

FICHA MATERIA MÁSTER PROPIO

O nome da materia debe indicarse en galego, castelán e inglés mentres que o resto dos apartados deberanse cubrir no idioma en que se impartirá o título propio

NOME MATERIA (Galego): Ciberoperacións Ofensivas		
NOME MATERIA (Castelán): Ciberoperaciones Ofensivas		
NOME MATERIA (Inglés): Offensive cyberoperations		
Módulo/Especialidade:		
Tipo: <input checked="" type="checkbox"/> Obrigatoria <input type="checkbox"/> Optativa		
ECTS TOTALES: 7,5	ECTS TEORICOS: 7,5	ECTS PRÁCTICOS:
Semestre/Cuadrimestre:Primeiro		
Modalidade: Síncrona virtual		
COMPETENCIAS ASOCIADAS: CG1, CG2, CE2, CE6, CE7, CE9 Indicar códigos da táboa 2.3 da proposta		
Descrición general: Esta materia proporciona una formación avanzada sobre las principales técnicas de ciberataque usadas en ciberoperaciones ofensivas en escenarios reales, con el objetivo de comprender las tácticas, técnicas y procedimientos (TTPs) empleadas por actores maliciosos y adversarios en el ciberespacio. La materia se centra en proporcionar a los alumnos una visión estratégica y operativa de los ciberataques en entornos críticos y estratégicos. A través de un enfoque práctico, el estudiante adquirirá conocimientos sobre la identificación y explotación de vulnerabilidades web , ataques a redes inalámbricas, denegación de servicio (DoS/DDoS) , ingeniería social , ataques a sistemas de autenticación , y el impacto de la inteligencia artificial adversarial (Adversarial Machine Learning) en la evolución de las ciberamenazas. El curso analizará cómo estas técnicas pueden ser utilizadas en ciberinteligencia y en ciberoperaciones , tanto desde un enfoque ofensivo como defensivo. Se explorará el uso de herramientas y frameworks de explotación de vulnerabilidades, además de estudiar los métodos empleados por adversarios para evadir mecanismos de detección y respuesta.		
Coordinador/a: Miguel Rodríguez Pérez Equipo docente: 1) Miguel Rodríguez Pérez 2) Raúl F. Rodríguez Rubio 3) Carlos Rivas Costa		

Resultados de aprendizaje:

Al finalizar la materia, el estudiante será capaz de:

1. **Identificar y explotar vulnerabilidades en aplicaciones web**
2. **Comprender y ejecutar ataques de Denegación de Servicio (DoS y DDoS)**, analizando las técnicas más utilizadas y explorando mecanismos de defensa y mitigación.
3. **Llevar a cabo ataques dirigidos contra redes inalámbrica.**
4. **Analizar y explotar debilidades en sistemas de autenticación y explotación de credenciales** en entornos críticos.
5. **Aplicar técnicas de ingeniería social** para evaluar y explotar la vulnerabilidad humana en el ámbito de la seguridad informática.
6. **Explorar técnicas de Adversarial Machine Learning (AML)**, entendiendo cómo los atacantes pueden manipular modelos de inteligencia artificial y aprendizaje automático para evadir la detección o degradar su desempeño.

Programa académico:

1. Identificación y Explotación de Vulnerabilidades Web
2. Ataques de Denegación de servicio (DoS y DDoS)
3. Ciberataques en Redes inalámbricas
4. Ataques a sistemas de Autenticación
5. Ingeniería social
6. *Adversarial Machine Learning*

Metodoloxía docente:

Durante el bimestre se imparten 50 horas de clase síncrona a través de videoconferencia. En estas clases se alternan explicaciones teóricas con la realización de actividades, ejercicios y demostraciones de tipo práctico por parte del profesorado. Cada dos semanas, se dedica una hora de clase semanal a realizar una tutoría grupal para resolver dudas, aclarar conceptos, etc.

Tras cada sesión de clase se proponen tareas en el aula virtual, esencialmente de tipo práctico, que debe realizar de forma asíncrona y autónoma cada alumno y deben ser entregadas dentro de los plazos establecidos.

Competencias asociadas	Actividades formativas SÍNCRONAS	Horas síncronas presenciais	Horas síncronas virtuais	Horas de traballo autónomo do estudante
	Clase magistral		50	100
	Tutoría grupal		5	0
	Pruebas de evaluación		5	27,5
	ECTS TOTALES = 7,50	0,00	60,00	127,50

Las horas síncronas estarán comprendidas entre 8 y 12 por ECTS en modalidade síncrona

Competencias asociadas	Actividades formativas ASÍNCRONAS	Horas titorización	Horas de traballo autónomo do estudante
	ECTS TOTALES = 0,00	0,00	0,00

Las horas de titorización estarán comprendidas entre 4 e 8 por ECTS en modalidade asíncrona

Metodoloxía de avaliación:

Se usará un **mecanismo de avaliación continua** que consiste, por un lado, en la realización a lo largo del período de docencia de **tareas** asociadas a los distintos temas, que deben ser entregadas en los plazos establecidos y, por otro lado, la realización de varias **pruebas intermedias de avaliación** para verificar la adecuada adquisición de conocimientos.

Cada **tarea** permite obtener una cantidad de puntos variable que depende de la dificultad y tiempo estimado de dedicación. Las tareas suman 1000 puntos en total.

Las **pruebas intermedias** consisten en cuestionarios con preguntas en las que hay que elegir la opción correcta entre varias opciones de respuesta. Se trata de 5 pruebas de 1 hora que se realizarán de forma síncrona a través de la plataforma MooVi mediante *Safe Exam Browser* y el uso obligatorio de una cámara durante la realización de la prueba. Todas las pruebas intermedias se puntúan entre 0 y 10 y poseen el mismo peso sobre la nota final (10%).

Para superar la materia es necesario realizar el 80% de las tareas, obteniendo una puntuación mínima de 500 puntos, y obtener una media de 5.0 en las 5 pruebas de avaliación. En ese caso, la calificación final de la materia se obtiene como:

$$CF = 0,5*(TOTAL_TAREAS)/100 + 0,1*(P1+P2+P3+P4+P5)$$

La **Segunda oportunidad de avaliación** consistirá en la entrega de un conjunto de tareas propuestas dentro del plazo señalado en el mes de Junio, y en la realización de un único examen oral de en torno a 1 hora de duración sobre el contenido teórico de toda la materia, así como sobre las tareas entregadas

Competencias avaliadas	Probas de avaliación	% Ponderación
	Tareas en aula virtual	50
	Pruebas intermedias de avaliación	50
		100%

Plataformas de Teledocencia e titorización:

Las clases síncronas se imparten a través de Campus Remoto. Toda la documentación y comunicación relacionada con el curso se realiza a través de una materia en MooVi. En dicha materia de MooVi se publicarán también las distintas tareas, en las que deben realizarse las entregas dentro del plazo establecido y donde el profesorado realizará su evaluación. Las calificaciones de todas las tareas y pruebas de avaliación serán visibles en MooVi. Se habilitará adicionalmente un foro en la materia de MooVi para la resolución colaborativa de dudas.