



# Ciberseguridad

El Máster en Ciberseguridad se dirige a un perfil técnico y es requisito estar en posesión de un título de ingeniero o graduado en ingeniería informática, telecomunicaciones, en cualquiera de las especialidades, o de un título similar relacionado con las TIC. Los candidatos con otras titulaciones serán evaluados por el director del Máster. Se valorará la experiencia personal y formación complementaria al área de estudio, además de la motivación por realizar el programa.

Las salidas profesionales son:

- Chief Information Security Officer (CISO).
- Administrador de seguridad de red.
- Consultor de seguridad informática.
- Consultor de seguridad y hacking ético.
- Especialista de respuesta a incidentes de seguridad.
- Analista de ataques y seguridad.
- Responsable de seguridad de servicios de TI.
- Responsable de gestión de ciberseguridad.
- Técnico de ciberseguridad en infraestructuras críticas.
- Hacker ético.

## Características de este Máster

	<b>Inicio:</b> Octubre		<b>Lugar:</b> Escuela Politécnica Superior C/ Tutor 35 - Madrid
	<b>Duración:</b> 9 meses		<b>Modalidad:</b> Presencial
	<b>Idioma:</b> Español		<b>Director:</b> Teodoro Rojo Aladro <a href="mailto:teo.rojo@ceu.es">teo.rojo@ceu.es</a> Isaac Gutiérrez <a href="mailto:isaac.gutierrez@atalantago.com">isaac.gutierrez@atalantago.com</a>
	<b>Horario:</b> Viernes 16-21h. Sábados 9-14h		<b>Coordinador:</b> Teodoro Rojo Aladro <a href="mailto:teo.rojo@ceu.es">teo.rojo@ceu.es</a>



## Profesorado

El claustro está formado por profesionales expertos en ciberseguridad de empresas relevantes. Compartirán en el aula su experiencia y aprendizajes. Además, durante el curso se llevarán a cabo diversas charlas magistrales donde participarán CISOS (Chief Information Security Officer) de empresas e instituciones. Tendrás contacto directo con el ámbito de la ciberseguridad y sus principales protagonistas.

El estudiante podrá contactar con el profesorado para dudas y/o tutorías a través de las herramientas de comunicación de la plataforma del Campus Virtual Blackboard, a la que se accede desde la intranet de la Universidad CEU San Pablo (<https://intranet.ceu.es>).

<https://www.uspceu.com/oferta/master/ciberseguridad/profesorado>

## Plan de estudios

TIPO	CRÉDITOS
OBLIGATORIAS	48 ECTS
PRÁCTICAS EXTERNAS	6 ECTS
TRABAJO FIN DE MÁSTER	6 ECTS
<b>TOTAL</b>	<b>60 ECTS</b>



## PROGRAMA FORMATIVO

**MÓDULOS / MATERIAS****Módulo de protección y defensa (Blue Team): Diploma Universitario de Experto en Protección y Defensa en Ciberseguridad** 22

Diploma Universitario de Experto en Protección y Defensa en Ciberseguridad

Fundamentos del Networking

Monitorización de Seguridad (SIEM)

Gestión de Vulnerabilidades

Seguridad Perimetral

Seguridad en la Nube (Cloud)

Ciberinteligencia

Análisis Forense

DevSecOps

**Módulo Ofensivo (Red Team): Diploma Universitario de Experto en Ofensivo** 16

Fundamentos de Hacking (hacking core skills)

Seguridad de Redes

CEH – Certified Ethical Hacker

**Módulo de Gestión (White Team): Diploma Universitario de Experto en Gestión** 10

Sistema de Gestión de la Ciberseguridad y Aspectos Legales

Sistemas de Gestión de la Seguridad de la Información (ISO 27000)

Análisis de Riesgos

Legislación y Normas

Framework de Seguridad

Concienciación

Métricas de Gestión

**Prácticas Profesionales** 6

**Trabajo Final del Máster** 6



# Metodologías Docentes - Actividades Formativas

- Permite la especialización en un área o realizar el máster completo: nos adaptamos a las necesidades del estudiante ofertando 3 áreas de conocimiento distintas a las que puedes acceder por separado o sí se prefiere, realizar el máster completo.
- Compatible con el ejercicio profesional: Las clases se imparten viernes por la tarde y sábado por la mañana, permitiendo la compatibilidad con la jornada de trabajo.
- Se trabajará sobre un proyecto real: El Trabajo Fin de Máster es un caso real de una empresa en el que se espera la resolución de una necesidad. Se trabajará y presentará en grupo.
- Prácticas en los departamentos de ciberseguridad de grandes empresas: Se cuenta con convenios con empresas cotizadas y no cotizadas en las que el estudiante podrá realizar sus prácticas.
- Claustro formado por profesionales del sector y networking: el estudiante estará en contacto con expertos en ciberseguridad en el aula, además de acudir a charlas de CISOS de empresas e instituciones.
- El estudiante accederá a las mejores herramientas y a soluciones avanzadas de ciberseguridad: Firewalls / WAF (Web Application Firewall), Soluciones antimalware, Soluciones SIEM, Soluciones MFA, Soluciones gestión de identidad, Soluciones para hacer hacking, Soluciones para seguridad de aplicaciones (DevSecOps).

Las prácticas se realizarán usando recursos y soluciones ubicados en la nube. Los alumnos tendrán que completar los objetivos propuestos con fechas límite para la finalización.

## Sistemas y Criterios de Evaluación

### ASISTENCIA A CLASE

- Para poder acogerse al sistema de evaluación continua es precisa la asistencia al 75% de las clases de teoría (se realizarán controles de asistencia). Ya que el alumno puede faltar el 25% del total de las clases, no se admitirán justificaciones de ausencia.
- La realización de las sesiones prácticas es obligatoria en un 100%.



## SISTEMAS Y CRITERIOS DE EVALUACIÓN

- Los principales sistemas de evaluación en el máster son la valoración de las prácticas, la realización de trabajos y un examen final de cada módulo.

Por la peculiaridad de estos módulos, se tratan de manera diferenciada:

## Prácticas Externas

La Dirección del máster gestionará la asignación de entidad colaboradora de prácticas con el estudiante, que posteriormente será gestionada con el Departamento de Carreras Profesionales del Campus a través de la Plataforma de Gestión de Prácticas Externas.

El estudiante contará con un tutor académico de prácticas de la universidad y con un tutor en la entidad colaboradora de prácticas.

En la evaluación de esta asignatura, se tiene en cuenta la evaluación del tutor de la entidad colaboradora (60%), la Memoria de Prácticas (20%) y la evaluación del seguimiento realizado por el Tutor Académico (20%).

El número de horas presenciales a realizar en las entidades colaboradoras de prácticas externas será de 60 horas, preferiblemente en los meses de julio a septiembre.

Las entidades colaboradoras de prácticas con las que se tiene convenio están disponibles en la web del título.

## Trabajo Fin de Máster

El Trabajo Fin de Máster se realizará fundamentalmente en la segunda mitad del máster, aunque la concreción del título definido y asignación de director se realizará entre los meses de diciembre y enero.

El TFM consiste en la realización de un trabajo de investigación, contando con la tutela del director, para luego exponerlo y defenderlo ante un Tribunal.

La evaluación del TFM se realizará por rúbrica, valorando en un 75% el trabajo, y un 25% su exposición y defensa oral.

Desde la Dirección del Máster se informará del proceso de adjudicación de director, tutela, exposición y defensa y tribunal correspondiente.