

## DATOS GENERALES

## Curso académico

|                             |  |
|-----------------------------|--|
| <b>Tipo de curso</b>        | Experto Universitario  |
| <b>Número de créditos</b>   | 15,00 Créditos ECTS  |
| <b>Matrícula</b>            | 295 euros (importe precio público)   |
| <b>Requisitos de acceso</b> | El curso de Experto Universitario en Ciberseguridad Empresarial está dirigido a titulados universitarios de cualquier rama de conocimiento o especialidad que quieran reforzar sus conocimientos en el área de la ciberseguridad. También está dirigido a titulados universitarios profesionales en puestos de gestión y liderazgo, directivos, consultores, profesionales técnicos o emprendedores que busquen adquirir o ampliar sus conocimientos cibernéticos. |
| <b>Modalidad</b>            | On-line  |
| <b>Lugar de impartición</b> | Online   |
| <b>Horario</b>              | Online   |

## Dirección

|                    |   |
|--------------------|---|
| <b>Organizador</b> | Departament d'Economia Aplicada   |
| <b>Dirección</b>   | Cristina Aybar Arias<br>Profesor/a Titular de Universidad. Departament d'Economia Aplicada. Universitat de València<br>Virgilio Pérez Giménez<br>Profesor/a Asociado de Universidad. Departament d'Economia Aplicada. Universitat de València |

## Plazos

|                                |                  |
|--------------------------------|------------------|
| <b>Preinscripción al curso</b> | Hasta 15/01/2023 |
| <b>Fecha inicio</b>            | Enero 2023       |
| <b>Fecha fin</b>               | Mayo 2023        |

## Más información

|                 |  |
|-----------------|--|
| <b>Teléfono</b> | 961 603 000  |
| <b>E-mail</b>   | <a href="mailto:informacion@adeituv.es">informacion@adeituv.es</a> |

## PROGRAMA

## Fundamentos de Ciberseguridad Empresarial

- Introducción a la ciberseguridad
- Diseño de la red corporativa
- Gestión de la información y monitorización
- Cultura de seguridad en la empresa
- Normativa vigente en materia de ciberseguridad
- Ciberinteligencia

## Ciberseguridad en la Cuarta Revolución Industrial

- Tipos de ataques cibernéticos y sus consecuencias
- Análisis de vulnerabilidades en la red corporativa
- Inversión en infraestructura digital
- Elaboración del Plan Director de Seguridad

## PROFESORADO

## Alejandro Aliaga Casanova

SOC Director en Disruptive Consulting SL

## Cristina Aybar Arias

Profesor/a Titular de Universidad. Departament d'Economia Aplicada. Universitat de València

## Noemí Brito Izquierdo

---

**Santiago González González**

Cuerpo Nacional de Policía (Escala Facultativa)

---

**Diego Núñez Macías**

Jefe Centro de Comunicaciones en Unidad Militar de Emergencias

---

**Virgilio Pérez Giménez**

Profesor/a Asociado de Universidad. Departament d'Economia Aplicada. Universitat de València

## OBJETIVOS

Las salidas profesionales que tiene el curso son:

Este programa formativo otorga a los participantes el conocimiento y la comprensión de los riesgos cibernéticos modernos, así como las estrategias para defenderse de los posibles ataques y valorar soluciones. Para ello, se darán a conocer las vulnerabilidades más habituales en las empresas y los métodos más utilizados por los ciberdelincuentes. También se darán a conocer diversas herramientas de prevención y protección existentes en la actualidad.

El objetivo del curso es proporcionar formación de alta cualificación en el ámbito de la ciberseguridad desde un enfoque empresarial.

Dicha formación permitirá gestionar los riesgos y amenazas de seguridad en entornos empresariales e industriales.

Al finalizar el curso los participantes serán capaces de:

- Comprender la importancia de la seguridad de la información.
- Comprender los fundamentos del riesgo cibernético.
- Diferenciar las diversas etapas de un ciberataque.
- Conocer las amenazas y vulnerabilidades más importantes en materia de ciberseguridad.
- Conocer los principales sistemas para la protección de la información.
- Conocer los métodos fundamentales para reducir los riesgos asociados a los ciberataques en el mundo empresarial.
- Conocer la estrategia de ciberseguridad nacional y los actores fundamentales que articulan sus líneas de actuación.
- Cuantificar el riesgo cibernético en términos comerciales.
- Valorar soluciones de ciberseguridad.

## METODOLOGÍA

Se utilizará una mezcla de teoría, práctica y lecturas de casos. Esta asignatura se aborda en metodología e-learning, con «Metodología de Presencia Virtual» con alta interacción entre alumnos y profesores, fomentándose un continuo flujo de comunicación y un proceso de aprendizaje dinámico, motivador y satisfactorio. Los alumnos pueden comunicarse e interactuar con sus compañeros y profesores tanto de forma asíncrona (foros de debate y/o correo electrónico), como en tiempo real (chat y videoconferencia). El desarrollo del trabajo se distribuye según una rigurosa planificación y se basará en documentación disponible en la plataforma para los participantes. Las unidades de estudio son semanales, por lo que esta asignatura comprende un total de 6 semanas. Cada semana lectiva comenzará en viernes, finalizando cada tema el jueves de la siguiente semana