

Máster de formación permanente en

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

	Inicio: Octubre		Lugar: Facultad de Humanidades Pº Juan XXIII 10. 28040 Madrid
	Duración: 9 meses		Modalidad**: Híbrida (semipresencial)
	Idioma: Español		Director: Teodoro Rojo Aladro teo.rojo@ceu.es Isaac Gutiérrez isaac.gutierrez@atalantago.com
	Horario*: Viernes 16-21h. Sábados 9-14h		Coordinador: Teodoro Rojo Aladro teo.rojo@ceu.es

* Se informará en el calendario del máster y en sus horarios de las actividades que requieran presencialidad y asistencia virtual síncrona.

** Las actividades formativas virtuales se impartirán de manera virtual y síncrona a través de la plataforma tecnológica Microsoft Teams. Asimismo, se contará con un Campus Virtual a través de la plataforma Blackboard.

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
TRABAJO FIN DE MÁSTER	12 ECTS
TOTAL	60 ECTS

PROGRAMA FORMATIVO	ECTS (60)
MÓDULO: PROTECCIÓN Y DEFENSA (BLUE TEAM)	19
(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	

PROGRAMA FORMATIVO	ECTS (60)
MÓDULO DE GESTIÓN (WHITE TEAM)	13
(DIPLOMA UNIVERSITARIO DE EXPERTO EN GESTIÓN)	
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	
MÓDULO: OFENSIVO (RED TEAM)	16
(DIPLOMA UNIVERSITARIO DE EXPERTO EN OFENSIVO)	
Fundamentos de hacking (hacking core skills)	
Seguridad de redes	
CEH – Certified Ethical Hacker	
MÓDULO TRABAJO FIN DE MÁSTER	12
TRABAJO FIN DE MÁSTER	
MÓDULO PRÁCTICAS EN EMPRESA	
PRÁCTICAS EN EMPRESA	9

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).

- Aunque el máster se imparte en modalidad semipresencial (híbrida), la mayor parte de las sesiones serán presenciales. Las sesiones online serán siempre síncronas, y se realizarán a través de la plataforma tecnológica Microsoft. Las pruebas de evaluación serán siempre presenciales.

Las actividades formativas que, en su caso, se desarrollen en modalidad online se impartirán con una metodología equivalente a la de las sesiones presenciales, adaptada al entorno virtual. Estas actividades podrán incluir la exposición y presentación de los contenidos por parte del profesorado, el análisis y resolución de ejercicios y casos prácticos, demostraciones, debates, actividades colaborativas, sesiones de resolución de dudas y seguimiento del aprendizaje, así como clases magistrales impartidas por expertos sobre competencias y temáticas transversales.

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. Los exámenes se realizarán en modalidad presencial.

Por la peculiaridad de los módulos que siguen, se tratan de manera diferenciada:

Prácticas Externas

El Máster no contempla la realización de prácticas externas curriculares. No obstante, el estudiante podrá realizar prácticas externas extracurriculares de carácter voluntario. En ese caso, el Coordinador del Máster orientará al estudiante en la selección y asignación de una entidad colaboradora adecuada a su perfil e intereses formativos. Una vez acordada dicha asignación, la gestión administrativa y formalización de las prácticas se llevará a cabo a través del Departamento de Carreras Profesionales.

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.

Las defensas de los TFM se realizarán en modalidad presencial.