PLAN DOCENTE DE LA ASIGNATURA: **Evidencias Digitales y Análisis Forense**

CÓDIGO: **503237**

CURSO ACADÉMICO: **2024/2025**

PLAN DOCENTE DE LA ASIGNATURA[1]

Curso académico: 2024/2025

Identificación y características de la asignatura			
Código[2]	503237	Créditos ECTS	6
Denominación (español)	Evidencias Digitales y Análisis Forense		
Denominación (inglés)	Digital Evidence and Forensic Analysis		
Titulaciones[3]	Grado en Ingeniería Informática en Tecnologías de la Información		
Centro[4]	Centro Universitario de Mérida		
Semestre	8	Carácter	Optativa
Módulo	Contenidos Optativos en Tecnologías de la Información		
Materia	Ciberseguridad		
Profesor/es			
Nombre	Despacho	Correo-e	Página web
José Carlos Sancho Núñez	16	jcsanchon@unex.es	
Área de conocimiento	Lenguajes y Sistemas Informáticos		
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos		
Profesor coordinador[5] (si hay más de uno)			

Competencias[6]
Competencias básicas
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

[1] En los casos de planes conjuntos, coordinados, intercentros, pceos, etc., debe recogerse la información de todos los títulos y todos los centros en una única ficha.
[2] Si hay más de un código para la misma asignatura, ponerlos todos.
[3] Si la asignatura se imparte en más de una titulación, consignarlas todas, incluidos los PCEOs.
[4] Si la asignatura se imparte en más de un centro, incluirlos todos
[5] En el caso de asignaturas intercentro, debe rellenarse el nombre del responsable intercentro de cada asignatura
[6] Deben ajustarse a lo recogido en la memoria verificada del título.

Competencias generales
CG3. Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
CG9. Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.
Competencias específicas
CEO3. Realizar análisis de los datos almacenados que permitan detectar ataques a la seguridad de los sistemas informáticos y obtener evidencias sobre los mismos. Utilizar y/o desarrollar software que permita llevar a efectos los análisis de seguridad.
Competencias transversales
CT5. Toma de decisiones
CT20. Iniciativa y espíritu emprendedor
Contenidos[6]
Breve descripción del contenido
Analizar y detectar ciberataques. Vulnerabilidades, amenazas y riesgos de seguridad. Fundamentos y análisis de Exploits, Payloads, malware y códigos maliciosos. Control y recuperación del sistema. Informe forense. Requisitos legales y reglamentos. Estudio de casos de ataques de seguridad. Análisis forense del sistema software, la red y el móvil. Implementación de la seguridad mediante el uso y desarrollo de herramientas software.
Temario de la asignatura
Denominación del tema 1: Tipos de investigaciones basadas en ordenador Contenidos del tema 1: • Tipos de investigaciones basadas en ordenador • Diferencias de investigaciones basadas en ordenador • Investigaciones criminales • Investigaciones corporativas
Denominación del tema 2: El proceso de análisis forense Contenidos del tema 2: • Consideraciones previas a la investigación • Comprender la información del caso y los aspectos legales • Comprender la adquisición de datos • Comprender el proceso de análisis • Reportando los hallazgos
Denominación del tema 3: Redacción de informes Contenidos del tema 3: • Toma de notas efectiva • Escribir el informe
Denominación del tema 4: Proceso de investigación informática Contenidos del tema 4: • Análisis de línea de tiempo • Análisis de medios • Búsqueda de cadenas

- Recuperando datos borrados

Denominación del tema 5: Adquisición de evidencias
Contenidos del tema 5:

- Explorando las evidencias
- Comprender el entorno del examen forense
- Validación de herramientas
- Creación de medios estériles
- Definición de imágenes forenses

Descripción de las actividades prácticas del tema 5: cada estudiante debe elaborar un informe pericial detallado sobre la toma de 10 evidencias digitales básicas en una investigación simulada.

Denominación del tema 6: Sistemas informáticos
Contenidos del tema 6:

- Comprender el proceso de arranque
- Comprender los sistemas de archivos
- Comprender el sistema de archivos NTFS

Descripción de las actividades prácticas del tema 6: cada estudiante debe realizar una investigación sobre el análisis forense de discos siguiendo los procedimientos habituales de la informática forense sobre la preservación de evidencias digitales que debe finalizar en la elaboración de un informe.

Denominación del tema 7: Análisis forense del correo electrónico: técnicas de investigación
Contenidos del tema 7:

- Comprender los protocolos de correo electrónico
- Decodificación de correo electrónico
- Comprender el análisis de correo electrónico basado en el cliente
- Comprender el análisis de WebMail

Descripción de las actividades prácticas del tema 7: cada estudiante debe realizar una investigación sobre la extracción y trazabilidad de correos electrónicos y conversaciones de WhatsApp en una investigación simulada, cuyo resultado debe concluir en la realización de un informe.

Denominación del tema 8: Análisis de artefactos de Windows
Contenidos del tema 8:

- Comprender los perfiles de usuario
- Entendiendo el Registro de Windows
- Determinar el uso de la cuenta
- Determinación del conocimiento del archivo
- Identificación de ubicaciones físicas
- Explorando la ejecución del programa
- Comprender los dispositivos USB/conectados

Descripción de las actividades prácticas del tema 8: cada estudiante debe realizar una investigación personalizada sobre este tema cuyo resultado debe concluir en la realización de un informe, en la exposición oral de la metodología seguida y en la simulación de un juicio real.

Denominación del tema 9: Análisis forense de la memoria RAM
Contenidos del tema 9:

- Fundamentos de la memoria
- ¿Memoria de acceso aleatorio?
- Identificar las fuentes de la memoria.
- Captura de memoria RAM
- Explorando las herramientas de análisis de RAM

Descripción de las actividades prácticas del tema 9: cada estudiante debe realizar una investigación personalizada sobre este tema cuyo resultado debe concluir en la realización de un informe, en la exposición oral de la metodología seguida y en la simulación de un juicio real.

Denominación del tema 10: Artefactos de Internet
Contenidos del tema 10:

- Comprender los navegadores
- Medios de comunicación social
- Uso compartido de archivos punto a punto
- Computación en la nube

Denominación del tema 11: Ética de los testigos expertos
Contenidos del tema 11:

- Comprender los tipos de procedimientos
- Comenzando la fase de preparación
- Comprender el currículum vitae
- Entender el testimonio y la evidencia
- Comprender la importancia del comportamiento ético.

Actividades formativas

Horas de trabajo del estudiante por tema		**Horas Gran grupo**	**Actividades prácticas**				**Actividad de seguimiento**	**No presencial**
Tema	**Total**	**GG**	**CH**	**L**	**O**	**S**	**TP**	**EP**
0	1	1						
1	10	3			2			5
2	11	3			2			6
3	11	3			2			6
4	12	3			2		1	6
5	11	3			2			6
6	11	3			2			6
7	11	3			2			6
8	12	3			2		1	6
9	11	3			2			6
10	12	3			2			7
11	15	4,5			2,5		1	7
Evaluación[7]	22	2						20
TOTAL	150	37,5			22,5		3	87

[7] Indicar el número total de horas de evaluación de esta asignatura.

GG: Grupo Grande (85 estudiantes).
CH: Actividades de prácticas clínicas hospitalarias (7 estudiantes)
L: Actividades de laboratorio o prácticas de campo (15 estudiantes)
O: Actividades en sala de ordenadores o laboratorio de idiomas (20 estudiantes)
S: Actividades de seminario o de problemas en clase (40 estudiantes).
TP: Tutorías Programadas (seguimiento docente, tipo tutorías ECTS).
EP: Estudio personal, trabajos individuales o en grupo, y lectura de bibliografía.

Metodologías docentes[6]

1. Clases expositivas de teoría y problemas: Presentación de los contenidos de la asignatura y planificación de la participación de todos los estudiantes en las distintas tareas. Discusión de aspectos teóricos. Adicionalmente se realizarán charlas divulgativas realizadas por expertos y/o empresas de la materia.
2. Enseñanza participativa: Trabajos prácticos en grupos medianos o pequeños.
3. Tutorización: Actividad de seguimiento para tutela de trabajos dirigidos, consultas de dudas y asesoría en grupos pequeños o individuales.
4. Aprendizaje autónomo mediante el análisis de documentos escritos, la elaboración de memorias, el estudio de la materia impartida y desarrollo de los supuestos prácticos planteados.
5. Aprendizaje virtual. Uso de herramientas virtuales de comunicación entre profesor y estudiante e incluso entre los estudiantes entre sí.

Resultados de aprendizaje[6]

- Saber analizar los sistemas para detectar amenazas y vulnerabilidades de seguridad.
- Saber realizar un informe de análisis forense.
- Implementar y desarrollar software que permita mantener los sistemas seguros.
- Demostrar seguridad e iniciativa para tomar decisiones responsables y acertadas en situaciones comprometidas.
- Emprender proyectos ambiciosos (complejos y desafiantes), que implican una decisión social.

Sistemas de evaluación[6]

Evaluación continua

La evaluación se basará en los siguientes criterios:

- **Resolución de trabajos dirigidos (70%). (Recuperable)**
  Se realizará trabajos dirigidos relacionados con el análisis informático forense, individualmente o en pareja, que será evaluado por el profesor.
- **Exposición oral de trabajos realizados (10%). (Recuperable)**
  Se realizará la exposición oral de trabajo relacionados con el análisis informático forense, individualmente o en pareja, que será evaluado por el profesor.
- **Examen final (20%). (Recuperable)**
  La evaluación final se realizará un examen escrito en la fecha propuesta.

Sistema de evaluación	Ponderación
Examen	20
Exposición oral de trabajos realizados	10
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	70
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	0

Evaluación global
La evaluación se basará en los siguientes criterios: • **Resolución de trabajos dirigidos (70%).** Se realizará trabajos dirigidos relacionados con el análisis informático forense, individualmente o en pareja, que será evaluado por el profesor. • **Exposición oral de trabajos realizados (10%).** Se realizará la exposición oral de trabajo relacionados con el análisis informático forense, individualmente o en pareja, que será evaluado por el profesor. • **Examen final (20%).** La evaluación final se realizará un examen escrito en la fecha propuesta por la subdirección académica del Centro Universitario de Mérida.
Bibliografía (básica y complementaria)
• W. Oettinger. *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing (2020) • G. Johansen. *Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats*. Packt Publishing (2020)
Otros recursos y materiales docentes complementarios
• R. Tamma, O. Skulkin, H. Mahalik, S. Bommisetty. *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices* (4ª edición). Packt Publishing (2020) • S. V. N. Parasram. *Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux 2019.x*. Packt Publishing (2020) • E. Ozkaya. *Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents.* Packt Publishing (2021) • N. Jaswal. *Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools*. Packt Publishing (2019)