PRESENCIAL

LEGISLACIÓN

ACADEMIA icare

Ciberseguridad y Protección de Datos Personales en Chile

INICIO: 18 de noviembre

Acerca del Curso

El uso de tecnologías de información y comunicaciones conlleva riesgos que pueden afectar los derechos de las personas, la seguridad pública y las infraestructuras críticas. En este contexto, Chile ha consolidado en los últimos años un nuevo mapa normativo en materia de ciberseguridad y protección de datos personales, marcado por la entrada en vigencia de la Ley 21.663 (Marco de Ciberseguridad) y la Ley 21.719 (Protección de Datos Personales), cuya vigencia comienza el 1 de diciembre de 2026.

Este curso entrega a los participantes una comprensión integral del ecosistema regulatorio chileno, permitiéndoles identificar las obligaciones legales aplicables a organismos del Estado y entidades privadas, la institucionalidad creada por ambas leyes (ANCI, CSIRT Nacional, Agencia de Protección de Datos Personales) y los mecanismos de reporte, notificación y gestión de incidentes.

Su enfoque combina el análisis normativo con la construcción de herramientas prácticas de cumplimiento —como matrices integradas de obligaciones— y una mirada especialmente dirigida a profesionales sin formación técnica en informática, que deben asumir un rol activo en la gobernanza de ciberseguridad y datos dentro de sus organizaciones.

RELATOR

José Ignacio Mercado

Director del Grupo de Protección de Datos y Tecnología de Carey

Abogado de la Universidad de Chile. Su práctica se enfoca en privacidad, protección de datos personales, ciberseguridad, transferencia de tecnología y propiedad intelectual. Asesora a empresas de diversos sectores en el diseño de programas de cumplimiento y en procesos de implementación de la nueva Ley de Protección de Datos Personales. También ha trabajado en materias regulatorias vinculadas a industrias farmacéuticas, cosméticas, alimentarias y de dispositivos médicos. Entre 2014 y 2018 se desempeñó como fiscal de Crystal Lagoons (Chile-Holanda).

Objetivos Generales

Comprender el marco normativo chileno en materia de ciberseguridad y protección de datos personales, identificando las obligaciones legales, la institucionalidad y los mecanismos de cumplimiento aplicables a organismos del Estado y entidades privadas, para construir e implementar herramientas de gestión del riesgo normativo en sus organizaciones.

Objetivos Específicos

Al finalizar el curso, los participantes serán capaces de:

1. Identificar las fuentes normativas del ecosistema chileno de ciberseguridad y protección de datos, y su jerarquía.
2. Reconocer los sujetos obligados, la institucionalidad (ANCI, CSIRT Nacional) y los deberes de reporte establecidos por la Ley 21.663.
3. Aplicar las obligaciones del responsable de datos, las bases de licitud y los mecanismos de seguridad establecidos por la Ley 21.719.
4. Construir matrices de cumplimiento normativo que integren las obligaciones de ambas leyes con controles operativos verificables.
5. Comprender el rol de los profesionales jurídicos, de auditoría, gestión de riesgos y compras públicas en el ecosistema de cumplimiento.
6. Aplicar lo aprendido a un caso práctico transversal, identificando obligaciones de reporte, plazos, canales y responsabilidades entre equipos técnicos y jurídicos/compliance.

Dirigido a

Profesionales sin formación técnica en informática que cumplen o deben cumplir un rol activo en la gobernanza de ciberseguridad y protección de datos dentro de sus organizaciones: abogados y equipos jurídicos, oficiales y equipos de compliance, auditores, profesionales de gestión de riesgos, y profesionales del área de compras públicas que participan en la adquisición de proyectos que involucran sistemas de IA y ciberseguridad.

Contenido del Curso

MÓDULO 1

Fundamentos y Contexto Regulatorio (2 horas)

- Ciberseguridad como bien jurídico protegido y objeto de la Ley 21.663.
- Mapa normativo chileno: la Ley 21.719 y su homologación al estándar del RGPD europeo.
- Normativa complementaria: Política Nacional de Ciberseguridad, instructivos sectoriales.
- Conceptos operativos clave: activo informático, auditoría de seguridad, ciberataque, ciberseguridad e incidente de ciberseguridad.

MÓDULO 2

Ley 21.663 – Marco sobre Ciberseguridad (3 horas)

- Institucionalidad: Agencia Nacional de Ciberseguridad (ANCI) y CSIRT Nacional.
- Ámbito de aplicación orgánico y Operadores de Importancia Vital (Decreto N° 285, 2025).
- Gestión y reporte de incidentes: plataforma de notificación ANCI 24/7 (Decreto Supremo N° 295, 2024) y obligaciones preexistentes (Decreto N° 273, 2022).
- Ejercicio práctico: simulación de protocolo de reporte conforme a plazos y canales regulatorios.

MÓDULO 3

Ley 21.719 – Protección de Datos Personales (3 horas)

- Principios y bases de licitud; derechos ARCO y portabilidad.
- Obligaciones del responsable de datos y medidas de seguridad; Evaluación de Impacto en Protección de Datos (EIPD).
- Tratamiento por mandato/encargo a terceros.
- Brechas de seguridad, la Agencia de Protección de Datos Personales y régimen sancionatorio.

MÓDULO 4

Construcción de Matrices de Cumplimiento Integradas (2 horas)

- Matriz tipo Ley 21.663: gobernanza, inventario, calificación OIV, incidentes y auditoría.
- Matriz tipo Ley 21.719: bases de licitud, derechos de titulares, seguridad, EIPD, brechas y encargados.
- Convergencia entre ambas leyes: seguridad de la información, gestión de incidentes, trazabilidad, notificación y controles sobre proveedores.

Contenido del Curso

MÓDULO 5

Rol de los Profesionales No Técnicos (1.5 horas)

- Gobernanza de datos y ciberseguridad como función transversal.
- El Oficial de Cumplimiento: lecciones desde el compliance general (lineamientos FNE).
- Equipos multidisciplinarios en contratación pública para proyectos de IA y ciberseguridad.
- Gestión contractual: cláusulas de seguridad de la información, notificación de incidentes y tratamiento por mandato.

MÓDULO 6

Taller Integrador (0.5 horas)

- Caso práctico transversal: incidente de ciberseguridad que compromete datos personales sensibles.
- Identificación de obligaciones de reporte, plazos y canales bajo ambas leyes.
- Construcción de una matriz de cumplimiento y asignación de responsabilidades entre equipo técnico y equipo jurídico/compliance.

Metodología

El curso se desarrolla mediante una metodología expositiva–aplicada, que combina:

- Clases expositivas sobre el marco normativo vigente.
- Análisis de definiciones legales y sus consecuencias regulatorias.
- Ejercicios prácticos de simulación (protocolo de reporte de incidentes).
- Construcción guiada de matrices de cumplimiento integradas.
- Taller integrador con caso práctico transversal y trabajo en equipo.

Se fomenta la participación activa y la aplicación directa de los conceptos a la realidad operativa de los participantes.

Beneficios

- Comprender de forma clara y aplicada el nuevo ecosistema normativo chileno de ciberseguridad y protección de datos.
- Contar con herramientas concretas (matrices de cumplimiento) para gestionar el riesgo normativo en la organización.
- Fortalecer el rol activo de profesionales jurídicos, de auditoría, riesgo y compras públicas en la gobernanza de ciberseguridad.
- Aplicar lo aprendido a un caso práctico transversal que integra obligaciones, matriz y asignación de roles.

Resultado esperado: los participantes fortalecerán su capacidad para identificar obligaciones legales, construir herramientas de control y cumplimiento, y gestionar contractual y documentalmente los deberes que imponen la Ley 21.663 y la Ley 21.719.

Acerca de la Academia ICARE

En ICARE creemos que el crecimiento sostenible de Chile comienza con el crecimiento de sus personas.

“En ICARE tenemos una convicción profunda: cuando las personas crecen, Chile crece. Y la Academia ICARE existe para acelerar ese crecimiento y acompañarte en ese camino”.

Bernardita Errázuriz
Directora de Academia ICARE

En **ICARE** creemos que el crecimiento sostenible de Chile comienza con el crecimiento de sus personas.

La **Academia ICARE** materializa esta convicción a través de una propuesta formativa orientada a fortalecer la excelencia empresarial y contribuir activamente al desarrollo del país.

Nuestros programas de educación continua están diseñados para profesionales y líderes que buscan actualizarse, reflexionar y actuar en contextos complejos y cambiantes. Los cursos de la **Academia ICARE** se caracterizan por ser ágiles, flexibles y pertinentes, transformando capacidades en acción y aprendizajes en impacto, e impulsando procesos donde la tecnología y la dimensión humana se potencian de manera integrada.

Este curso forma parte de la **vertical legislación,** cuyo propósito es entregar herramientas para comprender y aplicar la legislación laboral, tributaria y de compliance, apoyando una gestión organizacional responsable, actualizada y alineada con las exigencias regulatorias y los estándares de buen gobierno corporativo.

Información General

FECHA DE INICIO
Miércoles 18 de noviembre

FECHA DE TÉRMINO
Lunes 23 de noviembre

DÍAS
Miércoles, Jueves y Lunes

HORARIO
9:00 a 13:00 horas

DURACIÓN
12 horas
3 sesiones

MODALIDAD
Presencial

VALOR GENERAL
$260.000

VALOR SOCIO
$210.000

DESCUENTO: 10% de dcto por 5 o más inscripciones

+Info

DIRECCIÓN: El Golf 40, Piso Zócalo. Las Condes. Santiago - Chile
TELÉFONOS: +56 2 2280 5329 / +56 2 2280 5311 / +56 9 3185 8710
MAIL: seminarios@icare.cl
WEB: www.icare.cl/academia

ACADEMIA icare

Las actividades de la Academia ICARE no son conducentes al otorgamiento de un título o grado académico. El inicio del programa estará sujeto a un número mínimo de participantes. En caso de no alcanzarse, ICARE se reserva el derecho de suspender su realización.