Escola Aberta
de Formación Permanente
Universidade Vigo

# 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): Introducción á Intelixencia de Ciberamenazas | | |
| NOME MATERIA (Castelán): Introducción a la Inteligencia de Ciberamenazas | | |
| NOME MATERIA (Inglés): Introduction to CyberThreat Intelligence | | |
| 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, CG4, CE1, CE8, CE10<br>Indicar códigos da táboa 2.3 da proposta | | |

Descrición general:

Esta materia introduce al estudiante en los fundamentos, técnicas y metodologías esenciales para la obtención, análisis y producción de **inteligencia de ciberamenazas**, con un enfoque adaptado a los requisitos operativos y estratégicos de la **ciberdefensa** en el ámbito de la seguridad en sectores estratégicos y de la defensa nacional.
A través de un recorrido completo por el **ciclo de inteligencia**, el alumno comprenderá cómo se transforma la información técnica y contextual en productos de inteligencia útiles para la **toma de decisiones** en ciberoperaciones, tanto ofensivas como defensivas. Se trabajarán las **tipologías de inteligencia** (táctica, técnica, operativa y estratégica), así como los criterios de calidad y veracidad esenciales en entornos críticos.
El programa profundiza sobre todo en la aplicación práctica de técnicas de **Inteligencia de Fuentes Abiertas (OSINT)**, adaptadas al entorno digital y al análisis de amenazas, incluyendo la obtención de información sobre **infraestructuras** y **personas**, la exploración de **la Dark Web** y el uso de herramientas especializadas para la **cibervigilancia** de sectores estratégicos.
Además, se aborda la **Seguridad Operacional (OpSec)** aplicada a operaciones de ciberinteligencia, garantizando la protección de la identidad, las fuentes y la propia operación de obtención, empleando técnicas de **anonimización**, uso de **VPN**, **Tor** y otras herramientas de **privacidad operativa**.
Por último, el alumno adquirirá competencias en la **generación y consumo de productos de inteligencia técnico/táctica**, aplicando **estándares y patrones de intercambio** como **STIX/TAXII** y técnicas específicas como las **reglas Yara, Sigma, Suricata y Snort**, esenciales para traducir la ciberinteligencia en acciones defensivas concretas.

Coordinador/a: José Carlos López Ardao
Equipo docente:
1) José Carlos López Ardao
2) Sergio Herrería Alonso
3) Carlos Rivas Costa

Resultados de aprendizaje:
Al finalizar la materia, el estudiante será capaz de:

1. **Comprender el concepto, el propósito y la utilidad de la inteligencia de ciberamenazas** en el contexto de la seguridad y defensa nacional. Diferenciar los niveles de inteligencia: **táctica, operativa, estratégica y técnica**, y su aplicación en ciberoperaciones.
2. **Aplicar el ciclo de inteligencia al ámbito de la ciberinteligencia**, gestionando las fases de obtención, procesamiento, análisis, difusión y retroalimentación.
3. **Implementar medidas de Seguridad Operacional (OpSec)** en actividades de obtención y análisis, garantizando la protección de la identidad de los analistas, las fuentes y los productos generados.
4. **Realizar actividades de obtención y análisis de Inteligencia de Fuentes Abiertas (OSINT)** aplicadas a infraestructuras de red, personas, información técnica y táctica procedente de la **Dark Web** y foros clandestinos.
5. **Identificar y utilizar fuentes fiables de inteligencia de amenazas**, integrando información procedente de organismos internacionales, centros de respuesta a incidentes y plataformas de intercambio de inteligencia.
6. **Aplicar herramientas y frameworks OSINT** para automatizar la obtención y análisis de información en fuentes abiertas.
7. **Generar productos de inteligencia técnica adaptados a distintos niveles de mando**, aplicando formatos y patrones normalizados así como **reglas de detección basadas en inteligencia técnica.**
8. **Correlacionar la ciberinteligencia técnica con la inteligencia operativa y estratégica**, asegurando su integración en el ciclo de toma de decisiones de las ciberoperaciones en sectores estratégicos.

Programa académico:

1. Introducción a la Inteligencia de Ciberamenazas.
    - Concepto y propósito de la inteligencia de amenazas.
    - El ciclo de inteligencia aplicado a la ciberseguridad.
    - Tipos de inteligencia: táctica, operativa, estratégica y técnica.
2. Seguridad de las operaciones (OpSec)
    - Principios y técnicas de seguridad operativa en entornos de ciberinteligencia.
    - Protección de la identidad y las fuentes de información.
    - Anonimización, uso de VPN, Tor y herramientas de privacidad.
3. Inteligencia de fuentes abiertas (OSINT).
    - Métodos y herramientas para la recopilación y análisis de información en fuentes abierta
    - OSINT para infraestructura de red y de personas.
    - Fuentes de inteligencia de amenazas. Frameworks OSINT
    - Dark Web. Cibervigilancia.
4. Generación y consumo de ciberinteligencia:
    - Generación de productos de inteligencia técnica.
    - Patrones STIX/TAXII, OpenIOC
    - Reglas Yara, Sigma, Suricata y Snort

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 evaluación 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 evaluación** 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 evaluación. 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 evaluación** 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 evaluación | 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 evaluación serán visibles en MooVi. Se habilitará adicionalmente un foro en la materia de MooVi para la resolución colaborativa de dudas.