



CURSO

Curso de Gobernanza y Seguridad de Datos Personales según Ley 21.719



Descripción y Fundamentación

La entrada en vigencia de la Ley 21.719 moderniza el marco regulatorio de la protección de datos personales en Chile, estableciendo nuevas obligaciones para el sector público y privado, así como la creación de la Agencia de Protección de Datos Personales. En este contexto, las organizaciones deben fortalecer sus procesos de gobernanza, seguridad y cumplimiento normativo.

El curso entrega una formación integral y aplicada para que los profesionales comprendan el rol estratégico de la gobernanza de datos, apliquen medidas de seguridad obligatorias y desarrollen capacidades para cumplir con los estándares de la Ley 21.719.



Perfil de ingreso requerido

- Profesionales o técnicos que participen del tratamiento, gestión o resguardo de datos personales.
- Funcionarios públicos, trabajadores de instituciones privadas, analistas de información, encargados de seguridad, TI, compliance, jurídicos, RRHH, salud, educación o atención de usuarios.
- No se requiere formación jurídica previa.





Objetivos

Objetivo General:

Fortalecer las competencias para aplicar principios, obligaciones y estándares de gobernanza y seguridad de datos personales establecidos por la Ley 21.719 en organizaciones públicas y privadas.

Objetivos Específicos

- Comprender los conceptos fundamentales y alcances de la Ley 21.719.
- Identificar los derechos de los titulares y los procedimientos internos requeridos.
- Reconocer las obligaciones de responsables y encargados del tratamiento.
- Aplicar medidas técnicas y organizativas de seguridad de acuerdo con el estándar legal.
- Analizar el funcionamiento de la Agencia de Protección de Datos Personales y el régimen sancionatorio.
- Implementar lineamientos básicos de compliance y gobernanza de datos.



Duración

30 horas cronológicas



Modalidad

50% Asincrónico – 50% Sincrónico



Plan de Estudios

Nombre unidad	Duración en horas cronológicas
Módulo 1: Conceptos Fundamentales y Alcance de la Ley 21.719	6 horas
Módulo 2: Derechos de los Titulares y Procedimientos Internos Reactivos (Gestión ARCOP)	6 horas
Módulo 3: Obligaciones de Responsables y Encargados: Procedimientos Internos Proactivos.	4 horas
Módulo 4: Gestión De Riesgo y Seguridad Operativa.	6 horas
Módulo 5: Agencia de Protección de Datos Personales y Sanciones	6 horas
Módulo 6: Convergencia con la Ley Marco de Ciberseguridad y compatibilidades de roles.	2 horas



Contenidos

MODULO 1

- Definiciones clave: datos estadísticos, personales, datos sensibles, tratamiento, anonimización, seudonimización.
 - Ámbito de aplicación de la ley: sectores públicos y privados.
 - Principios de tratamiento de datos: licitud, finalidad, proporcionalidad, calidad y exactitud, seguridad, lealtad y transparencia e información, y Principios Complementarios: responsabilidad proactiva, confidencialidad, limitación de conservación, no discriminación y transferencia internacional.
 - Bases de licitud del tratamiento según la nueva ley.
-

MODULO 2

- Derechos ampliados: acceso, rectificación, cancelación/supresión, oposición, portabilidad y revocación del consentimiento.
 - Plazos y requisitos para atender solicitudes.
 - Impacto de los derechos en instituciones públicas y empresas privadas.
 - Procedimientos internos obligatorios: Clasificación general: reactivo y proactivo.
 - Procedimiento interno reactivo ARCOP
-

MODULO 3

- Procedimientos Internos Obligatorios Proactivos.
 - Gobernanza y Demostración de Cumplimiento.
 - Registro de Actividades de Tratamiento (RAT).
 - Políticas de Privacidad y Tratamiento.
 - Contratos con encargados: cláusulas mínimas.
 - Minimización de datos y análisis de riesgos.
 - Designación del Delegado de Protección de Datos (DPD).
-

MODULO 4

- Requisitos mínimos de seguridad establecidos por la Ley 21.719.
- Evaluación de impacto en privacidad (EIP).
- Gestión de Vulnerabilidades y Brechas.
- Protocolo de Notificación de incidentes y brechas. Notificación a la Agencia ante incidentes.
- Gestión documentada del riesgo.
- Buenas prácticas basadas en ISO 27001 y estándares internacionales.

MODULO 5

- Naturaleza y funciones de la Agencia.
 - Potestades y Procedimiento Sancionatorio.
 - Régimen de Sanciones y Multas por incumplimiento.
 - Recomendaciones para construir un plan de cumplimiento interno.
 - Checklist operativo para instituciones públicas y privadas.
-

MODULO 6

- Protección de datos personales y su convergencia con la Ley Marco de Ciberseguridad. Introducción. Puntos de convergencia central e impacto en las organizaciones.
- Roles mínimos dentro de las instituciones públicas y empresas privadas, compatibilidad de roles.



Evaluación

Unidad y porcentaje de cada unidad	
Módulo 1: Quiz	20%
Módulo 2: Quiz	15%
Módulo 3: Quiz	15%
Módulo 4: Quiz	20%
Módulo 5: Quiz	25%
Módulo 6: Quiz	5%



Requisitos de aprobación

- Nota mínima de aprobación: 4,0.
- Completar 100% de las actividades y evaluaciones asincrónicas.



Ficha Técnica

Valor	\$300.000
-------	-----------

Consulte por descuentos y modalidades de pago.



Subdirección de Educación
Continua y Capacitación
Dirección General
de Admisión

capacitacion@ubo.cl | +562 2988 4850

General Gana 1702, Edificio Rondizzoni I, Santiago



@uboeducacion



/uboeducacioncontinuaycapacitacion



/company/ubo-educación-continua-y-capacitación

5
AÑOS


Comisión Nacional
de Acreditación
CNA-Chile

UNIVERSIDAD ACREDITADA
MEDIANTE ACUERDO DEL
CONSEJO NACIONAL DE EDUCACIÓN
NIVEL AVANZADO
• GESTIÓN INSTITUCIONAL
• DOCENCIA DE PREGRADO
• VINCULACIÓN CON EL MEDIO
HASTA 9 DE NOVIEMBRE DE 2027