# Descriptor oferta formativa

# Marco legal y de ley de protección de datos personales

## Resumen

**Modalidad de Enseñanza:**
Elearning asincrónico

**Horas disponibles:**
60 Hrs.

**Código Sence:**
1238097340

**Objetivos Generales:**
Reconocer procedimientos normativos, técnicos y organizacionales para el tratamiento de datos personales, de acuerdo con la Ley N° 21.719.

## Descripción

El presente curso entrega una visión clara y práctica sobre los principios, derechos y obligaciones asociados al tratamiento de datos personales en Chile. A través de un enfoque normativo y aplicado, permite comprender el marco legal vigente, las responsabilidades de las organizaciones y las buenas prácticas necesarias para una gestión segura, responsable y alineada con el cumplimiento normativo.

## Contenidos

**Módulo 1: Fundamentos y el Nuevo Paradigma de la Autodeterminación Informativa**

- Evolución histórica y contexto geopolítico: De la Ley 19.628
- Taxonomía de los datos: Definición legal y técnica de Dato Personal, Dato Sensible (biometría, origen étnico, salud, perfil biológico) y Datos de Niños, Niñas y Adolescentes.
- Sujetos regulados y territorialidad: Rol del Titular, Responsable del Tratamiento y Tercero Encargado. Aplicación extraterritorial de la ley.
- Principios rectores del tratamiento: Licitud, lealtad, finalidad, proporcionalidad, calidad, seguridad, transparencia, confidencialidad y responsabilidad.

**Objetivos módulo 1**

Identificar los fundamentos normativos de la Ley N° 21.719, según conceptos, sujetos regulados y principios aplicables.

**Módulo 2: Derechos de los Titulares y Bases de Licitud**

- Nuevos mecanismos de consentimiento: Erradicación del opt-out y requisitos del consentimiento libre, específico, inequívoco e informado.
- Bases de licitud alternativas: Ejecución de contratos, cumplimiento de obligación legal y la correcta aplicación del "Interés Legítimo".
- Gestión de Derechos ARCO-P: Procedimientos para garantizar el Acceso, Rectificación, Cancelación (Supresión), Oposición y la nueva Portabilidad.
- Plazos legales y derecho a bloqueo: Mecanismos de respuesta en 30 días (prorrogables) y bloqueo temporal en 2 días hábiles.

**Objetivos módulo 2**

Reconocer derechos de titulares y bases de licitud, considerando procesos de consentimiento, respuesta y bloqueo.

**Módulo 3: Gobernanza Corporativa y Gestión de Terceros**

- Inventario y mapeo de datos (Data Mapping): Construcción del Registro de Actividades de Tratamiento (RAT) y catálogo de bases de datos.
- Elaboración de Políticas de Tratamiento: Requisitos de transparencia, avisos de privacidad y deberes de información (Art. 14 ter).
- Gestión de Encargados de Tratamiento: Negociación y redacción de Acuerdos de Procesamiento de Datos (DPAs) con proveedores (SaaS, Cloud, RRHH).
- Transferencias Internacionales de Datos: Mecanismos lícitos, jurisdicciones adecuadas, Normas Corporativas Vinculantes y Cláusulas Contractuales Modelo

**Objetivos módulo 3**

Reconocer instrumentos de gobernanza de datos, considerando registros, políticas, contratos y transferencias internacionales.

# Descriptor oferta formativa

# Marco legal y de ley de protección de datos personales

**Módulo 4: Ingeniería de Privacidad, Ciberseguridad y Gestión de Incidentes.**

- Privacidad desde el Diseño y por Defecto (Privacy by Design): Minimización de datos, anonimización irreversible y seudonimización.
- Medidas técnicas de seguridad proporcionales: Cifrado de discos, autenticación multifactor (MFA), borrado remoto (wipe) y copias de respaldo.
- Evaluaciones de Impacto en Privacidad (DPIA): Metodología para evaluar riesgos en tratamientos a gran escala o uso de biometría/IA.
- Notificación obligatoria de brechas (Data Breaches): Protocolos de detección, contención técnica y reporte perentorio a la Agencia en un plazo máximo de 72 horas.

**Objetivos módulo 4**

Identificar controles de privacidad y ciberseguridad, según riesgos, evaluaciones de impacto y protocolos de brechas.

**Módulo 5: Modelo de Prevención de Infracciones (MPI) y Plan de Adecuación.**

- Componentes del MPI (Art. 49): Matrices de riesgo, canales de denuncia (whistleblowing) y regímenes disciplinarios laborales.
- El Oficial de Protección de Datos (DPO): Perfil, autonomía, designación y responsabilidades frente al directorio y la autoridad.
- Estrategia de Certificación: Cómo la certificación del MPI opera como eximente o atenuante crítico frente a investigaciones.
- Hoja de Ruta Ágil (Plan 30/60/90 días): Metodología de adecuación progresiva desde el levantamiento de información hasta las pruebas end-to-end antes de diciembre de 2026.

**Objetivos módulo 5**

Reconocer los componentes de un modelo de prevención de infracciones, considerando riesgos, roles, certificación y adecuación normativa.

**Módulo 6: Institucionalidad, Fiscalización y Sector Público.**

- La Agencia de Protección de Datos Personales: Atribuciones fiscalizadoras, normativas, y el Registro Nacional de Sanciones y Cumplimiento.
- Régimen Sancionatorio en el Sector Privado: Tipificación de infracciones (leves, graves, gravísimas), atenuantes, agravantes y multas de hasta 20.000 UTM (o 2%-4% de ingresos globales).
- Cumplimiento en el Estado (Administración Pública): Legalidad funcional, interoperabilidad, limitación del interés legítimo y cesión entre órganos.
- Responsabilidades de la Jefatura Superior: Sumarios administrativos, multas pecuniarias personales a jefes de servicio y rol del funcionario público

**Objetivos módulo 6**

Identificar las facultades fiscalizadoras y sanciones aplicables, según institucionalidad, tipo de infracción y sector regulado.