ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001004 - Evidencias Forenses

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2024/25 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos.....1
2. Profesorado.....1
3. Competencias y resultados de aprendizaje.....2
4. Descripción de la asignatura y temario.....3
5. Cronograma.....5
6. Actividades y criterios de evaluación.....6
7. Recursos didácticos.....8

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001004 - Evidencias Forenses
No de créditos	3 ECTS
Carácter	Optativa
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario en Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2024-25

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Juan Manuel Castelo Gomez (Coordinador/a)		juanmanuel.castelo@upm.es	- -
Julio Cesar Hernandez Castro		jc.hernandez.castro@upm.es	Sin horario.
Alejandro Barreiro Morante		alejandro.bmorante@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB07 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB08 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB09 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CE08 - Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa

CG05 - Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia

CT05 - Gestión de la información

CT09 - Capacidad de análisis y síntesis

CT10 - Resolución de problemas

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

3.2. Resultados del aprendizaje

RA31 - Identificar las fases de un análisis forense informático y los requisitos de cada una de ellas.

RA30 - Conocer los fundamentos del análisis forense informático y las evidencias digitales.

RA33 - onocer y aplicar las técnicas forenses informáticas en los principales entornos digitales (escritorio, móvil, cloud e IoT) con el objetivo de extraer conclusiones a partir del análisis de evidencias digitales.

RA34 - Determinar qué herramientas son necesarias para la adquisición y análisis de fuentes digitales dependiendo del entorno a analizar, así como qué información se puede extraer de ellas.

RA35 - Conocer la estructura y contenido de los informes forenses y adquirir la capacidad para el desarrollo de los mismos.

RA32 - Adquirir la habilidad para discernir las necesidades forenses de los principales entornos digitales y sus particularidades.

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

En esta asignatura se realizará una introducción a la informática forense. Se explicará el concepto de evidencia digital y su importancia dentro del proceso del análisis forense informático, del que se describirán las fases que lo componen. Además, se explicarán las técnicas comunes que se utilizan para la adquisición y análisis de fuentes de evidencias, así como las relativas a la extracción de la información que pueden contener. Por último, se introducirán los distintos contextos digitales en los que se suelen realizar investigaciones forenses y las particularidades de cada uno de ellos.

4.2. Temario de la asignatura

1. Introducción al Análisis Forense Informático

    1.1. Conceptos Básicos de Análisis Forense Informático

    1.2. Evidencias Digitales

    1.3. Tipos de Análisis Forense Informático.

    1.4. La Cadena de Custodia.

    1.5. Elaboración de Informes Forenses

2. Técnicas Comunes de Análisis Forense Informático

    2.1. El Laboratorio Forense

    2.2. Adquisición de Fuentes de Evidencia

    2.3. Análisis de Fuentes de Evidencia

    2.4. Técnicas Comunes de Extracción de Información (Hashing, Filtrado de Datos, Creación de Líneas Temporales, Análisis de Metadatos, Recuperación de Archivos, Estegoanálisis, Análisis de Documentos...)

    2.5. Herramientas Comunes para la Realización de Análisis Forense Informáticos

3. Análisis Forense en Entornos Digitales

    3.1. Análisis Forense en Entornos Windows

    3.2. Análisis Forense en Entornos Linux

    3.3. Análisis Forense en Entornos Móviles

    3.4. Análisis Forense en Entornos Cloud

    3.5. Análisis Forense en Entornos IoT

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad tipo 1	Actividad tipo 2	Tele-enseñanza	Actividades de evaluación
1		**Tema 1 - Introducción al Análisis Forense Informático** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 1. RA7, R29** TG: Técnica del tipo Trabajo en Grupo Evaluación Progresiva No presencial Duración: 12:00
2		**Tema 2. Técnicas Comunes de Análisis Forense Informático** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 2. RA7** TG: Técnica del tipo Trabajo en Grupo Evaluación Progresiva No presencial Duración: 12:00
3		**Tema 3. Análisis Forense en Entornos Digitales** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 3. RA7** TG: Técnica del tipo Trabajo en Grupo Evaluación Progresiva No presencial Duración: 12:00 **Práctica Final. RA7** TG: Técnica del tipo Trabajo en Grupo Evaluación Progresiva No presencial Duración: 12:00
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Práctica 1. RA7, R29	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	15%	0 / 10	CT05 CE08 CB08 CB07 CG05
2	Práctica 2. RA7	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	35%	0 / 10	CT10 CT09 CT05 CT12 CB09 CE08 CB08 CB07
3	Práctica 3. RA7	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	25%	0 / 10	CT10 CT09 CT05 CT12 CB09 CE08 CB08 CB07
3	Práctica Final. RA7	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	25%	0 / 10	CT10 CT09 CT05 CT12 CB09 CE08 CB08 CB07

6.1.2. Prueba evaluación global

No se ha definido la evaluacion sólo por prueba final.

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Práctica 1. RA7, R29	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	15%	0 / 10	CB08 CB07 CG05 CT05 CE08
Práctica 2. RA7	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	35%	0 / 10	CT10 CT09 CT05 CT12 CB09 CE08 CB08 CB07
Práctica 3. RA7	TI: Técnica del tipo Trabajo Individual	Presencial	12:00	25%	0 / 10	CT10 CT09 CT05 CT12 CB09 CE08 CB08 CB07
Práctica Final. RA7	PI: Técnica del tipo Presentación Individual	Presencial	12:00	25%	/ 10	CT05 CT12 CB09 CT10 CT09 CE08 CB08 CB07

6.2. Criterios de evaluación

La evaluación progresiva se compondrá de 4 prácticas a realizar en grupo con una distribución de pesos de 15%, 35%, 25% y 25%.

Del mismo modo, la evaluación extraordinaria estará formada por el mismo número de prácticas con un reparto de pesos idéntico, pero estas serán individuales. Las prácticas que hayan sido superadas en la evaluación progresiva no será necesario recuperarlas de cara a la evaluación extraordinaria.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Digital Archeaeology - The Art and Science of Digital Forensics. Addison-Wesley (1ª Edición)	Bibliografía	
Computer Forensics and Cyber Crime - An Introduction. Prentice-Hall (3ª Edición)	Bibliografía	
Guide to Computer Forensics and Investigations. Course Technology (4ª Edición)	Bibliografía	
Computer Forensics - Evidence Collection & Preservation. Course Technology (1ª Edición)	Bibliografía	