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): Técnicas de Ciberintelixencia		
NOME MATERIA (Castelán): Técnicas de Ciberinteligencia		
NOME MATERIA (Inglés): CyberThreat Intelligence Techniques		
Módulo/Especialidade:		
Tipo: ☒ Obrigatoria ☐ Optativa		
ECTS TOTALES: 7,5	ECTS TEORICOS: 7,5	ECTS PRÁCTICOS:
Semestre/Cuadrimestre:Primeiro		
Modalidade: Síncrona virtual		
COMPETENCIAS ASOCIADAS: CG1, CG2, CG3, CG4, CE1, CE2, CE7, CE8, CE10		
Indicar códigos da táboa 2.3 da proposta		
Descrición general:		
<p>Esta materia proporciona una formación avanzada en las técnicas y metodologías clave para la recolección, análisis y difusión de inteligencia de ciberamenazas, con un enfoque práctico aplicado a la detección, prevención y respuesta ante ciberataques.</p> <p>Se explorarán herramientas y metodologías para el análisis estructurado de amenazas, incluyendo el uso de Maltego para la correlación de datos, el análisis de redes sociales para la identificación de actores maliciosos y la aplicación de técnicas de análisis estructurado en la producción de inteligencia. Además, se abordará la difusión y compartición de inteligencia en entornos colaborativos de ciberseguridad, estudiando el uso de plataformas de inteligencia de amenazas (MISP) para la gestión y distribución de Indicadores de Compromiso (IoCs) y tácticas, técnicas y procedimientos (TTPs) de actores maliciosos.</p> <p>Por último, la asignatura profundiza en la aplicación de Inteligencia Artificial (IA) en la generación de inteligencia de amenazas, explorando cómo el procesamiento del lenguaje natural (NLP) permite la detección automatizada de amenazas emergentes en fuentes OSINT, foros clandestinos, redes sociales y la dark web, permitiendo la anticipación a ataques y campañas maliciosas.</p>		
Coordinador/a: José Carlos López Ardao		
Equipo docente:		
1) José Carlos López Ardao		
2) Andrés Suárez González		
3) Alberto Gil Solla		

Resultados de aprendizaje:

Al finalizar la materia, el estudiante será capaz de:

1. **Aplicar inteligencia de amenazas en la detección y prevención de ciberataques**, correlacionando datos de diferentes fuentes y contextualizando amenazas en el marco estratégico de la ciberdefensa.
2. **Utilizar herramientas de análisis visual y correlación de datos** como **Maltego**, para mapear relaciones entre actores, infraestructuras y campañas de amenazas.
3. **Implementar técnicas de análisis estructurado** en la producción de inteligencia de ciberamenazas
4. **Aplicar análisis de redes sociales** para la identificación de amenazas y actores maliciosos, evaluando el impacto de campañas de desinformación, propaganda y operaciones psicológicas en el ciberespacio.
5. **Integrar plataformas de compartición de inteligencia (MISP)** en el flujo de trabajo de ciberinteligencia, gestionando Indicadores de Compromiso (**IoCs**) y tácticas, técnicas y procedimientos (**TTPs**) de actores hostiles.
6. **Emplear inteligencia artificial para el análisis automatizado de fuentes OSINT**, procesando grandes volúmenes de datos con herramientas avanzadas para identificar tendencias y amenazas emergentes.
7. **Utilizar técnicas de Procesamiento de Lenguaje Natural (NLP) para la detección de amenazas en redes sociales, foros clandestinos y la dark web**, desarrollando capacidades de alerta temprana para detectar amenazas emergentes y exploits de día cero.
8. **Desarrollar productos de inteligencia técnica, operativa y estratégica**, aplicando técnicas de análisis avanzado y automatización en la generación de informes para la toma de decisiones en ciberdefensa.

Programa académico:

1. Análisis de inteligencia de ciberamenazas:
 - Aplicación de inteligencia de amenazas en la detección y prevención de ciberataques.
 - Herramientas visuales de análisis: Maltego
 - Técnicas de Análisis Estructurado.
 - Análisis de Redes Sociales.
2. Difusión y Compartición de Inteligencia.
 - Plataformas de Inteligencia de Amenazas: MISP.
3. Uso de IA para Generación de Inteligencia de Amenazas:
 - Análisis de fuentes OSINT.
 - Uso de NLP para identificar amenazas emergentes y exploits de día cero en foros, redes sociales, dark web.

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.