ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001004 - Evidencias Forenses

PLAN DE ESTUDIOS

09AW - Master Universitario en Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2020/21 - 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 responsable de la titulación	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2020-21

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Borja Bordel Sanchez (Coordinador/a)	4305	borja.bordel@upm.es	Sin horario. Actualizadas en la página web de la ETSISI

* 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

CT01 - Uso de la Lengua Inglesa

CT05 - Gestión de la información

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

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

RA29 - Conocer los procedimientos y técnicas de análisis forense 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 - El proceso de investigación forense

- Introducción

- Objetivos de la informática forense

- Características y tipos de evidencias

- Actores relevantes en la toma de evidencias

- Análisis forense digital: fases

- Ideas relevantes

Tema 2 - Evidencias digitales, los first responders

- Request for Comments: 3227

- Forensic Examination of Digital Evidence: A Guide for Law Enforcement

- Electronic Crime Scene Investigation: A Guide for First Responders

- UNE 71506

Tema 3 - El laboratorio de informática forense

- Procedimientos forenses básicos

- Laboratorio forense en Sistemas Windows: herramientas

- Laboratorio forense en Sistemas MAC OS: herramientas

- Laboratorio forense en Android: herramientas

- Laboratorio forense en Sistemas iOS: herramientas

- Laboratorio forense para sistema empotrados: herramientas

Tema 4 - Introducción a la Esteganografía práctica

- Introducción

- Principios de funcionamiento

- Esteganografía práctica

- Estegoanálisis

Tema 5 - Obtención de Logs y Correlación de eventos

- Introducción

- Obtención de logs

- Correlación de eventos y analizadores lógicos

- Forensic Toolkits

- Reconocimiento heurístico y detección de anomalías

5.2. Temario de la asignatura

1. El proceso de investigación forense
    1.1. Introducción
    1.2. Objetivos de la informática forense
    1.3. Características y tipos de evidencias
    1.4. Actores relevantes en la toma de evidencias
    1.5. Análisis forense digital: fases
    1.6. Ideas relevantes
2. Evidencias digitales, los first responders
    2.1. Request for Comments: 3227
    2.2. Forensic Examination of Digital Evidence: A Guide for Law Enforcement
    2.3. Electronic Crime Scene Investigation: A Guide for First Responders
    2.4. UNE 71506
3. El laboratorio de informática forense
    3.1. Procedimientos forenses básicos
    3.2. Laboratorio forense en Sistemas Windows: herramientas
    3.3. Laboratorio forense en Sistemas MAC OS: herramientas
    3.4. Laboratorio forense en Android: herramientas
    3.5. Laboratorio forense en Sistemas iOS: herramientas ? Laboratorio forense para sistema empotrados: herramientas

4. Introducción a la Esteganografía práctica

   4.1. Introducción

   4.2. Principios de funcionamiento

   4.3. Esteganografía práctica

   4.4. Estegoanálisis

5. Obtención de Logs y Correlación de eventos

   5.1. Introducción

   5.2. Obtención de logs

   5.3. Correlación de eventos y analizadores lógicos

   5.4. Forensic Toolkits

   5.5. Reconocimiento heurístico y detección de anomalías

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1		**Tema 1 - El proceso de investigación forense. Tema 2 - Evidencias digitales, los first responders** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Participación en debates, presentaciones, trabajo personal. R29** PI: Técnica del tipo Presentación Individual Evaluación continua Presencial Duración: 10:00
2		**Tema 3 - El laboratorio de informática forense** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 1. RA7, R29** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 18:00
3		**Tema 4 - Introducción a la Esteganografía práctica Tema 5 - Obtención de Logs y Correlación de eventos** Duración: 09:00 PL: Actividad del tipo Prácticas de Laboratorio		**Práctica 2. RA7** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 12:00 **Práctica 3. RA7** TG: Técnica del tipo Trabajo en Grupo Evaluación continua No presencial Duración: 12:00 **Asistencia. RA7, RA29** OT: Otras técnicas evaluativas Evaluación continua Presencial Duración: 00:00
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

16				**Práctica 1. RA7, R29** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final No presencial Duración: 18:00 **Práctica 2. RA7** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final No presencial Duración: 12:00 **Práctica 3. RA7** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final No presencial Duración: 12:00
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.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

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	Participación en debates, presentaciones, trabajo personal. R29	PI: Técnica del tipo Presentación Individual	Presencial	10:00	30%	0 / 10	CT01 CT09 CB09 CB10
2	Práctica 1. RA7, R29	TG: Técnica del tipo Trabajo en Grupo	No Presencial	18:00	20%	0 / 10	CT05 CE08 CB08 CT01
3	Práctica 2. RA7	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	20%	0 / 10	CB08 CT01 CT05 CE08
3	Práctica 3. RA7	TG: Técnica del tipo Trabajo en Grupo	No Presencial	12:00	20%	0 / 10	CB09 CB08 CT01 CT09 CT12 CB10
3	Asistencia. RA7, RA29	OT: Otras técnicas evaluativas	Presencial	00:00	10%	0 / 10	CT12

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
16	Práctica 1. RA7, R29	TI: Técnica del tipo Trabajo Individual	No Presencial	18:00	40%	0 / 10	CB08 CT01 CT05 CE08
16	Práctica 2. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	12:00	30%	0 / 10	CB08 CT01 CT05 CE08

16	Práctica 3. RA7	TI: Técnica del tipo Trabajo Individual	No Presencial	12:00	30%	0 / 10	CB09 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. No se imponen restricciones adicionales.

En la convocatoria extraordinaria las actividades de evaluación y la obtención de la calificación final, sigue el mismo esquema.

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	

9. Otra información

9.1. Otra información sobre la asignatura

En previsión de posibles recidivas de la epidemia de COVID, la presente guía contempla la impartición de la asignatura en formato bimodal: todas las actividades formativas planificadas inicialmente como actividades presenciales, en caso de ser necesario pasarán a desarrollarse a través de plataformas online.