

100% online



Continental  
International  
Universities

# **| Máster en Hacking y Ciberseguridad Empresarial**

Te conectamos con el mundo

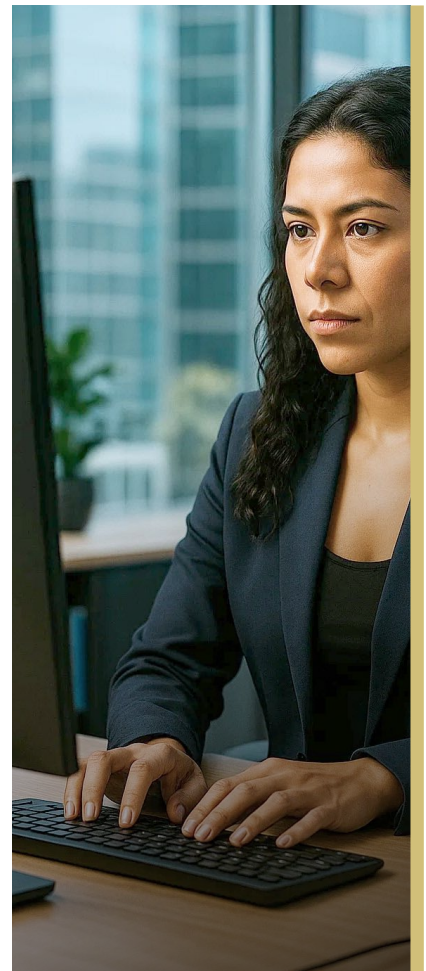
Estudia sin fronteras.

# ¿POR QUÉ ESTUDIAR EL MÁSTER EN HACKING Y CIBERSEGURIDAD EMPRESARIAL?

---

**En Continental International Universities te preparamos para liderar la protección de infraestructuras digitales en un contexto marcado por el incremento de ataques informáticos.**

El Máster en Hacking y Ciberseguridad Empresarial forma profesionales capaces de auditar sistemas, detectar vulnerabilidades, implementar defensas avanzadas y responder a incidentes con rigor técnico y ético. Atendiendo a la creciente demanda global de especialistas en seguridad digital, el programa prepara expertos que fortalecen la confianza en entornos digitales, protegen a usuarios, incluyendo menores, grupos vulnerables y pequeñas empresas; elevando los estándares de ciberprotección en organizaciones de cualquier sector.



# En CIU **obtendrás:**



## EXPERIENCIAS DE APRENDIZAJE

Enseñanza 100% virtual con **docentes internacionales** que te brindan perspectivas actuales en temas de tecnología, análisis de datos y liderazgo.



## COMUNIDAD INTERNACIONAL

Conecta y comparte ideas con compañeros de **diferentes países.**



## EDUCACIÓN EUROPEA

Estudia en España sin salir de casa y obtén una **formación global.**



## SEMANA INTERNACIONAL

Podrás participar de manera presencial en una **Semana Internacional en Madrid** con visitas empresariales, clases magistrales y actividades de networking.







## Objetivo del Máster



El Máster en Hacking y Ciberseguridad Empresarial tiene como objetivo desarrollar especialistas capaces de anticipar riesgos, evaluar la seguridad tecnológica y aplicar soluciones de protección avanzadas que fortalezcan la integridad digital de las organizaciones. El programa prepara a los participantes para actuar con criterios éticos, responder de manera estratégica ante incidentes y garantizar entornos más seguros para usuarios, empresas y comunidades vulnerables.

## Perfil del egresado

El egresado del Máster en Hacking y Ciberseguridad Empresarial se convierte en un líder capaz de fortalecer la resiliencia digital de organizaciones públicas, privadas y comunitarias, reduciendo la exposición a ciberataques, vulneraciones de privacidad y riesgos tecnológicos que comprometen la seguridad colectiva. Su formación combina criterio técnico, visión directiva y responsabilidad social, permitiéndole diseñar entornos digitales más seguros.

# Competencias **Generales**



## INNOVACIÓN TECNOLÓGICA ESTRATÉGICA

Transformar sistemas con tecnologías y datos.



## TRANSFORMACIÓN DIGITAL

Implementar estrategias organizacionales y tecnologías emergentes.



## GOBERNANZA ÉTICA Y SOSTENIBLE

Integrar ética y normativas para asegurar soluciones tecnológicas responsables.



## LIDERAZGO TRANSFORMADOR

Impulsar equipos multidisciplinares mediante pensamiento crítico y aprendizaje colaborativo.

# Competencias **Específicas**



**Protección Estratégica:** identificar y mitigar vulnerabilidades para elevar la seguridad y resiliencia digital.



**Gestión de Riesgos y Cumplimiento:** evaluar riesgos y aplicar marcos normativos para asegurar resiliencia y continuidad operativa.



**Seguridad Ética Aplicada:** implementar marcos de hacking responsable adaptados a distintos sectores con un enfoque ético.



**Gestión de Incidentes y Forense Digital:** mitigar brechas y fortalecer defensas de forma proactiva.



**Cumplimiento y Protección de Datos:** asegurar la integridad y conformidad legal aplicando ISO 27001 y el Reglamento General de Protección de Datos (GDPR).



**Responsabilidad Social:** actuar con integridad en pruebas de seguridad digital priorizando los impactos sociales.

# Ruta Profesional

---

## Puedes trabajar como:

- ✓ Director de Infraestructura y Seguridad Digital
- ✓ Director de Ciberseguridad (CISO)
- ✓ Coordinador de Seguridad Ofensiva (Red Team Lead)
- ✓ Coordinador de Arquitectura y Defensa Digital (Blue Team Lead)

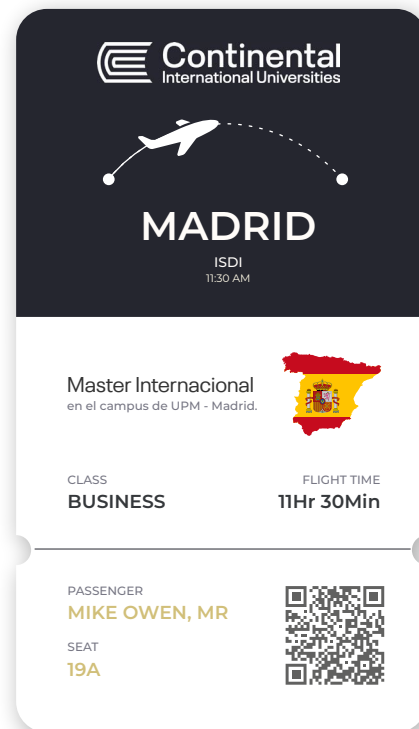
## Podrás desempeñarte en:



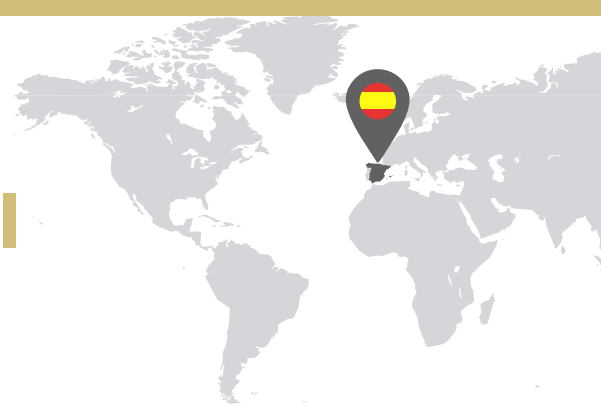
# SEMANA INTERNACIONAL

El Máster incluye una **Semana Internacional en Madrid** con visitas empresariales, clases magistrales y espacios de networking con profesionales de todo el mundo, disponible en modalidad presencial.

Al finalizar esta experiencia formativa, **recibirás un certificado oficial emitido por la Universidad Politécnica de Madrid (UPM)**, una de las instituciones académicas más prestigiosas de España, que respaldará tu desarrollo profesional a nivel internacional.



# Admisión Internacional



## ¿Cómo postular?

### Documentos si eres exalumno de Continental International Education (CIE):

- ✓ DNI
- ✓ Certificado Grado Bachiller
- ✓ Acta de convalidación

### Documentos que solicitamos a externos:

- ✓ Documento de Identificación
- ✓ Certificado de Bachiller
- ✓ Solicitud de admisión
- ✓ Pago de Matricula
- ✓ Certificado de trabajo mínimo de 3 años (formulario de autoevaluación de experiencia laboral y formulario de experiencia laboral de Jefe Inmediato)



Con respaldo de:



Fundación  
Universidad Empresa



POLITÉCNICA

\*Agenda una cita con nuestro asesor y conoce las opciones de becas disponibles.



# Malla Curricular

## Primer Trimestre

- I. Fundamentos de Ciberseguridad y Amenazas (8 ECTS)
- II. Liderazgo Transformador y Gestión del Cambio (3 ECTS)
- III. Herramientas Computacionales para la Innovación (5 ECTS)
- IV. Toma de decisiones (2 ECTS)

## Segundo Trimestre

- I. Gestión y Manejo de Crisis (2 ECTS)
- II. Análisis de Vulnerabilidades y Pentesting (8 ECTS)
- III. Aseguramiento de la Calidad (EQAVET) (5 ECTS)
- IV. IA aplicada al trabajo (3 ECTS)

## Tercer Trimestre

- I. Seguridad en Redes y Cloud (8 ECTS)
- II. Criptografía y Seguridad Aplicada (6 ECTS)
- III. Trabajo Final de Máster (10 ECTS)



**Modalidad:**  
En vivo + activ. asincrónicas



**Sesiones sincrónicas:**  
4 a 6 horas semanales

# Certificaciones Internacionales



Continental  
Florida  
University

## Emitidas por Continental Florida University (USA)

- 1. Análisis de Vulnerabilidades y Pentesting
- 2. Fundamentos de Ciberseguridad y Amenazas



