ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001004 - Evidencias forenses

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo semestre

Índice

Guía de Aprendizaje

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 en el que se imparte	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Eduardo Garcia Pardo (Coordinador/a)	4305 (C.Sur)	eduardo.pardo@upm.es	Sin horario. Horario de tutorías publicado en los tablones de la universidad y página web para el segundo cuatrimestre

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

con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Ciberseguridad: contexto y amenazas

- Auditoría técnica de seguridad

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Master Universitario en Ciberseguridad no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

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

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

CT01 - Uso de la Lengua Inglesa

CT09 - Capacidad de análisis y síntesis

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

4.2. Resultados del aprendizaje

RA29 - Conocer los procedimientos y técnicas de análisis forense más comunes

RA7 - Comprender y utilizar en casos simples las técnicas de la informática forense así como utilizar las herramientas más comunes

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

En esta asignatura se realizará una introducción a la informática forense, se describirá el concepto de evidencia, tanto desde el punto de vista técnico como legal y se repasará la búsqueda y extracción de pruebas. En concreto, el enfoque de la asignatura estudiará la informática forense desde diferentes perspectivas, comprendiendo sistemas de ficheros, sistemas operativos y sistemas empotrados. Por último se revisarán las herramientas de análisis forense más comunes.

Temario:

Tema 1 - Introducción a la informática forense

- Motivación

- Historia y evolución

- ¿Qué es el análisis forense?

- Conceptos iniciales

Tema 2 - Procedimientos forenses

- Introducción al procedimiento forense

- Fases de un análisis forense

- Características de un procedimiento forense

- Metodologías y guías

- Acciones a evitar

Tema 3 - Discos duros y sistemas de ficheros

- Estructura física

- Estructura lógica

- Sistemas de ficheros

- Copias de discos duros

Tema 4 - Forensía en sistemas

- Sistemas operativos

- Dispositivos móviles

- Dispositivos empotrados

Tema 5 - Esteganografía

- Introducción a la esteganografía

- Historia y evolución

- Procedimientos esteganográficos

- Herramientas

Tema 6 - Herramientas para la investigación forense

- Toolkits y discos live

- Herramientas por temáticas

- Software libre vs Software privativo

5.2. Temario de la asignatura

1. Introducción a la informática forense
   1.1. Motivación
   1.2. Historia y evolución
   1.3. ¿Qué es el análisis forense?
   1.4. Conceptos iniciales
2. Procedimientos forenses
   2.1. Introducción al procedimiento forense
   2.2. Fases de un análisis forense
   2.3. Características de un procedimiento forense
   2.4. Metodologías y guías
   2.5. Acciones a evitar
3. Discos duros y sistemas de ficheros
   3.1. Estructura física
   3.2. Estructura lógica
   3.3. Sistemas de ficheros
   3.4. Copias de discos duros
4. Forensía en otros sistemas
   4.1. Sistemas operativos
   4.2. Dispositivos móviles
   4.3. Sistemas empotrados
5. Esteganografía

5.1. Introducción a la esteganografía

5.2. Historia y evolución

5.3. Procedimientos esteganográficos

5.4. Herramientas

6. Herramientas para la investigación forense

6.1. Toolkits y discos live

6.2. Herramientas por temáticas

6.3. Software libre vs Software privativo

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1		**Tema 1 - Introducción a la informática forense. Tema 2 - Procedimientos forenses** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Test 1. RA29** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:00 **Práctica 1. RA7** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 17:00
2		**Tema 3 - Discos duros y sistemas de ficheros. Tema 4 - Forensía en sistemas operativos** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Test 2. RA29** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:00 **Práctica 2. RA7** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 17:00
3		**Tema 5 - Esteganografía Tema 6 - Herramientas para la investigación forense** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Test 3. RA29** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:00 **Trabajo. RA7** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 17:00 **Asistencia. RA7, RA29** OT: Otras técnicas evaluativas Evaluación continua Duración: 00:00
4				
5				
6				
7				
8				
9				
10				
11				
12				

13				
14				
15				
16				**Test. RA29** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 01:00 **Práctica 1. RA7** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Duración: 17:00 **Práctica 2. RA7** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Duración: 17:00 **Trabajo. RA7** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Duración: 17:00
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

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.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Test 1. RA29	EX: Técnica del tipo Examen Escrito	Presencial	01:00	10%	/ 10	CT12 CB10 CG02
1	Práctica 1. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB08 CT01 CE08
2	Test 2. RA29	EX: Técnica del tipo Examen Escrito	Presencial	01:00	10%	/ 10	CG02 CT12 CB10
2	Práctica 2. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB08 CT01 CE08
3	Test 3. RA29	EX: Técnica del tipo Examen Escrito	Presencial	01:00	10%	/ 10	CG02 CT12 CB10
3	Trabajo. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB09 CB08 CT01 CT09 CT12 CB10
3	Asistencia. RA7, RA29	OT: Otras técnicas evaluativas	Presencial	00:00	10%	/ 10	

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas

16	Test. RA29	EX: Técnica del tipo Examen Escrito	Presencial	01:00	40%	/ 10	CG02 CT12 CB10
16	Práctica 1. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB08 CT01 CE08
16	Práctica 2. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB08 CT01 CE08
16	Trabajo. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	17:00	20%	3 / 10	CB09 CB08 CT01 CT09 CT12 CB10

7.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

7.2. Criterios de evaluación

La calificación final de la asignatura se obtendrá calculando la media ponderada de las calificaciones de las distintas actividades evaluables, expuestas en el apartado anterior, tomando en consideración los pesos de cada actividad. Para que un alumno pueda obtener su nota promediada es obligatorio obtener, al menos, un 30% de la nota en cada una de las dos prácticas obligatorias y en el trabajo, con independencia de la modalidad que siga (evaluación continua o solo prueba final). Adicionalmente, en la modalidad de evaluación continua será necesario asistir y participar activamente en al menos el 70% de las clases para que la actividad de asistencia sea considerada como apta. Si el alumno no alcanza el mínimo en alguna de las actividades evaluables, o bien el promedio obtenido es inferior a 5, la asignatura se dará por suspensa, debiendo acudir a la convocatoria extraordinaria.

En la convocatoria extraordinaria las actividades de evaluación, así como la ponderación de las mismas será igual a las detalladas en evaluación solo prueba final.

8. Recursos didácticos

8.1. 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	