de proceso antes de la entrevista para recopilar información básica como el nombre del proceso, los principales sistemas o aplicaciones que utiliza, los tipos generales de personas sobre los que se trata información (clientes, empleados, proveedores) y los principales departamentos con los que interactúa. Esto permite que la entrevista se enfoque directamente en los detalles del flujo de datos y los elementos del RAT.

### Ejercicio Práctico del Módulo 1

* **Escenario**: El participante asume el rol de DPO en una empresa de retail de tamaño mediano.
* **Tarea**: Se le pide que seleccione el departamento de Marketing y, utilizando la **Plantilla de Plan de Proyecto**, realice las siguientes acciones:
  1. Identificar y listar al menos cinco procesos de negocio que probablemente traten datos personales (ej. "Gestión de Programa de Lealtad", "Campañas de Email Marketing", "Análisis de Comportamiento de Clientes en E-commerce", "Gestión de Redes Sociales y Sorteos", "Atención de Reclamos Post-Venta").
  2. Asignar roles hipotéticos (ej. "Gerente de Fidelización", "Jefe de Marketing Digital") como dueños de proceso para cada actividad listada.
  3. Redactar un borrador del correo electrónico de comunicación inicial que se enviaría a estos dueños de proceso, explicando el proyecto y solicitando su colaboración para agendar una entrevista.

## Módulo 2: La Entrevista de Mapeo: Técnicas y Documentación en Vivo

La entrevista con el dueño del proceso es el momento de la verdad en el mapeo de datos. Es donde la teoría se encuentra con la realidad operativa. Este módulo dota al DPO de las técnicas y herramientas para conducir entrevistas productivas y capturar la información necesaria de manera eficiente.

### Estructura de la Entrevista

Una entrevista de mapeo exitosa sigue una estructura lógica:

1. **Introducción y Contexto**: Iniciar reafirmando el propósito de la reunión, el marco de confidencialidad y el objetivo de entender el proceso desde la perspectiva del entrevistado.
2. **Mapeo del Proceso de Negocio**: Solicitar al dueño del proceso que describa la actividad de principio a fin, como si se lo estuviera explicando a un nuevo miembro de su equipo. Es vital que el DPO escuche activamente y utilice un diagrama de flujo simple o notas para visualizar el proceso.
3. **Identificación de Puntos de Contacto con Datos**: En cada paso del flujo descrito, el DPO debe intervenir con preguntas clave: "¿En este punto, qué información de personas se recoge, se crea, se utiliza, se modifica, se consulta o se comparte?".
4. **Profundización en los Elementos del RAT**: Una vez identificado un punto de contacto con datos, el DPO utiliza el flujo del proceso como guía para completar sistemáticamente los campos requeridos por el RAT, transformando la narrativa del proceso en un registro estructurado.

### Técnicas de Interrogación Avanzadas

El DPO debe actuar como un investigador, utilizando preguntas abiertas y de sondeo para descubrir detalles que el entrevistado podría pasar por alto. Utilizando el ejemplo de RRHH de la documentación base 1 como modelo, se pueden desarrollar guiones para otras áreas:

* **Finanzas (Proceso de Cobranza)**: "¿Cuál es el flujo completo desde que una factura vence hasta que se recupera el pago? ¿Qué datos del deudor utilizan para contactarlo? ¿Utilizan sistemas de enriquecimiento de datos para encontrar nueva información de contacto? ¿En qué punto y bajo qué criterios se decide compartir la información de la deuda con una agencia de cobranza externa? ¿Qué base legal ampara esa cesión de datos?".
* **Marketing (Programa de Lealtad)**: "¿Qué datos se solicitan al cliente para inscribirse en el programa? ¿Cómo se utiliza el historial de compras para personalizar ofertas y comunicaciones? ¿Se crean perfiles o segmentos de clientes basados en su comportamiento? ¿Qué base de licitud se utiliza para esta actividad de perfilamiento? ¿Se comparten estos perfiles con algún socio comercial?".

### Gestión de la Entrevista

* **Mantener el Foco**: Es común que las conversaciones se desvíen. El DPO debe guiar amablemente la entrevista de vuelta al flujo del proceso y al tratamiento de datos.
* **Manejar la Incertidumbre**: A menudo, el dueño del proceso no tendrá todas las respuestas, especialmente las técnicas (ej. "No sé en qué servidor se guarda eso"). La tarea del DPO es registrar la pregunta y asignarla a la persona correcta (generalmente de TI) para su posterior seguimiento.
* **Validación Activa**: Es fundamental parafrasear y resumir para asegurar la comprensión. Por ejemplo: "Para confirmar, lo que entiendo es que los datos del formulario web viajan directamente al sistema CRM, y desde allí, una vez por noche, un proceso automático envía el nombre y el correo electrónico a nuestro proveedor de email marketing. ¿Es eso correcto?".

#### Herramienta Práctica 3: Guion Estructurado de Entrevista para el Mapeo

Se proporciona un documento guía que no es un script rígido para ser leído, sino un marco de referencia. Contiene las fases de la entrevista, preguntas clave asociadas a cada campo del RAT, ejemplos de sondeo para distintas situaciones y consejos prácticos para el entrevistador sobre cómo documentar las respuestas en tiempo real.

### Ejercicio Práctico del Módulo 2

* **Escenario**: Continuando con el caso de la empresa de retail, el participante es el DPO y se le proporciona un breve perfil del "Gerente de Fidelización", quien es el dueño del proceso "Gestión de Programa de Lealtad".
* **Tarea**: Se solicita al participante que realice un ejercicio de *role-playing* (puede ser un documento escrito que simule el diálogo). Utilizando el **Guion Estructurado de Entrevista**, el participante debe formular las preguntas necesarias al Gerente de Fidelización para desentrañar el proceso completo del programa de lealtad, desde la inscripción del cliente hasta el envío de ofertas personalizadas, con el objetivo de recopilar toda la información necesaria para llenar una entrada completa en el RAT.

## Módulo 3: Construcción del Registro de Actividades de Tratamiento (RAT)

Una vez recopilada la información a través de las entrevistas, el siguiente paso es estructurarla y formalizarla en el Registro de Actividades de Tratamiento (RAT). Este módulo se centra en la anatomía del RAT y en las mejores prácticas para su redacción y mantenimiento.

### Anatomía del RAT

El RAT es un documento o sistema que debe contener, como mínimo, la información estipulada por la ley. Se analizará en detalle cada campo requerido, consolidando la lista práctica de la documentación base 1 con los requisitos formales de la normativa.14 Cada campo cumple un propósito específico en la demostración del cumplimiento:

* **Nombre de la actividad y Responsable del Proceso**: Identifica y asigna propiedad interna.
* **Finalidad(es) del tratamiento**: Responde al principio de finalidad, asegurando que el tratamiento tiene un propósito legítimo.2
* **Base de licitud**: Fundamenta la legalidad del tratamiento, respondiendo al principio de licitud.2
* **Categorías de titulares y de datos personales**: Define el alcance y la naturaleza de la información tratada.
* **Categorías de destinatarios (internos y externos)**: Aporta transparencia sobre con quién se comparten los datos.
* **Transferencias internacionales**: Permite gestionar los riesgos asociados al flujo transfronterizo de datos.
* **Plazos de conservación y supresión**: Demuestra el cumplimiento del principio de proporcionalidad o limitación del plazo.1
* **Descripción de las medidas de seguridad**: Evidencia el cumplimiento del principio de seguridad.1

### Guía de Redacción y Contenido

La calidad del RAT depende de la precisión y claridad de su contenido.

* **Finalidades**: Se debe enseñar a redactar finalidades que sean "específicas, explícitas y lícitas".2 Se deben evitar descripciones vagas como "para fines de marketing" y optar por formulaciones precisas como "para enviar comunicaciones comerciales personalizadas sobre productos de la categoría X, basadas en el historial de compras del cliente".
* **Bases de Licitud**: La correcta elección de la base de licitud es una de las decisiones más críticas. Define los derechos del titular y las obligaciones de la empresa. Se proporcionará una guía detallada sobre las bases de licitud aplicables bajo la Ley 21.719, con ejemplos claros.
* **Medidas de Seguridad**: No es necesario ni recomendable describir las medidas de seguridad con un detalle que pueda comprometerlas. Se debe enseñar a utilizar terminología estándar y reconocida que demuestre la diligencia debida, como "Cifrado de datos en tránsito (protocolo TLS≥1.2) y en reposo (algoritmo AES−256)", "Control de acceso basado en roles (RBAC) con revisión trimestral de permisos", o "Plataforma SIEM para monitoreo de accesos y generación de alertas".1

#### Herramienta Práctica 4: Plantilla Maestra del RAT (Formato Spreadsheet)

Se entrega una plantilla avanzada en formato Excel o Google Sheets, diseñada para ser el núcleo del sistema de cumplimiento. Esta plantilla incluye:

* Todos los campos del RAT consolidados de las fuentes.1
* Listas desplegables para campos estandarizados (ej. Bases de Licitud, Categorías de Titulares, Tipos de Medidas de Seguridad) para garantizar la consistencia en toda la organización.
* Formato condicional para resaltar visualmente las filas con campos obligatorios incompletos.
* Columnas adicionales para la gestión interna del DPO: ID único de la actividad, Fecha de creación, Fecha de última revisión, Dueño del Proceso (contacto), y Estado (Borrador, En Revisión, Aprobado).

### Tabla Clave 1: Guía de Bases de Licitud (Ley 21.719)

La selección de la base jurídica correcta es una decisión fundamental que impacta todo el ciclo de vida del dato. Para facilitar esta tarea crítica, se proporciona la siguiente tabla de referencia. Esta herramienta actúa como un soporte decisional rápido (*job aid*) para el DPO durante las entrevistas y la formalización del RAT, estandarizando la toma de decisiones, reduciendo el riesgo de errores y asegurando que cada actividad de tratamiento esté anclada en un fundamento legal sólido y defendible.

| Base de Licitud | Descripción y Aplicación Práctica |
| --- | --- |
| **Consentimiento** | El titular ha manifestado su voluntad de forma libre, específica, informada e inequívoca. Es la base por defecto cuando ninguna otra aplica. Debe ser demostrable y revocable.15 | **Ejemplos**: Suscripción a un newsletter de marketing; instalación de cookies no esenciales en un sitio web; participación en un estudio de mercado. |
| **Ejecución de Contrato o Medidas Precontractuales** | El tratamiento es necesario para cumplir con las obligaciones de un contrato en el que el titular es parte, o para aplicar medidas a petición de este antes de celebrar un contrato.1 | **Ejemplos**: Tratar la dirección de un cliente para despachar un producto comprado online; analizar el currículum de un candidato para un puesto de trabajo; procesar datos de pago para una suscripción. |
| **Cumplimiento de una Obligación Legal** | El tratamiento es necesario para cumplir con una ley o normativa a la que el responsable está sujeto.12 | **Ejemplos**: Reportar información de transacciones a la Unidad de Análisis Financiero (UAF); conservar los registros laborales de un empleado por los plazos que exige el Código del Trabajo; emitir y conservar facturas con los datos del cliente para fines tributarios. |
| **Interés Legítimo** | El tratamiento es necesario para satisfacer un interés legítimo del responsable o de un tercero, siempre que sobre dicho interés no prevalezcan los derechos y libertades fundamentales del titular.15 Requiere un análisis de ponderación. | **Ejemplos**: Implementar medidas de seguridad de red y prevención de fraude; monitorear accesos a instalaciones por seguridad; realizar análisis internos para mejorar un servicio (con datos pseudoanonimizados). |
| **Protección de Intereses Vitales** | El tratamiento es necesario para proteger la vida o la integridad física del titular o de otra persona. **Ejemplos**: Compartir el grupo sanguíneo de un paciente inconsciente con el personal de una ambulancia; contactar a un familiar de emergencia de un empleado que ha sufrido un accidente laboral. |
| **Interés Público o Ejercicio de Poderes Públicos** | El tratamiento es realizado por organismos públicos en el cumplimiento de sus funciones legales.18 | **Ejemplos**: Tratamiento de datos de contribuyentes por el Servicio de Impuestos Internos; gestión de datos de beneficiarios de programas sociales por el Ministerio de Desarrollo Social. |

### Ejercicio Práctico del Módulo 3

* **Escenario**: El participante debe utilizar la información recopilada durante el ejercicio de *role-playing* del Módulo 2 sobre el "Gestión de Programa de Lealtad".
* **Tarea**: Abrir la **Plantilla Maestra del RAT** y completar una fila entera para esta actividad de tratamiento. El participante deberá redactar las finalidades de forma precisa, seleccionar la base de licitud más adecuada de la lista desplegable (probablemente una combinación de Ejecución de Contrato para los beneficios básicos y Consentimiento para el marketing personalizado), listar las categorías de datos y titulares, describir los destinatarios y proponer un plazo de conservación razonable.

## Módulo 4: Clasificación de Datos y Mapeo de Flujos

Un inventario de datos no es solo una lista estática; es un mapa dinámico que debe reflejar la sensibilidad de la información y su movimiento a través de la organización y hacia el exterior.1 Este módulo enseña a clasificar los datos y a visualizar sus flujos.

### Metodología de Clasificación de Datos

Se establece un sistema de clasificación de datos pragmático y alineado con la ley, basado en tres niveles de sensibilidad 1:

1. **Datos Personales Comunes**: Toda información que no califica como sensible o de NNA (ej. nombre, correo electrónico, dirección, historial de compras no revelador).
2. **Datos Sensibles**: Se realiza un análisis profundo de la definición legal 9, que incluye origen étnico, convicciones religiosas, afiliación sindical, datos de salud, vida sexual, datos biométricos, etc. Se presta especial atención a la categoría única en la legislación chilena: la  
   **"situación socioeconómica"**.1 Se explica que datos comúnmente manejados como el nivel de ingresos, el historial crediticio, la afiliación a un sistema de previsión social (AFP/Fonasa), o incluso un análisis detallado del patrón de consumo, pueden ser considerados datos sensibles y deben ser tratados con el máximo nivel de protección.
3. **Datos de Niños, Niñas y Adolescentes (NNA)**: Cualquier dato perteneciente a menores de edad, cuyo tratamiento impone requisitos reforzados como la obtención del consentimiento de los padres o tutores y la consideración primordial del interés superior del niño.1

### Técnicas para Documentar y Visualizar Flujos de Datos (Data Flows)

El objetivo es ir más allá de un simple listado de destinatarios en el RAT para crear un mapa visual del ciclo de vida del dato.1

* **Flujos Internos**: Se enseña a trazar el recorrido de un dato entre los sistemas internos clave. Por ejemplo, el registro de un nuevo cliente puede iniciar en el servidor web, viajar al sistema de gestión de relaciones con clientes (CRM), luego al sistema de planificación de recursos empresariales (ERP) para la facturación, y finalmente a un *data warehouse* para análisis de *business intelligence*.1
* **Flujos Externos**: Se documentan todas las transferencias a terceros, distinguiendo claramente entre "Encargados del tratamiento" (proveedores que tratan datos por cuenta y bajo instrucción del responsable, como un proveedor de servicios en la nube o una agencia de marketing) y "Cesionarios" (terceros que reciben los datos para sus propios fines).1 Para cada flujo externo, se debe registrar el nombre del tercero, el propósito específico de la transferencia y la base legal que la ampara.
* **Caso Práctico Sectorial**: Se profundiza en el ejemplo de la industria acuícola.1 Se explica cómo datos generados por sensores de IoT (temperatura del agua, niveles de oxígeno) o datos de geolocalización del personal en terreno, que a primera vista pueden parecer datos operativos, se convierten en datos personales en el momento en que pueden ser vinculados a un operario específico o al responsable de un centro de cultivo. En ese instante, quedan bajo el ámbito de la ley y sus flujos deben ser mapeados, por ejemplo, desde los sensores en Chile hasta una plataforma de análisis de IA en la nube ubicada en el extranjero.1

El mapeo de flujos de datos no es meramente un ejercicio de documentación para cumplir con un requisito legal. Es una herramienta de gestión de riesgos fundamental. Al visualizar qué categorías de datos, y cuán sensibles son, fluyen hacia qué proveedores externos, el DPO puede construir una matriz de riesgo de terceros basada en evidencia. Un proveedor de *cloud computing* que almacena la base de datos completa de clientes, incluyendo datos sensibles, representa un riesgo inherentemente mayor que una herramienta de encuestas que solo recibe correos electrónicos para un sondeo puntual. Este mapa de flujos permite al responsable priorizar sus esfuerzos de debida diligencia, exigir cláusulas contractuales de protección de datos más robustas a los proveedores de alto riesgo y tomar decisiones informadas sobre con quién compartir los activos de información más críticos de la organización.16

#### Herramienta Práctica 5: Matriz de Clasificación de Datos y Checklist de Requisitos

Se proporciona una tabla que cruza las categorías de datos (Común, Sensible, NNA) con los requisitos de protección obligatorios bajo la Ley 21.719. Las columnas incluyen preguntas como: ¿Requiere consentimiento explícito por defecto? ¿Es obligatorio realizar una Evaluación de Impacto (EIPD)? ¿Existen restricciones especiales para su transferencia internacional?

#### Herramienta Práctica 6: Formato para Documentación de Flujos de Datos

Se entrega una plantilla simple, que puede ser usada en Word, PowerPoint o una herramienta de diagramación online (como Lucidchart o Diagrams.net). Incluye una leyenda de símbolos estandarizados para representar sistemas, bases de datos, procesos manuales, flujos internos y transferencias externas, facilitando la creación de diagramas de flujo consistentes y fáciles de entender en toda la organización.

### Ejercicio Práctico del Módulo 4

* **Escenario**: Se retoma la actividad de tratamiento "Gestión de Programa de Lealtad" de los ejercicios anteriores.
* **Tarea**:
  1. Utilizando la **Matriz de Clasificación**, clasificar cada uno de los datos personales tratados en el programa (ej. Nombre [Común], RUT [Común], Email [Común], Historial de Compras).
  2. Utilizando el **Formato de Documentación de Flujos**, crear un diagrama de flujo simple que muestre cómo los datos de un nuevo miembro fluyen desde el formulario de inscripción en la tienda, al sistema de punto de venta (POS), luego se sincronizan con el CRM central, y finalmente un subconjunto de datos (nombre, email, segmento de cliente) se envía a una agencia de marketing externa para la ejecución de campañas de correo electrónico.

## Módulo 5: Definición de Políticas de Retención y Supresión

El tratamiento de datos personales no puede ser indefinido. Este módulo aborda cómo establecer políticas de retención y procedimientos de eliminación que cumplan con el principio de proporcionalidad y limitación del plazo de conservación, uno de los pilares de la Ley 21.719.1

### Metodología para Definir Plazos de Retención

Establecer por cuánto tiempo se deben conservar los datos requiere un análisis estructurado que equilibre las necesidades del negocio con las obligaciones legales. El enfoque a seguir es:

1. **Identificar Obligaciones Legales**: El primer paso es investigar los plazos de prescripción o conservación obligatoria definidos en la legislación sectorial. Esto incluye, por ejemplo, los plazos para conservar documentación tributaria, contratos comerciales o expedientes laborales.1
2. **Revisar Obligaciones Contractuales**: Analizar contratos con clientes, proveedores o socios que puedan estipular períodos específicos durante los cuales la información debe ser conservada.
3. **Determinar la Necesidad Operativa**: Evaluar por cuánto tiempo un dato es genuinamente útil y necesario para la finalidad para la cual fue recogido. Por ejemplo, conservar los currículums de candidatos no seleccionados por 6 a 12 meses puede justificarse por la posibilidad de que surja una nueva vacante similar.1 Pasado ese tiempo, su utilidad disminuye drásticamente.
4. **Establecer el Plazo y la Justificación**: El plazo de retención final para una categoría de datos será el período máximo que resulte de los tres análisis anteriores. Es crucial que cada plazo definido tenga una justificación clara y documentada.

### Procedimientos de Supresión Segura

Una vez que expira el período de retención, los datos deben ser eliminados o anonimizados de forma segura.

* **Métodos de Eliminación**: Se debe diferenciar entre el borrado lógico (simplemente marcar un registro como "eliminado" en una base de datos, sin borrarlo físicamente) y el borrado físico (sobrescribir los datos para hacerlos irrecuperables). La ley exige una eliminación efectiva.
* **Alternativas a la Eliminación**: En ciertos casos, como para análisis estadístico a largo plazo, la anonimización (eliminar irreversiblemente cualquier posibilidad de identificar a una persona) o la pseudoanonimización (reemplazar identificadores directos por seudónimos) pueden ser alternativas válidas.
* **Auditabilidad**: El procedimiento de eliminación debe ser sistemático, programado (ej. ejecutado trimestralmente por TI) y, fundamentalmente, debe generar un registro de auditoría que evidencie qué datos se eliminaron, cuándo y en virtud de qué política, tal como se especifica en la documentación base.1

#### Herramienta Práctica 7: Plantilla para la Política de Retención de Datos

Se proporciona un documento maestro de política de retención. Es una tabla estructurada que permite al DPO definir, para cada categoría de dato identificada en el RAT (ej. "Datos de facturación de clientes", "Registros de acceso a oficinas", "CV de postulantes"), el período de retención, la justificación específica (legal, contractual u operativa), el método de supresión aprobado (ej. "Borrado físico mediante script SQL", "Anonimización de campos X, Y, Z") y el área o rol responsable de ejecutar la supresión.

### Tabla Clave 2: Tabla de Referencia de Plazos de Retención Legales en Chile

Definir los plazos de retención requiere una investigación legal que puede ser compleja. Esta tabla de referencia proporciona una guía rápida sobre algunos de los plazos mínimos de conservación más comunes establecidos por la legislación chilena. Sirve para ahorrar tiempo, reducir el riesgo de incumplimiento por desconocimiento y proporcionar una base sólida y defendible para la política de retención de la empresa, transformando el abstracto "principio de proporcionalidad" en una guía de acción concreta.

| Tipo de Documento / Dato | Normativa Aplicable (Referencial) | Plazo Mínimo de Conservación Legal |
| --- | --- | --- |
| **Libros de Contabilidad y Documentación Tributaria (Facturas, etc.)** | Código Tributario (Art. 17, 200) | 6 años desde la última anotación o declaración. |
| **Contratos de Trabajo, Finiquitos y Liquidaciones de Sueldo** | Código del Trabajo | Al menos 5 años desde la terminación de la relación laboral (plazo de prescripción de acciones laborales). |
| **Documentación Previsional y de Seguridad Social** | Normativa de la Superintendencia de Pensiones y de Salud | Varía, pero se recomienda conservar durante toda la vida laboral del empleado y varios años después. |
| **Contratos Comerciales y Civiles** | Código de Comercio / Código Civil | 5 años para acciones ejecutivas, 10 años para acciones ordinarias. Se recomienda conservar durante la vigencia del contrato y al menos 10 años después. |
| **Información de Consumidores (Garantías, Contratos de Adhesión)** | Ley N° 19.496 de Protección de los Derechos de los Consumidores | Durante la vigencia de la garantía y plazos de prescripción aplicables (generalmente 6 meses a 2 años). |

*Nota: Esta tabla es una guía referencial y no reemplaza la asesoría legal específica para cada caso de negocio.*

### Ejercicio Práctico del Módulo 5

* **Escenario**: El participante debe desarrollar la política de retención para el proceso de "Reclutamiento y Selección" de una empresa.
* **Tarea**: Utilizando la **Plantilla de Política de Retención**, debe completar las entradas para dos categorías de datos distintas:
  1. **"Currículums y datos de postulantes no seleccionados"**: Deberá definir un plazo basado en la necesidad operativa (ej. 12 meses), justificarlo (ej. "Para considerar al candidato en futuras vacantes apropiadas") y describir un método de supresión (ej. "Ejecución de un script automatizado que realiza un borrado físico de los registros en la base de datos de postulantes y elimina los archivos adjuntos del servidor de archivos").
  2. **"Expediente laboral de empleados contratados"**: Deberá investigar o asumir plazos legales (ej. basados en el Código del Trabajo) y definir un período de retención post-empleo (ej. "5 años después de la terminación del contrato"), justificándolo en la prescripción de acciones legales laborales.

## Módulo 6: Especificaciones Técnicas y Automatización

El cumplimiento efectivo y eficiente de la Ley 21.719 a escala empresarial requiere el apoyo de la tecnología. Este módulo capacita al DPO para actuar como un puente entre los requisitos legales de privacidad y los equipos de TI o proveedores de software, traduciendo la necesidad de cumplimiento en especificaciones funcionales claras.

### Del Requisito Legal a la Especificación Funcional

El DPO debe ser capaz de describir los requerimientos del programa de privacidad en un lenguaje que un ingeniero de software o un arquitecto de sistemas pueda entender. Se analizará la arquitectura de sistema propuesta en la documentación base 1 como un modelo de especificación:

* **Base de Datos del Inventario**: Necesidad de una base de datos relacional con tablas interconectadas como processing\_activities, data\_assets, data\_categories y data\_flows, que permitan consultas complejas (ej. "¿Qué actividades tratan datos de salud y en qué sistemas se almacenan?").1
* **Interfaz de Usuario (UI)**: Requisito de una interfaz web intuitiva que guíe al personal no técnico (los dueños de proceso) a través de la documentación de una actividad de tratamiento.1
* **Visualización de Flujos**: El sistema debe poder generar diagramas de flujo de datos automáticamente a partir de la información registrada, para facilitar el análisis de riesgos.1
* **Motor de Políticas de Retención**: El sistema debe permitir definir reglas de retención de forma declarativa (ej. "SI categoría\_dato = 'CV No Seleccionado' ENTONCES retener por 180 días desde fecha\_creacion") y automatizar su ejecución mediante un proceso programado (*cron job*) que identifique datos expirados y ejecute la acción de eliminación o anonimización, dejando un rastro de auditoría inmutable.1

### Revisión de Herramientas de Mercado (Panorama Tecnológico)

Se proporcionará una visión general de las categorías de software que apoyan la gestión de la privacidad, permitiendo al DPO conocer las soluciones disponibles:

* **Plataformas de Gestión de Privacidad (PMP)**: Son suites de software integradas que buscan centralizar todas las tareas de cumplimiento. Líderes del mercado como **OneTrust** 16 y  
  **BigID** 12 ofrecen módulos específicos para el mapeo de datos (inventario y RAT), la gestión del consentimiento, la automatización de la respuesta a solicitudes de derechos de los titulares y la gestión de incidentes.
* **Herramientas de Descubrimiento y Clasificación Automatizada**: Estas herramientas son cruciales para acelerar el mapeo inicial y mantenerlo actualizado. Escanean de forma continua los repositorios de datos de la organización (bases de datos, servidores de archivos, almacenamiento en la nube) para encontrar y clasificar datos personales, incluyendo datos sensibles y regulados.1 Ejemplos de estas tecnologías incluyen soluciones de  
  **Kriptos** 23,  
  **Forcepoint** 24, y las capacidades nativas de plataformas como  
  **Microsoft Purview** 25 y  
  **Thales CipherTrust**.26
* **Motores de Políticas de Retención**: Algunas plataformas, como las ofrecidas por **BigID** 27 o  
  **Smartsheet** 28 en sus planes avanzados, permiten automatizar la aplicación de las políticas de retención, identificando y gestionando la eliminación de datos que han cumplido su ciclo de vida.

### Elaboración de un Caso de Negocio para Inversión en Tecnología

Se guiará al DPO en la construcción de un caso de negocio sólido para justificar la inversión en estas herramientas. El argumento no debe centrarse únicamente en el "cumplimiento", sino en el valor para el negocio: reducción del riesgo de multas, aumento de la eficiencia operativa (automatizando tareas manuales), mejora en la toma de decisiones al tener un mapa claro de los datos, y fortalecimiento de la confianza del cliente.

#### Herramienta Práctica 8: Checklist de Requisitos Funcionales para una Plataforma de Gestión de Privacidad

Se entrega una checklist detallada que el DPO puede utilizar para evaluar y comparar a diferentes proveedores de software. Los criterios incluyen:

* **Módulo RAT**: ¿Permite personalizar los campos del registro? ¿Soporta flujos de aprobación?
* **Mapeo de Flujos**: ¿Genera diagramas de flujo de datos de forma automática o semi-automática?
* **Motor de Retención**: ¿El motor de reglas es configurable? ¿Se integra con los sistemas de origen para ejecutar la eliminación? ¿Genera logs de auditoría?
* **Integraciones**: ¿Posee conectores pre-construidos para los principales sistemas de la empresa (ej. SAP, Salesforce, AWS S3)?
* **Portal de Titulares**: ¿Ofrece un portal de autoservicio para que los titulares ejerzan sus derechos?

### Ejercicio Práctico del Módulo 6

* **Escenario**: El DPO de la empresa de retail ha completado el mapeo manual de varios procesos clave y ahora necesita proponer la adquisición de una plataforma tecnológica para escalar y automatizar la gestión del RAT y las políticas de retención.
* **Tarea**: Utilizando el **Checklist de Requisitos Funcionales**, se pide al participante que navegue por el sitio web público de un proveedor como OneTrust o BigID. Deberá encontrar la información sobre sus módulos de "Data Mapping" / "Data Discovery" y "Data Retention". Luego, deberá llenar el checklist evaluando, basándose en la información pública, en qué medida la herramienta parece cumplir con los requisitos definidos. Finalmente, deberá escribir un párrafo recomendando (o no) solicitar una demostración personalizada de la herramienta, justificando su decisión en base a la evaluación realizada.

## Conclusión: Del Inventario a la Gobernanza Continua de Datos

La finalización del mapeo inicial de datos y la creación de la primera versión del RAT no es el final del camino, sino el comienzo de un ciclo de gobernanza de datos continua. El RAT no es un documento que se crea una vez y se archiva; es un organismo vivo que debe evolucionar junto con la organización. Los procesos de negocio cambian, se adoptan nuevas tecnologías, se lanzan nuevos productos y el RAT debe reflejar fielmente esta realidad para mantener su valor como herramienta de gestión.

Este inventario se convierte en el insumo fundamental para otras obligaciones críticas de la Ley 21.719. Es la base para identificar qué actividades de tratamiento, por su naturaleza, alcance o uso de tecnologías, presentan un alto riesgo para los derechos de las personas y, por lo tanto, requieren una Evaluación de Impacto en la Protección de Datos (EIPD).5 Asimismo, es la herramienta indispensable para responder de manera eficiente y completa a las solicitudes de derechos de los titulares, permitiendo localizar rápidamente todos los datos de una persona en los diversos sistemas de la empresa.10

Para asegurar su vigencia, se debe establecer un proceso de revisión y auditoría periódica del RAT. Una buena práctica es realizar una revisión anual completa, además de revisiones puntuales cada vez que se implemente un nuevo proceso de negocio significativo o se adquiera un nuevo sistema tecnológico que vaya a tratar datos personales. Solo a través de esta mejora continua, el RAT cumplirá su doble propósito: ser la prueba documental del cumplimiento ante la autoridad y la guía estratégica para una gestión de datos responsable y confiable.

## Apéndices: Caja de Herramientas del DPO

Esta sección consolida todas las plantillas y herramientas prácticas desarrolladas a lo largo del curso, presentadas en formatos limpios y listos para ser adaptados y utilizados por el DPO en su organización.

* **A. Plantilla Maestra del RAT (Formato Spreadsheet)**
* **B. Guion Estructurado de Entrevista para el Mapeo de Datos**
* **C. Matriz de Clasificación de Datos y Checklist de Requisitos de Protección**
* **D. Formato y Leyenda para Documentación de Flujos de Datos**
* **E. Plantilla para la Política de Retención y Supresión de Datos**
* **F. Checklist de Requisitos Funcionales para Plataformas de Gestión de Privacidad**
* **G. Guía de Referencia Rápida de Bases de Licitud (Tabla Clave 1)**
* **H. Tabla de Referencia de Plazos de Retención Legales en Chile (Tabla Clave 2)**

#### Obras citadas

1. Mod\_Inventario.txt
2. Ley Orgánica Protección de Datos Personales de Chile | GSS - GlobalSuite Solutions, fecha de acceso: agosto 16, 2025, <https://www.globalsuitesolutions.com/es/claves-ley-organica-proteccion-de-datos-personales-chile/>
3. Ley 21.719 de Protección de Datos: Desafíos y oportunidades para empresas chilenas, fecha de acceso: agosto 16, 2025, <https://www.amsoft.cl/ley-21719-proteccion-datos-oportunidades-empresas-chilenas/>
4. Protección de Datos Personales en el Ámbito Laboral - Cámara de Comercio de Santiago, fecha de acceso: agosto 16, 2025, <https://www.ccs.cl/wp-content/uploads/2025/04/2025-04-07-Curso-Proteccio%CC%81n-de-Datos-Personales-en-la-Empresa_CCS-3.pdf>
5. Conoce la nueva Ley de protección de datos personales de Chile - Pirani, fecha de acceso: agosto 16, 2025, <https://www.piranirisk.com/es/blog/nueva-ley-proteccion-datos-chile>
6. Ley 21.719 y la seguridad de los datos en Chile: beneficios y desafíos, fecha de acceso: agosto 16, 2025, <https://www.insightspm.com/blog/ley-21.719-y-la-seguridad-de-los-datos-en-chile-beneficios-y-desaf%C3%ADos>
7. Nueva Ley de Datos Personales: clave para la sostenibilidad del comercio electrónico, fecha de acceso: agosto 16, 2025, <https://www.amddchile.com/magazine/nueva-ley-de-datos-personales-clave-para-la-sostenibilidad-del-comercio-electronico/>
8. Lecciones del GDPR para la nueva ley de datos en Chile - Prey Project, fecha de acceso: agosto 16, 2025, <https://preyproject.com/es/blog/gdpr-y-nueva-ley-de-datos-en-chile>
9. Ley 21.719: Regulación y Tratamiento de Datos Personales y Creación de la Agencia de Protección de Datos, fecha de acceso: agosto 16, 2025, <https://www.uhc.cl/wp-content/uploads/2025/02/proteccion-datos-personales.pdf>
10. ¿Qué derechos tienes ahora con la nueva Ley de Protección de Datos Personales en Chile? - Gabriel Castillo, fecha de acceso: agosto 16, 2025, <https://gabrielcastillo.work/ley-21719-19628-tus-derechos-y-diferencias/>
11. Guía simplificada Ley 21.719: Protección de Datos Personales en Chile - Valuetech, fecha de acceso: agosto 16, 2025, <https://www.valuetech.cl/guia-simplificada-ley-21-719-proteccion-de-datos-personales-en-chile/>
12. La nueva Ley de Privacidad de Datos de Chile: Una guía de cumplimiento para la legislación aprobada 21.719 - BigID, fecha de acceso: agosto 16, 2025, <https://bigid.com/es/blog/chile-new-data-privacy-law-21-719/>
13. Ley de Protección de Datos Personales en Chile, ¿cómo afecta a tu empresa? - Rankmi, fecha de acceso: agosto 16, 2025, <https://www.rankmi.com/blog/nueva-ley-de-proteccion-de-datos-personales-como-afecta-a-tu-empresa>
14. Registro de actividades de tratamiento, fecha de acceso: agosto 16, 2025, <https://protecciondedatos.uc.cl/guia/rat/>
15. Novedades de Ley de Protección y Tratamiento de Datos Personales (Ley 21.719), fecha de acceso: agosto 16, 2025, <https://www.circuloverde.cl/novedades-de-ley-de-proteccion-y-tratamiento-de-datos-personales-ley-21-719/>
16. Guía Completa sobre la ley 21.719 - alayiatrust.com, fecha de acceso: agosto 16, 2025, <https://alayiatrust.com/guia-completa-sobre-la-ley-21-719/>
17. www.bcn.cl, fecha de acceso: agosto 16, 2025, <https://www.bcn.cl/leychile/navegar?idNorma=1209272#:~:text=En%20el%20tratamiento%20de%20los,filtraci%C3%B3n%2C%20da%C3%B1o%20accidental%20o%20destrucci%C3%B3n.>
18. Descripción y síntesis de la ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agen - BCN, fecha de acceso: agosto 16, 2025, <https://www.bcn.cl/obtienearchivo?id=repositorio/10221/37137/1/Informe_12_25_Ley_Datos_Personales_rev.pdf>
19. Ley de protección de datos personales en Chile: guía completa - Prey Project, fecha de acceso: agosto 16, 2025, <https://preyproject.com/es/blog/ley-de-proteccion-de-datos-en-chile>
20. Guía completa para el cumplimiento del RGPD | Blog - OneTrust, fecha de acceso: agosto 16, 2025, <https://www.onetrust.com/es/blog/gdpr-compliance/>
21. OneTrust: Soluciones de uso responsable de datos e IA, fecha de acceso: agosto 16, 2025, <https://www.onetrust.com/es/>
22. Compliance | BigID, fecha de acceso: agosto 16, 2025, <https://bigid.com/es/compliance/>
23. Descubrimiento, Clasificación y Etiquetado Automático (DCL) - Kriptos, fecha de acceso: agosto 16, 2025, <https://www.kriptos.io/es/soluciones/casos-de-uso/dcl>
24. Impulse su Descubrimiento y Clasificación de Datos con Forcepoint, fecha de acceso: agosto 16, 2025, <https://www.forcepoint.com/es/blog/insights/supercharge-data-discovery-and-classification>
25. ¿Qué es el gobierno de datos para empresas? | Seguridad de Microsoft, fecha de acceso: agosto 16, 2025, <https://www.microsoft.com/es-cl/security/business/security-101/what-is-data-governance-for-enterprise>
26. Descubrimiento y clasificación de datos confidenciales - Thales CPL, fecha de acceso: agosto 16, 2025, <https://cpl.thalesgroup.com/es/encryption/data-discovery-and-classification>
27. Data Retention App - BigID, fecha de acceso: agosto 16, 2025, <https://bigid.com/es/perspective/data-retention-app/>
28. Configurar una política de retención de datos | Artículos de ayuda de Smartsheet, fecha de acceso: agosto 16, 2025, <https://help.smartsheet.com/es/articles/2482386-configure-data-retention>
29. Ley de Protección de Datos: pasos para su implementación en organizaciones, fecha de acceso: agosto 16, 2025, <https://www.icdt.cl/ley-de-proteccion-de-datos-21-719-pasos-para-su-implementacion-en-organizaciones/>