

MALLA CURSO LEY N° 21.719 DE PROTECCIÓN DE DATOS PERSONALES Y SU IMPACTO EN LA EMPRESA

Contexto: La **Ley N° 21.719 de Protección de Datos Personales**, que entra en vigencia en Chile el **1 de diciembre de 2026**, cambia profundamente la gestión de los Recursos Humanos al exigir que las empresas traten los datos de postulantes, trabajadores y extrabajadores bajo estrictos estándares internacionales.

Relator: Rony Núñez Mesqida, Académico Derecho del Trabajo y Derecho Administrativo

Contenidos

1. Bases de Licitud en el Ámbito Laboral

Conceptos Fundamentales y Ámbito de Aplicación

- Qué es la ley: Reemplaza la antigua normativa y crea la Agencia de Protección de Datos Personales.
- A quién aplica: Obliga a empresas, instituciones públicas y personas que manejan datos.
- Diferencia de roles: Distingue entre el *Responsable* (quien decide el uso de los datos) y el *Encargado* (quien los procesa)

2. Tratamiento de Datos Sensibles y Biométricos

El control de asistencia y acceso mediante huella dactilar o reconocimiento facial tiene regulaciones muy estrictas debido a su naturaleza.

- Principio de Necesidad: Demostrar que el uso de datos biométricos es estrictamente necesario y proporcional para el fin perseguido.
- Evaluación de Impacto (EIPD): Obligación de realizar un análisis previo de riesgos antes de implementar sistemas de control masivos o biométricos.
- Datos de Salud: Restricción estricta en el manejo de licencias médicas o exámenes ocupacionales. Solo se deben tratar para lo legalmente requerido.

3. Actualización de Instrumentos Laborales

Las empresas deben adecuar sus documentos legales para evitar multas de la nueva Agencia de Protección de Datos.

- Contratos de Trabajo: Inclusión de cláusulas informativas transparentes sobre qué datos se guardan y para qué fines.
- Reglamento Interno (RIOHS): Incorporación de obligaciones, prohibiciones y sanciones disciplinarias para los trabajadores que manejen bases de datos.
- Convenios con Proveedores (Payroll): Firma de mandatos explícitos de procesamiento de datos con proveedores de software de remuneraciones, seguros o TI.

4. Gestión y Derechos del Trabajador (Derechos ARCO+)

El trabajador, en su rol de titular, puede ejercer sus derechos directamente ante el empleador.

- Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición a sus datos personales.

- Derecho de Portabilidad: El trabajador puede exigir una copia estructurada y tecnológica de sus datos laborales.
- Plazo de Respuesta: El empleador tiene un límite de **30 días hábiles** (prorrogables por otros 30 en casos complejos) para responder al trabajador.

5. Modelo de Prevención e Infracciones

La ley exige un rol proactivo para demostrar que se protege la información en el día a día.

- Registro de Actividades (RAT): Inventario obligatorio que detalle qué datos de RRHH se tienen, dónde se guardan y cuánto tiempo se conservan.
- Delegado de Protección de Datos (DPD): Designación de un responsable encargado de supervisar el cumplimiento interno (altamente recomendado en grandes empresas).
- Reporte de Brechas: Obligación de notificar a la Agencia de Protección de Datos ante cualquier filtración de datos de los trabajadores en un plazo oportuno.

6. Descripción del Proceso Laboral

- Nombre de la Actividad: Proceso específico (ej. Reclutamiento, Pago de Remuneraciones, Control de Asistencia).
- Finalidad: El objetivo del tratamiento (ej. "Gestionar el pago de sueldos y cotizaciones previsionales").

7. Categorías de Titulares y Datos

- Tipo de Titulares: Postulantes, trabajadores activos, extrabajadores o cargas familiares.
- Tipos de Datos Personales: Nombres, RUT, dirección, teléfono, cuenta bancaria.
- Datos Sensibles/Biométricos: Detallar si se manejan huellas dactilares, afiliación sindical, licencias médicas o datos de salud.

8. Destinatarios y Transferencias

- Cesionarios Externos: Entidades a las que se envían los datos por obligación (ej. Dirección del Trabajo, Previred, AFC, Mutuales, SII).
- Proveedores (Encargados): Empresas externas de software de remuneraciones (Payroll), control de asistencia en la nube o empresas de TI.
- Transferencia Internacional: Indicar si el software o los servidores de la empresa están alojados fuera de Chile.

9. Contratación e Incorporación (Onboarding)

- Es el momento donde se formaliza la relación laboral y se recopila la información sensible del trabajador y su entorno cercano.
- Titulares: Trabajadores contratados y sus cargas familiares.
- Datos recolectados: RUT, estado civil, dirección, datos de contacto de emergencia, certificados de nacimiento de hijos (para asignaciones familiares), datos de cuentas bancarias.
- Alerta de cumplimiento: La base de licitud aquí es puramente la ejecución del contrato. Toda la información solicitada debe ser estrictamente necesaria para dar de alta al trabajador.

10. Gestión de Remuneraciones, Beneficios y Obligaciones Previsionales

- Involucra el cálculo mensual de sueldos y la transferencia de datos a entidades estatales o privadas.
- Titulares: Trabajadores activos y prestadores de servicios (honorarios).
- Datos recolectados: Sueldo base, bonos, horas extras, licencias médicas (días de ausentismo), retenciones judiciales (ej. pensiones de alimentos), aportes a sindicatos.
- Alerta de cumplimiento: Compartir estos datos con plataformas como Previred, la Dirección del Trabajo o el SII está respaldado por el cumplimiento de una obligación legal, por lo que no requiere consentimiento del trabajador.

11. Control de Asistencia, Acceso y Seguridad Operacional

- Titulares: Trabajadores activos y personal externo (contratistas).
- Datos recolectados: Huella dactilar, rasgos faciales, hora de ingreso/salida, geolocalización (en teletrabajo o rutas), grabaciones de cámaras de seguridad (CCTV).
- Alerta de cumplimiento: Los datos biométricos son datos sensibles. Este proceso requiere obligatoriamente una Evaluación de Impacto (EIPD) previa para demostrar que el sistema elegido es proporcional y seguro.

12. Desvinculación e Historial de Extrabajadores (Offboarding)

- Titulares: Extrabajadores.
- Datos recolectados: Finiquito, causales de despido (artículos del Código del Trabajo), actas de comparendo, demandas laborales en curso, cartas de recomendación.
- Alerta de cumplimiento: Se debe bloquear el acceso masivo a estos datos. Solo deben conservarse en un archivo histórico restringido durante el plazo legal de prescripción de acciones laborales (habitualmente 5 años).