Mondragon Unibertsitatea

MICROCREDENCIAL UNIVERSITARIA ONLINE EN GOBIERNO DE LA SEGURIDAD Y ANÁLISIS DE RIESGOS

TEMÁTICA	Informática, Telecomunicaciones y Sistemas Empotrados
HORAS/ECTS	75 HORAS
CALENDARIO	15/09/2025 - 28/11/2025
IDIOMA	Español
MODALIDAD	Online

Más información e inscripción

PRESENTACIÓN

Este curso está diseñado para proporcionar a los participantes los conocimientos fundamentales sobre gobierno de la seguridad de la información y gestión de riesgos en las organizaciones. A lo largo de las sesiones, se explorarán conceptos clave como la planificación estratégica de la seguridad, modelos de gobierno y madurez, así como la identificación, análisis y tratamiento de los riesgos. Se trabajará con estándares y metodologías reconocidas, con un enfoque práctico que permitirá a los asistentes aplicar lo aprendido en entornos reales. Este curso combina una base teórica sólida con una actividad práctica orientada a que los participantes puedan implementar planes y acciones efectivas en gobierno de seguridad y gestión de riesgos en sus respectivas organizaciones.

OBJETIVOS

Comprender los principios del gobierno de la seguridad de la información y su importancia en la gestión estratégica de las organizaciones, abordando aspectos presupuestarios, políticas de seguridad y sistemas de gestión basados en modelos de madurez y marcos de referencia.
Desarrollar habilidades para identificar y gestionar riesgos de seguridad utilizando estándares y metodologías internacionales (ISO 31000, ISO 27005, MAGERIT, COBIT, OCTAVE, NIST), incluyendo el uso de herramientas y la realización de análisis prácticos aplicados a entornos reales.

DIRIGIDO A

Este itinerario formativo se concibe desde un ejercicio de síntesis de conocimientos en materia de ciberseguridad GRC: tratando de conjugar el ser lo suficientemente exhaustivos (en este sentido es de los más completos del mercado en la actualidad), y que pueda ser abordado en un tiempo razonable.

Se orienta principalmente a ejecutivos, líderes o profesionales de capas intermedias en el mundo corporativo o análogo, que buscan adquirir conocimientos en el ámbito de la seguridad de la información GRC con una formación a su ritmo, y que les permita incorporar la visión de ciberseguridad, buenas

prácticas y normativa asociada en su organización. No son necesarios conocimientos técnicos informáticos para la realización de este curso.

- La finalidad es proporcionar:
- Conocimiento en materia de ciberseguridad
- Herramientas para la toma de decisiones
- Soporte a la implantación de políticas, buenas prácticas y observancia de regulaciones.

De esta manera, les permitirá:

- A nivel personal o individual, robustecer su perfil con conocimientos de ciberseguridad GRC, en un mercado con una gran carencia de profesionales*.
- A nivel corporativo, incrementar la protección de sus organizaciones y por tanto reducir el nivel de riesgo en el cumplimiento de sus objetivos.

*Según el Observatorio de INCIBE (Instituto de Ciberseguridad de España), la brecha de talento en el mercado de ciberseguridad era de 22K profesionales en 2022, y crecerá hasta los 83K en 2024.

PROGRAMA

1. Introducción
2. Gobierno de la Seguridad. Una introducción a su necesidad, qué es la seguridad de la información, las dimensiones de la seguridad de los activos a proteger, aspectos económicos/presupuestarios del coste de la seguridad, qué es el gobierno de la seguridad, qué es un sistema de gestión de seguridad de la información y sus implicaciones, qué es un plan de director de seguridad y cómo elaborarlo en el mundo real, en qué consiste la metodología CMMI para evaluar el grado de madurez de los sistemas de una organización, las buenas prácticas de ITIL, y qué son los programas, políticas y procedimientos y su importancia, como base de la gestión de la ciberseguridad en una compañía.
- Introducción y necesidad
- Seguridad de la información
- Dimensiones de la seguridad
- Seguridad vs Presupuesto
- Gobierno de la Seguridad
- SGSI
- Plan Director de Seguridad
- CMMI
- ITIL
- Programas y políticas
Ejercicio: Política de Seguridad
Ejercicio: Plan Director de Seguridad
Ejercicio: Plan de Respuesta ante incidentes

3. Análisis de Riesgos. Introducción, estándares internacionales de gestión del riesgo ISO 31000 e ISO 27005 (Tecnologías de Ia Información), enfoques de gestión del riesgo y metodologías asociadas (MAGERIT, COBIT, OCTAVE, NIST SP 800-30 y SP 800-37), ejemplos de herramientas, y actividad práctica asociada.
- Introducción
- ISO 31000
- ISO 27005
- Metodologías: MAGERIT, COBIT, OCTAVE, NIST SP 800-30, NIST SP 800-37
- Herramientas
- Ejercicio: Análsiis de Riesgos

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 15 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.

- **Consultor o analista de seguridad de la información**: Lidera la implementación de medidas de seguridad para proteger los activos de información de una organización, diseñando controles tecnológicos y organizativos.
- **Analista o gestor de riesgos:** El gestor de riesgos se dedica a identificar y analizar los ciberriesgos a los que se enfrenta una entidad, proponiendo medidas que equilibren costes y beneficios.
