



MASTER EN FINTECH & BANCA DIGITAL

CIBERSEGURIDAD OFENSIVA FINANCIERA

Guia Docente / Syllabus 2025

ESAE Business School

European School of Administration and Enterprise

www.esae.es

01 DATOS BASICOS

Campo	Valor
Asignatura	Ciberseguridad Ofensiva Financiera
Titulacion	Especializacion en Fintech y Mercados Digitales
Escuela/Facultad	Escuela de Negocios y Economia Digital
Curso	Primero
ECTS	6
Caracter	Obligatorio
Idioma/s	Espanol e Ingles
Modalidad	Online
Semestre	Segundo
Curso academico	2025/2026
Docente coordinador	Dr. Roberto Sanchez Blanco (rsanchez@esae.es)

02 PRESENTACION

Esta asignatura aborda la ciberseguridad desde una perspectiva ofensiva, enseñando al estudiante a pensar como un atacante para mejorar significativamente las defensas de las organizaciones financieras. Se estudian vectores de ataque reales, técnicas de penetración utilizadas por grupos APT y metodologías de red teaming empleadas por equipos de seguridad de elite.

El estudiante aprenderá a realizar evaluaciones de seguridad completas, identificar vulnerabilidades críticas en infraestructuras financieras y diseñar controles de mitigación efectivos. Se enfatiza particularmente el cumplimiento de normativas específicas del sector como PCI-DSS para pagos, DORA para resiliencia operativa y las guías de la EBA sobre riesgos TIC.

El programa incluye laboratorios prácticos de hacking ético, simulaciones de incidentes de seguridad y ejercicios de respuesta a crisis. Se trabaja con herramientas profesionales utilizadas por pentesters y red teamers, siempre dentro de un marco ético y legal estricto.

03 RESULTADOS DE APRENDIZAJE

Al finalizar esta asignatura, el estudiante será capaz de demostrar los siguientes resultados de aprendizaje, alineados con las competencias del título y los descriptores de Dublin para el nivel de master:

3.1 Conocimientos

- CON1: Identificar y definir con precisión los conceptos fundamentales, teorías relevantes y actores principales que configuran el ámbito de estudio de esta asignatura, demostrando comprensión profunda del contexto sectorial y las dinámicas de mercado.
- CON2: Comprender de manera integral las dinámicas competitivas del mercado, los modelos de negocio predominantes y emergentes, así como las tendencias que están transformando el sector, permitiendo un análisis crítico de las oportunidades y amenazas.
- CON3: Distinguir las tecnologías habilitadoras clave y su aplicación práctica en contextos reales, evaluando su madurez, potencial disruptivo y las implicaciones para la estrategia empresarial y la operación de organizaciones financieras.
- CON4: Conocer en profundidad el marco regulatorio aplicable, las mejores prácticas sectoriales y los estándares internacionales, comprendiendo su evolución y anticipando cambios que puedan afectar a los modelos de negocio.

3.2 Habilidades

- HAB1: Analizar casos de estudio complejos aplicando de forma rigurosa frameworks teóricos y metodológicos, sintetizando información de múltiples fuentes y generando conclusiones fundamentadas y recomendaciones accionables.
- HAB2: Diseñar soluciones innovadoras y viables para problemas complejos del sector financiero, integrando conocimientos técnicos, estratégicos y regulatorios, y considerando las restricciones operativas y los requisitos de los diferentes stakeholders.

3.3 Competencias

- COMP01: Liderar con autonomia proyectos de transformacion e innovacion en el ambito de la asignatura, demostrando capacidad de toma de decisiones en contextos de incertidumbre, comunicacion efectiva con diferentes audiencias y vision estrategica a largo plazo.

04 CONTENIDOS

1. Panorama de Amenazas Financieras: APTs contra bancos, ransomware financiero y ataques a infraestructura critica SWIFT
2. Vectores de Ataque: Phishing avanzado, social engineering, business email compromise y supply chain attacks
3. Penetration Testing: Metodologias OWASP, PTES, OSSTMM y ejecucion practica de pentests en entornos financieros
4. Red Teaming: Simulacion de adversarios APT, evaluaciones de seguridad avanzadas y purple teaming
5. Seguridad en Aplicaciones Fintech: APIs financieras, mobile banking, pagos digitales y Open Banking
6. Cumplimiento y Respuesta: PCI-DSS, DORA, gestion de incidentes NIST, BCP/DRP y comunicacion de crisis

05 METODOLOGIAS DE ENSEÑANZA-APRENDIZAJE

La asignatura emplea un conjunto diversificado de metodologias pedagogicas disenadas para maximizar el aprendizaje activo y la aplicacion practica de conocimientos en contextos profesionales reales:

- Clases sincronas mediante videoconferencia (Zoom): Sesiones interactivas en tiempo real donde el profesorado presenta conceptos clave, facilita discusiones y responde preguntas. Se fomenta la participacion activa mediante polls, breakout rooms y ejercicios colaborativos.
- Metodo del caso virtual: Analisis detallado de casos reales del sector fintech, fomentando el pensamiento critico, la toma de decisiones bajo incertidumbre y el debate fundamentado entre estudiantes con diferentes perspectivas y experiencias.
- Aprendizaje Basado en Problemas (ABP) online: Resolucion de retos empresariales reales proporcionados por empresas colaboradoras, integrando conocimientos de multiples areas y desarrollando competencias de trabajo en equipo distribuido.
- Aprendizaje cooperativo en entornos virtuales: Proyectos grupales que fomentan la colaboracion, la division eficiente del trabajo y el desarrollo de habilidades de comunicacion y coordinacion en equipos remotos.
- Foros de discusion guiados: Debates asincronos moderados por el profesorado sobre temas de actualidad, fomentando la reflexion critica, la argumentacion fundamentada y el aprendizaje entre pares.
- Videoclases y recursos asincronos: Contenidos multimedia de alta calidad disponibles en el campus virtual para estudio autonomo, incluyendo videos explicativos, podcasts con expertos y materiales de lectura complementarios.
- Tutorias virtuales individuales y grupales: Sesiones de orientacion personalizada para resolver dudas, profundizar en temas de interes y proporcionar feedback sobre el progreso academico.

06 ACTIVIDADES FORMATIVAS

Actividad formativa	Horas
Clases sincronas (videoconferenci...	20
Lectura de materiales y recursos c...	25
Actividades individuales: casos, pr...	35
Actividades colaborativas virtuales	15
Participacion en foros y debates	10
Tutorias virtuales	15
Autoevaluacion y pruebas de cono...	10
Estudio autonomo	20
TOTAL	150

07 EVALUACION

Sistema de evaluacion	Peso (%)
Pruebas de conocimiento online	40
Análisis de casos y resolución de ...	25
Proyectos/informes escritos	15
Exposiciones orales (videoconferencia...)	10
Participación en foros y debates	10
TOTAL	100

7.1 Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria, el estudiante deberá obtener una calificación final igual o superior a 5,0 sobre 10,0. Será requisito indispensable obtener una calificación mínima de 5,0 en la prueba final de conocimientos para que esta pueda hacer media con el resto de actividades evaluables. La evaluación continua representa el 60% de la calificación final y permite al estudiante demostrar su progreso a lo largo del semestre.

7.2 Convocatoria extraordinaria

En la convocatoria extraordinaria se aplican los mismos requisitos y criterios de evaluación que en la convocatoria ordinaria. El estudiante deberá entregar las actividades evaluables no superadas o no presentadas durante el curso, tras recibir las indicaciones y correcciones correspondientes del equipo docente. Se mantiene el requisito de obtener mínimo 5,0 en la prueba final para hacer media. El profesorado proporcionará orientación específica para la preparación de esta convocatoria.

08 CRONOGRAMA

Actividad evaluable	Fecha
Actividad individual 1	Semana 3-4
Actividad individual 2	Semana 6-7
Actividad individual 3	Semana 9-10
Actividad grupal	Semana 14

09 BIBLIOGRAFIA

Obra de referencia

- Stuttard, D. & Pinto, M. (2011). The Web Application Hacker's Handbook. Wiley.

Bibliografía recomendada

- Weidman, G. (2014). Penetration Testing. No Starch Press.
- Kim, P. (2018). The Hacker Playbook 3. Secure Planet.
- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.
- ENISA. (2020). Threat Landscape for the Financial Sector.

10 UNIDAD DE ORIENTACION EDUCATIVA Y DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad de ESAE Business School ofrecemos un servicio integral de acompañamiento a todos los estudiantes, con el objetivo de facilitar el logro de sus metas académicas y profesionales, garantizando la inclusión y la accesibilidad universal en todos nuestros programas.

Desde esta Unidad se ofrece a los estudiantes los siguientes servicios:

1. Acompañamiento y seguimiento personalizado: Realizamos asesorías individuales y seguimiento continuo del progreso académico, identificando de forma temprana posibles dificultades y diseñando planes de acción específicos para superarlas. Nuestro equipo de orientadores está disponible para consultas tanto sincrónicas como asincrónicas.
1. Atención a la diversidad: Realizamos ajustes curriculares y metodológicos razonables para estudiantes con necesidades específicas de apoyo educativo, garantizando la igualdad de oportunidades. Esto incluye adaptaciones en formatos de materiales, tiempos de exámenes y metodologías de evaluación cuando sea necesario.
1. Recursos formativos extracurriculares: Ofrecemos a los estudiantes diferentes recursos formativos complementarios al plan de estudios, incluyendo talleres de habilidades de estudio, gestión del tiempo, técnicas de presentación, preparación para certificaciones profesionales y desarrollo de competencias transversales.
1. Orientación vocacional y profesional: Proporcionamos herramientas y acompañamiento para la definición del proyecto profesional, incluyendo sesiones de coaching, revisión de CV, preparación de entrevistas, networking con antiguos alumnos y conexión con oportunidades laborales en el sector fintech.

Contacto: orientacioneducativa@esae.es

11 ENCUESTAS DE SATISFACCIÓN

Te animamos encarecidamente a participar en las encuestas de satisfacción que estarán disponibles en el campus virtual al finalizar cada bloque temático y al concluir la asignatura. Tu opinión y valoración son fundamentales para la mejora continua de la calidad de la titulación y de la experiencia formativa de futuros estudiantes.

Las encuestas son completamente anónimas y los resultados agregados se analizan cuidadosamente por el equipo académico para identificar áreas de mejora en contenidos, metodologías, materiales y atención al estudiante. Cada sugerencia es valorada y, cuando es viable, implementada en siguientes ediciones del programa.

Tu participación activa en este proceso de evaluación continua contribuye directamente a la excelencia académica que caracteriza a ESAE Business School y nos ayuda a mantenernos como referentes en la formación de profesionales fintech. Agradecemos sinceramente tu tiempo y tu compromiso con la mejora de nuestro programa.

Muchas gracias por tu participación.

ESAE Business School

FORMANDO LIDERES FINTECH

www.esae.es

Madrid, Espana | info@esae.es

2025 ESAE Business School