

Compliance. Riesgos de ciberseguridad. Compliance de competencia

Compliance. Riesgos de ciberseguridad. Compliance de competencia

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Metodología:

El Curso será desarrollado con una metodología a Distancia/on line. El sistema de enseñanza a distancia está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales, también se realiza en esta modalidad para permitir el acceso al curso a aquellos alumnos que viven en zonas rurales lejos de los lugares habituales donde suelen realizarse los cursos y que tienen interés en continuar formándose. En este sistema de enseñanza el alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a sus circunstancias personales de tiempo

El alumno dispondrá de un extenso material sobre los aspectos teóricos del Curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado se exigirá un mínimo de 75% del total de las respuestas acertadas.

El Alumno tendrá siempre que quiera a su disposición la atención de los profesionales tutores del curso. Así como consultas telefónicas y a través de la plataforma de teleformación si el curso es on line. Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá del tipo de curso elegido y de las horas del mismo.

© icaformación2026

Profesorado:

Nuestro Centro fundado en 1996 dispone de 1000 m2 dedicados a formación y de 7 campus virtuales.

Tenemos una extensa plantilla de profesores especializados en las diferentes áreas formativas con amplia experiencia docentes: Médicos, Diplomados/as en enfermería, Licenciados/as en psicología, Licencidos/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadodores/as sociales etc…

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas de las siguientes formas:

-Por el aula virtual, si su curso es on line
-Por e-mail
-Por teléfono

Medios y materiales docentes

-Temario desarrollado.

-Pruebas objetivas de autoevaluación y evaluación.

-Consultas y Tutorías personalizadas a través de teléfono, correo, fax, Internet y de la Plataforma propia de Teleformación de la que dispone el Centro.



© icaformación2026

Titulación:

Una vez finalizado el curso, el alumno recibirá por correo o mensajería la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Programa del curso:

El objetivo general consiste en capacitar al alumnado en el diseño, implementación y evaluación de programas de cumplimiento normativo (compliance) centrados en la competencia, la ciberseguridad y el uso responsable de tecnologías en la empresa, conforme al marco legal vigente y los estándares de buen gobierno corporativo. Objetivos específicos 1. Analizar el impacto del uso de medios tecnológicos y redes sociales en el entorno empresarial, identificando riesgos y estableciendo pautas claras de actuación. 2. Comprender las bases de la ciberseguridad en la empresa, incluyendo la gestión de ciberincidentes, el marco legal aplicable, y las herramientas para protegerse de ciberataques. 3. Aplicar criterios de control y supervisión sobre terceros y cadenas de valor tecnológicas, para mitigar riesgos de cumplimiento derivados de la subcontratación o la externalización. 4. Identificar las tecnologías RegTech más relevantes y distinguir entre mecanismos preventivos y detectivos en programas de compliance, especialmente en entornos digitales. 5. Interpretar el marco normativo europeo y la praxis de la CNMC en materia de competencia, diferenciando prácticas legales (lobby) de ilícitas (cárteles), y analizando su impacto en la contratación pública y privada. Qué incluye este contenido: ? 10 Supuestos prácticos ? 20 Vídeos ? 21 Presentaciones y guías interactivas ? 16 Recursos descargables ? Glosario de términos con definiciones clave

ÍNDICE 42420 COMPLIANCE: RIESGOS DE CIBERSEGURIDAD. COMPLIANCE DE COMPETENCIA UNIDAD 1. COMPLIANCE TECNOLÓGICO EN EL ÁMBITO EMPRESARIAL ? Uso de medios tecnológicos en la empresa ? Uso de redes sociales en el ámbito empresarial UNIDAD 2. CIBERSEGURIDAD ? Elemento imprescindible de protección empresarial UNIDAD 3. CONTROLES SOBRE TERCEROS ? Fraccionamientos en las cadenas de valor tecnológicas UNIDAD 4. CONTRATACIÓN ELECTRÓNICA, PROTECCIÓN A CONSUMIDORES Y FIRMA DIGITAL ? Nuevas problemáticas UNIDAD 5. REGTECH: TECNOLOGÍAS PREVENTIVAS Y DETECTIVAS EN COMPLIANCE ? Tecnologías preventivas en Compliance ? Tecnologías detectivas en Compliance UNIDAD 6. GESTIÓN DEL RIESGO OPERATIVO ? Planes de continuidad de negocio y recuperación ante desastres ? Clasificación de la información Empresarial UNIDAD 7. ACTIVIDAD DE COMPLIANCE DE COMPETENCIA ? Marco Normativo Europeo ? Elementos fundamentales de caracterización UNIDAD 8. PRAXIS DE LA CNMC EN RELACIÓN CON LOS PROGRAMAS DE CUMPLIMIENTO ? Programas de cumplimiento eficaces. ? Criterios de evaluación de CNMC. ? El cártel y el Lobby. ? Ejemplo: la Ley de Lobby chilena UNIDAD 9. CONTRATACIÓN PÚBLICA Y LUCHA CONTRA LA CORRUPCIÓN ? Nuevas tecnologías para la mitigación de riesgos de competencia ? Instrucciones de precios, información y estrategias de exclusión UNIDAD 10. NUEVAS TECNOLOGÍAS PARA LA MITIGACIÓN DE RIESGOS DE COMPETENCIA ? Instrucciones de precios, información y estrategias de exclusión ANEXO ? Bibliografía ? Glosario de términos ? Supuestos prácticos

© icaformación2026

© icaformación2026