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 defensivas		
NOME MATERIA (Castelán): Ciberoperaciones defensivas		
NOME MATERIA (Inglés): Defensive cyberoperations		
Módulo/Especialidade:		
Tipo: ☒ Obrigatoria ☐ Optativa		
ECTS TOTALES: 7,5	ECTS TEORICOS: 7,5	ECTS PRÁCTICOS:
Semestre/Cuadrimestre:Segundo		
Modalidade: Síncrona virtual		
COMPETENCIAS ASOCIADAS: CG2, CG3, CE2, CE6, CE7, CE8, CE9		
Indicar códigos da táboa 2.3 da proposta		
Descrición general:		
<p>Esta materia ofrece una formación integral y práctica sobre las ciberoperaciones defensivas en sectores estratégicos para la seguridad nacional, donde la gestión y respuesta eficiente a ciberincidentes es clave para garantizar la resiliencia operativa de sistemas críticos y redes militares.</p> <p>El contenido abarca el ciclo completo de gestión de incidentes, comenzando por la fase de preparación para minimizar vectores de ataque, seguido de la monitorización continua mediante registro de logs y despliegue de plataformas SIEM, donde se hace especial hincapié en la aplicación de inteligencia artificial para la detección temprana y el triaje automatizado de eventos sospechosos.</p> <p>La materia profundiza en técnicas de análisis forense digital (DFIR) aplicadas a entornos operativos, utilizando herramientas avanzadas como Velociraptor IR. Asimismo, se aborda la respuesta a incidentes, haciendo de nuevo especial hincapié en la mitigación y recuperación mediante el uso de inteligencia artificial y el uso de herramientas SOAR (Security Orchestration, Automation, and Response).</p> <p>Por último, el alumnado adquirirá competencias en Threat Hunting, también valiéndose de la aplicación de la inteligencia artificial, adoptando una mentalidad proactiva que permite anticiparse a las amenazas avanzadas persistentes (APT) y detectar actividades maliciosas ocultas antes de que se materialicen como incidentes críticos.</p>		
Coordinador/a: José Carlos López Ardao		
Equipo docente:		
1) José Carlos López Ardao		
2) Yolanda Blanco Fernández		
3) Andrés Suárez González		
4) Miguel Rodelgo Lacruz		

Resultados de aprendizaje:

Al finalizar la materia, el estudiante será capaz de:

1. **Explicar el ciclo de vida completo de la gestión y respuesta a ciberincidentes**, comprendiendo las fases de preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.
2. **Desplegar y operar plataformas de monitorización y detección (SIEM)**, configurando la recogida de logs, definiendo reglas de correlación y aplicando criterios de clasificación y triaje de incidentes.
3. **Emplear inteligencia artificial en el proceso de monitorización y triaje**, integrando capacidades de aprendizaje automático y análisis predictivo en plataformas SIEM.
4. **Realizar análisis forense digital (DFIR)** utilizando herramientas como **Velociraptor**, identificando trazas de actividad maliciosa y obteniendo evidencias digitales útiles para el análisis post-incidente.
5. **Emplear inteligencia artificial en los procedimientos de respuesta a incidentes**, incluyendo acciones de contención, mitigación y recuperación en entornos operativos, adaptando las respuestas al impacto y la criticidad de los activos afectados.
6. **Utilizar Playbooks y procedimientos normalizados** para guiar la respuesta coordinada a ciberincidentes, asegurando la alineación con los procedimientos establecidos por las Fuerzas Armadas y organismos de seguridad.
7. **Aplicar técnicas de Threat Hunting** proactivas para identificar amenazas ocultas o actividad maliciosa latente, utilizando herramientas de análisis avanzado, inteligencia artificial y técnicas basadas en inteligencia de amenazas (Threat Intelligence).
8. **Elaborar informes post-incidente adaptados a distintos niveles (técnico, operativo, estratégico)**, asegurando la adecuada transferencia de conocimiento para mejorar la preparación futura.

Programa académico:

1. Introducción a la Gestión y Respuesta de Incidentes: Ciclo de vida aplicado a los sectores estratégicos
2. La fase de preparación: Herramientas de ciberdefensa.
3. Monitorización: Registro de logs. Despliegue y operaciones de un SIEM. Clasificación y Triage de ciberincidentes. Uso de IA en el SIEM.
4. Análisis Forense. Uso de herramientas DFIR (Velociraptor IR)
5. Respuesta a Incidentes (IR): Contención, Mitigación y Recuperación. Velociraptor para IR. Aplicación de la IA a los procedimientos de respuesta a incidentes. Herramientas SOAR (**Security Orchestration, Automation, and Response**).
6. Caza de amenazas (*Threat Hunting*): Herramientas de análisis avanzado. Aplicación de inteligencia artificial en la caza de amenazas. Técnicas de caza basadas en ciberinteligencia.

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 oportunidade 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.