ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

595310251 - Analisis Forense Digital Sistemas Informacion

PLAN DE ESTUDIOS

59ET - Doble Grado En Ing.Electronica De Comunicaciones Y En Ing.Telematica

CURSO ACADÉMICO Y SEMESTRE

2019/20 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	595310251 - Analisis Forense Digital Sistemas Informacion
No de créditos	4.5 ECTS
Carácter	Optativa
Curso	Cuarto curso
Semestre	Octavo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	59ET - Doble Grado En Ing.electronica De Comunicaciones Y En Ing.telematica
Centro responsable de la titulación	59 - Escuela Tecnica Superior de Ingenieria y Sistemas de Telecomunicacion
Curso académico	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Carlos Carrillo Sanchez (Coordinador/a)	A4401	carlos.carrillo@upm.es	Sin horario. Se determinará al principio del semestre

* 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

- Seguridad En Redes Y Servicios

- Sistemas Operativos

- Programacion Ii

- Redes De Ordenadores

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Doble Grado en Ing.electronica de Comunicaciones y en Ing.telematica no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE B2 - Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.

CE SC06 - Capacidad para analizar, codificar, procesar y transmitir información multimedia empleando técnicas de procesado analógico y digital de señal.

CE SO01 - Capacidad de construir, explotar y gestionar servicios y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, tratamiento analógico y digital, codificación, transporte, representación, procesado, almacenamiento, reproducción, gestión y presentación de servicios audiovisuales e información multimedia.

CE TEL01 - Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.

CG 02 - Capacidad de búsqueda y selección de información, de razonamiento crítico y de elaboración y defensa de argumentos dentro del área.

CG 03 - Capacidad para expresarse correctamente de forma oral y escrita y transmitir información mediante documentos y exposiciones en público.

CG 10 - Capacidad para manejar especificaciones, reglamentos y normativas y la aplicación de las mismas en el desarrollo de la profesión.

4.2. Resultados del aprendizaje

RA704 - RA1157 - Conocer los procedimientos y técnicas de análisis forense más comunes

RA699 - RA1160 - Análisis de metadatos existentes en Sistemas de información

RA700 - RA1158 - Utilizar técnias de análisis forense en casos simples mediante herramientas de uso general

RA701 - RA1161 - Análisis de tráfico de datos en Sistemas de Información

RA703 - RA1162 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

RA702 - RA1159 - Conociimiento de la normativa legal y jurídica aplicable a la extracción de información en análisis forense

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Al ser una asignatura optativa, se introdudirá al alumno en el análisis forense digital en sistemas de Información. A partír del concepto de evidencia digital, dentro del entorno jurídico nacional y europeo, se establecerán las directrices de extracción de evidencias digitales según normas ISO. Al tener una fuerte componente práctica, se realizarán sesiones de laboratorio para capturar y analizar evidencia existentes en diferentes soportes de información, como son discos duros, dispositivos USB, etc., análisis de tráfico entre ordenadores, así como análisis de la información existente en los ficheros contenedores de datos, que se corresponden con los metadatos de imagenes, documentos de cualquier tipo, o incluso cabeceras de correos electrónicos. Por todo esto, se complementará estos conocimientos con aquellos conceptos esenciales de sistemas operativos, de redes de comunicaciones, etc., que permitan la perfecta compresión de los conceptos relacionados con analisis forense digital en sistemas de la informaciónn ejecución. Por último, se utilizarán algunas de las herramientas de análisis forense más comunes.

5.2. Temario de la asignatura

1. Introducción al análisis forense digital
   1.1. Introducción a la ciencia forense
   1.2. Responsabilidades de un perito forense digital
   1.3. Introducción al Derecho informático
2. Metodología del análisis forense digital
   2.1. Estrategias básicas de análisis forense. La cadena de custodia
   2.2. Adquisición de evidencias digitales
   2.3. Presentación e informe. Normas ISO
3. El laboratorio de informática forense digital
   3.1. Evidencias digitales en entornos MS-Windows.
   3.2. Evidencias digitales en entornos Linux
   3.3. Análisis de Logs y Metadatos de información
   3.4. Datos en redes de comunicación
   3.5. Análisis de Cabeceras IMAP, POP, HTTP; HTTPS.
4. Herramientas de Análisis Forense en Sistemas de Información
   4.1. Clonación de pruebas digitales
   4.2. Adquisición de evidencias en:
      4.2.1. Sistemas de ficheros. Extracción de evidencias
      4.2.2. Memoria. Procesos en ejecución
      4.2.3. Protocolos de comunicación en redes de ordenadores
      4.2.4. Metadatos de ficheros, imágenes y audio
      4.2.5. Internet y correo electrónico
      4.2.6. Análisis en dispositivos móviles
      4.2.7. Análisis de ciberataque
5. Otros ámbitos forenses
   5.1. Gestión documental
   5.2. Drones

5.3. Bus CAN

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** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
2	**Tema 2** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
3	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Temas 1 y 2** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:00
4	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
5	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
6	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
7				**Evaluación Tema 3** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 03:00
8	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
9				
10	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
11	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
12	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		

13	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		
14				**Evaluación Tema 4** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 03:00
15	**Tema 5** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
16				
17				**Evaluación final** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Duración: 03:00

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
3	Evaluación Temas 1 y 2	EX: Técnica del tipo Examen Escrito	Presencial	01:00	20%	2 / 10	CG 10 CE TEL01 CG 02 CG 03
7	Evaluación Tema 3	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	40%	3 / 10	CG 10 CE SC06 CE SO01 CE TEL01 CE B2 CG 02 CG 03
14	Evaluación Tema 4	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	40%	3 / 10	CG 02 CG 03 CG 10 CE SC06 CE SO01 CE TEL01 CE B2

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Evaluación final	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	100%	5 / 10	CG 03 CG 10 CE SC06 CE SO01 CE TEL01 CE B2 CG 02

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Evaluación extraordinaria	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	100%	5 / 10	CG 02 CG 03 CG 10 CE SC06 CE SO01 CE TEL01 CE B2

7.2. Criterios de evaluación

El alumno podrá elegir entre dos itinerarios de evaluación según la normativa de la UPM en esta materia, como son:

- De evaluación continua.
- De sólo prueba final.

Itinerario de evaluación continua.

Es el itinerario por defecto. El alumno deberá trabajar de forma continuada durante todo el cuatrimestre, asistiendo y participando en las clases teóricas y de laboratorio. El objetivo fundamental de la evaluación continua es que los alumnos estudien y comprendan los principales conceptos de la asignatura de forma gradual. Por ello, se considera que es de especial importancia la asistencia a clase y el trabajo sistemático que incluye la realización de todas las actividades relaciondas con los contenidos estudiados en las clases teóricas.

En el itinerario de evaluación continua se realizarán tres pruebas de evaluación comunes a todos los alumnos: Estas pruebas se realizarán en las semanas indicadas en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Todas las pruebas se realizarán en el aula asignada a esta asignaturam ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

Itinerario de evaluación solo prueba final.

El alumno deberá realizar una práctica final que será el compendio de todas y cada una de las prácticas realizadas por los alumnos que realicen una evaluación continua. **Además se realizará una examen-práctica más que se realizará el día programado**. Por lo tanto, será objeto de examen todo los conceptos impartidos en las diferentes actividades que se realicen, incluido aquellas presentaciones realizadas por profesionales expertos en el ámbito del análisis forense digital en sistemas de información

Esta prueba se realizará en la semana indicada en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Está prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

tinerario de evaluación convocatoria extraordinarial.

El alumno deberá realizar una práctica final que será el compendio de todas y cada una de las prácticas realizadas por los alumnos que realicen una evaluación continua. Además se realizará una examen-práctica más que se realizará el día programado. Por lo tanto, será objeto de examen todo los conceptos impartidos en las diferentes actividades que se realicen, incluido aquellas presentaciones realizadas por profesionales expertos en el ámbito del análisis forense digital en sistemas de información .

Esta prueba se realizará en la semana indicada en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Está prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Guía de toma de evidencias en entornos Windows?. Asier Martinez Retanaga. INCIBE. 2014	Bibliografía	
Análisis Forense Digital en Entornos Windows. Juan Garrido Caballero, 0xWord	Bibliografía	
Técnicas de Análisis Forense informático para Peritos Judiciales profesionales?. Pilar Vila Avendaño, 0xWord	Bibliografía	
Hacking Windows: Ataques a sistemas y redes Microsoft. Carlos García, Valentín Martín y Pablo González. 0xWord	Bibliografía	
Windows Forensics Cookbook. Oleg Skulkin. Packt 2017	Bibliografía	
Análisis de tráfico con Wireshark. Borja Merino Febrero. INTECO-CERT	Bibliografía	
Documentación aportada por diferentes ponentes en las charlas presenciales	Otros	
Páginas Web de las principales compañías relacionadas con la forensía digital (búsqueda de manuales, tutoriales, descarga de aplicaciones a utilizar, etc.)	Recursos web	