Mondragon Unibertsitatea

CALENDARIO 02/06/2025 - 02/06/2025

Más información e inscripción

PRESENTACIÓN

Este curso proporciona una visión integral sobre el **cumplimiento normativo en ciberseguridad** y las **auditorías de seguridad**, abordando los principales estándares nacionales e internacionales aplicables a diversos sectores. Se profundizará en normas transversales, sectoriales y específicas, como **ISO 27001, ENS, NIST, IEC 62443, PCI-DSS** y normativas de entornos cloud o privacidad. Asimismo, se explorará el proceso de auditoría de seguridad, tanto desde una perspectiva **estratégica** como **técnica**, permitiendo a los asistentes comprender las metodologías, controles y buenas prácticas para planificar, ejecutar y reportar auditorías efectivas.Este curso está diseñado para combinar la teoría con ejemplos prácticos, facilitando a los asistentes el entendimiento y aplicación de las **normativas de ciberseguridad** y la ejecución de **auditorías rigurosas** en sus organizaciones.

OBJETIVOS

- **Adquirir un conocimiento detallado de las principales normas y estándares de ciberseguridad**, tanto de carácter general como sectorial, incluyendo entornos industriales, cloud, financiero y sanitario, con énfasis en su aplicación práctica para garantizar el cumplimiento normativo.
- **Desarrollar competencias en la planificación y realización de auditorías de seguridad**, comprendiendo los activos a auditar, los controles necesarios y las metodologías aplicables (ISO 27001, ENS, etc.), así como la elaboración de informes y el rol del auditor durante todo el proceso.

PROGRAMA

1. Cumplimiento normativo. Revisión de aspectos principales de normas y estándares nacionales e internacionales:

- Transversales como ISO 27001, Esquema Nacional de Seguridad, ISO 22301 de continuidad de negocio, o NIST Cybersecurity Framework, entre otras.
- Normas del sector industrial como NIST SP 800-82 o ISA/IEC 62443.
- De entornos cloud, como ISO 27017, ISO 27018 o los recursos de la Cloud Security Alliance.
- De otros sectores de actividad, como el sanitario (HIPAA, ISO 27799…), marítimo, financiero, telecomunicaciones, transporte, energía, …
- De pagos electrónicos, como PCI-DSS.
- De firma electrónica.
- De privacidad.

Ejercicio: Plan de continuidad de negocio

2. Auditorías de Seguridad. Auditorías tanto generales y estratégicas, como técnicas. Trataremos aspectos como los activos a auditar, la definición de auditoría, los controles informáticos, cómo se hace una planificación de auditoría, cómo se elabora una auditoría técnica, en qué consiste el proceso EDR para conducirla, cómo se elaboran las auditorías de la ISO 27001 o ENS en la práctica, y cuál es el papel del auditor en todo este proceso.

- Activos de información
- Auditoría
- Controles informáticos
- Planificación
- Auditoría técnica
- Elementos de la auditoría
- EDR/ROA
- Auditorías ISO 27001
- El auditor
- Ejercicio: auditoría ISO 27001
- Ejercicio: auditoría ENS
- Ejercicio: auditoría técnica e informe

METODOLOGÍA

- 2 meses de formación teórico/práctica tutorizada.
- Plataforma de e-learning online.
- Avance flexible a ritmo del alumno.
- 2 bloques teóricos de contenido.
- Más de 20 vídeos de clases pregrabadas
- Ejercicios tipo test para autoevaluar conocimientos adquiridos tras cada lección.
- 4 actividades prácticas representativas (un 80-90% de las actividades en seguridad de la información GRC realizadas en el mundo profesional).
- 1 tutoría grupales en directo para la resolución de dudas.
- Referencias bibliográficas a nivel nacional e internacional (libros, normas, leyes, artículos, posts…).
- Normas, leyes y reglamentos nacionales o internacionales analizados.
- Soporte al alumno mediante foro.

Ventajas:

- Avanza de manera ordenada, y a tu propio ritmo
- Especializado y teórico/práctico
- Trato con tu tutor en las sesiones en directo
- Foro grupal con resto de alumnos para resolución de dudas
- Contenidos actualizados
- Cobertura multisectorial (IT, industrial, cloud, pagos electrónicos, protección de datos…)
- Actividad práctica muy detallada, con contexto teórico profundo, bibliografía, y propuesta de resolución. Enfocada a la vida real
- Tests de autoevaluación exhaustivos
- Formación desarrollada desde la práctica profesional
- Orientación laboral y múltiples salidas
- Menor competencia que en el ámbito de la seguridad informática (ciberseguridad)

COORDINACIÓN

Coordinación académica: Jesús Lizarraga

Formación

- Ingeniero Técnico Industrial por la Universidad del País Vasco (EHU)
- Ingeniero en Informática por Mondragon Unibertsitatea
- Máster (MSc) en Computación por Staffordshire University
- Instructor homologado de CCNA de CISCO
- Cursos de especialización en seguridad de redes y protección de datos

Experiencia

- Más de 30 años dedicados a la docencia universitaria y a la formación de profesionales en el ámbito de la informática
- Experiencia de más de 20 años en seguridad de la información
- CISO de Mondragon Unibertsitatea
- Coordinador del Máster en Ciberseguridad para profesionales

PERFIL DE SALIDA

El gobierno, riesgo y cumplimiento (GRC) en ciberseguridad es una pieza fundamental para las organizaciones que buscan proteger sus activos digitales, cumplir con normativas internacionales y gestionar riesgos de forma estratégica. Especializarse en esta **disciplina no solo ofrece oportunidades laborales diversas y de alta demanda, sino que también asegura un impacto significativo en el éxito de las organizaciones** actuales.

- Especialista en cumplimiento normativo: Este perfil adapta procesos y procedimientos internos para asegurar el cumplimiento de normativas como ISO 27001 o ENS, actuando como enlace entre los equipos de seguridad y las áreas legales.
- Auditor normativo: Especializado en identificar deficiencias en el cumplimiento de normativas específicas, el auditor normativo evalúa controles en entornos tradicionales, u otros como redes industriales, entornos cloud o sistemas IT.
