Guía Docente
Curso Académico 2026/27

Datos Generales

Asignatura: THREAT INTELLIGENCE- INTELIGENCIA DE AMENAZAS
Titulación: GRADO EN CIBERSEGURIDAD
Carácter: OBLIGATORIA.
Créditos ECTS: 6 ECTS
Curso: 3º
Distribución temporal: 1º SEMESTRE.
Idioma de impartición: CASTELLANO.
Equipo docente: Javier Valencia
Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura orientada al análisis, recopilación y uso estratégico de inteligencia de amenazas para anticipar, identificar y mitigar riesgos en entornos digitales. Se trabajará con metodologías para la detección proactiva de ciberamenazas, el análisis de indicadores de compromiso y el uso de fuentes abiertas y plataformas especializadas para generar conocimiento accionable.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)[1]

Contenidos o conocimientos (C)	C1	Desarrollar habilidades de cálculo para el análisis en los lenguajes de programación.
	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C3	Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.
	C6	Identificar distintas tipologías de virus informáticos.
	C7	Reconocer técnicas antiforense y su aplicación.

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	C8	Aplicar bases matemáticas y técnicas de diseño de algoritmos a la criptografía y ciberseguridad.
	C11	Conocer las diferentes topologías de malware para su posterior análisis y mitigación.
	C13	Analizar la gestión de identidades, cifrado, autenticación, confidencialidad, integridad y disponibilidad de la información.
	C14	Valorar los riesgos que suceda un determinado suceso mediante métodos estadísticos y probabilísticos.
Competencias (CO)	CO2	Usar diferentes herramientas de ingeniería y ciberseguridad para la resolución de problemas relacionados con los ciberataques.
	CO3	Llevar a cabo distintos procesos de análisis en las diferentes áreas de la ciberseguridad.
	CO5	Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.
	CO7	Implementar soluciones criptográficas.
	CO11	Gestionar evidencias de vulnerabilidades.
	CO12	Elaborar análisis forenses.
Habilidades y destrezas (H)	H1	Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
	H2	Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

Unidad 1: Introducción y fundamentos de Threat Intelligence

- 1.1. Definición y objetivos de la Inteligencia de Amenazas
- 1.2. Diferencias entre datos, información e inteligencia
- 1.3. Ciclo de vida de la inteligencia

- 1.4. Estándares y marcos de referencia
- 1.5. Rol de la TI en la defensa proactiva, detección y respuesta

Unidad 2. Fuentes de datos y recolección de inteligencia

- 2.1. Fuentes abiertas (OSINT) y cerradas
- 2.2. Inteligencia de red
- 2.3. Inteligencia en sistemas endpoint
- 2.4. Recolección de indicadores de compromiso (IoCs)
- 2.5. Herramientas de recolección y análisis

Unidad 3. Análisis y correlación

- 3.1. Técnicas de pivoting y enriquecimiento de indicadores
- 3.2. Correlación de IoCs con SIEMs y TIPs
- 3.3. Análisis de campañas y agrupación de incidentes
- 3.4. Uso de MITRE ATT&CK para mapear TTPs
- 3.5. Introducción al análisis de patrones y atribución de amenazas
- 3.6. Integración de feeds en SIEM/MISP y correlación

Unidad 4. Actores de amenazas y TTPs

- 4.1. Clasificación de adversarios
- 4.2. Modelos de motivación, capacidades y oportunidades
- 4.3. Casos de estudio
- 4.4. Técnicas de persistencia, evasión y comando y control (C2)

Unidad 5. Plataformas y herramientas de inteligencia

- 5.1. Threat Intelligence Platforms (TIPs)
- 5.2. Estandarización de intercambio de inteligencia
- 5.3. SIEMs y su integración con inteligencia

Unidad 6. Aplicación práctica de la inteligencia

- 6.1. Integración de TI en SOCs y CSIRTs
- 6.2. Uso en Threat Hunting
- 6.3. Detección temprana de amenazas específicas

Unidad 7. Producción de inteligencia y comunicación

- 7.1. Elaboración de informes según audiencia
- 7.2. Mejores prácticas en redacción y visualización
- 7.3. Casos de estudio de informes reales

Unidad 8. Tendencias y futuro de Threat Intelligence

- 8.1. Inteligencia colaborativa: ISACs y proyectos comunitarios
- 8.2. Automatización e IA aplicada a la inteligencia
- 8.3. Riesgos emergentes
- 8.4. Ética, legalidad y responsabilidad

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudios de caso.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	22,5	100
AF9: Clase en laboratorio	15	100
AF3: Realización de trabajos (individuales y/o grupales).	12,5	50
AF3: Tutorías (individuales y/o grupales).	5	50
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	89	0
AF6: Pruebas de evaluación.	6	100
Total	**150**	**--**

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	10	35
SE6: Evaluación de laboratorios	50	70

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).
- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)
Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio Ciberseguridad

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Wilhoit, K., & Opacki, J. (2022). Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs. Packt.
- Bergmann, I. (2023). OSINT and Threat Intelligence: Building a Robust Security Framework. Independently published.
- Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill.

Bibliografía Complementaria

- Conti, M., Dehghantanha, A., & Dargahi, T. (2018). Cyber Threat Intelligence: Challenges and Opportunities. ArXiv.
- Roccia, T. (2024). Visual Threat Intelligence. Security Break.
- Sindiramutty, S. R. (2023). Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence. ArXiv.

Otros Recursos de Aprendizaje Recomendados[3]

- GitHub – Awesome Threat Intelligence – Repositorio comunitario con herramientas, formatos (STIX/TAXII/VERIS), y bibliotecas
- 2024 Global Threat Intelligence Report (CyberProof) – visión actual de amenazas

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.