



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería y Sistemas
de Telecomunicación

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

2021/22 - Primer 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.....	4
5. Cronograma.....	6
6. Actividades y criterios de evaluación.....	9
7. Recursos didácticos.....	12
8. Otra información.....	13

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	Séptimo semestre
Período de impartición	Septiembre-Enero
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	2021-22

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 especificará en el directorio personal existente en la Web de la Escuela

David Jesus Meltzer Camino	A4403	david.meltzer@upm.es	Sin horario. Se especificará en el directorio personal existente en la Web de la Escuela
----------------------------	-------	----------------------	---

* 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

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 04 - Capacidad de abstracción, de análisis y de síntesis y de resolución de problemas.

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

CG 13 - Habilidades de aprendizaje con un alto grado de autonomía.

CG 14 - Actitudes de ética y responsabilidad profesional, respeto a los Derechos Humanos y a la diversidad cultural.

3.2. Resultados del aprendizaje

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

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

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

RA761 - Comprender y utilizar en casos simples las técnicas de la informática forense así como utilizar las herramientas más comunes

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

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

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

RA1 - RA232 - Se concretarán para cada asignatura optativa o para la realización de prácticas en empresas

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

Al ser una asignatura optativa, se introducirá al alumno en el análisis forense digital en sistemas de Información. A partir 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 imágenes, 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 comprensión de los conceptos relacionados con análisis forense digital en sistemas de la informaciónn ejecución. Por último, se utilizarán algunas de las herramientas de análisis forense más comunes.

Toda la planificación de la asignatura está pensada para ser impartida de manera bimodal. Es decir, puede ser 100% presencial como, si así lo determinan las autoridades universitarias y sanitarias, pasar a ser impartida 100% en modalidad teleenseñanza

4.2. 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 Sistemas de información
 - 3.2. Clonación de pruebas digitales

- 3.3. Análisis de Cabeceras IMAP, POP, HTTP; HTTPS.
- 3.4. Adquisición de evidencias en Sistemas de información. Correo electrónico
- 3.5. Adquisición de evidencias en redes de comunicación
- 3.6. Análisis de Logs y Adquisición de evidencias en Metadatos de información
- 3.7. Adquisición de evidencias en sistemas de ficheros
- 3.8. Adquisición de evidencias en memoria
- 3.9. Herramientas de Análisis Forense en Sistemas de Información
 - 3.9.1. Autopsy
- 4. Otras herramientas de Análisis Forense en Sistemas de Información
 - 4.1. Kali linux
 - 4.2. OS forensics
 - 4.3. Caine

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1	Tema 1 Duración: 03:00 LM: Actividad del tipo Lección Magistral		Tema 1 Duración: 03:00 LM: Actividad del tipo Lección Magistral	
2	Tema 2 Duración: 03:00 LM: Actividad del tipo Lección Magistral		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: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio	
4				Evaluación Temas 1 y 2 EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 03:00
5	Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		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		Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio	
7	Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio		Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio	

8	<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>	
9	<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>	
10	<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>	
11	<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>	
12	<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>		<p>Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral</p> <p>Tema 3 Duración: 02:30 PL: Actividad del tipo Prácticas de Laboratorio</p>	
13				<p>Evaluación Tema 3 EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 03:00</p>
14	<p>Tema 4 Duración: 03:00 LM: Actividad del tipo Lección Magistral</p>		<p>Tema 4 Duración: 03:00 LM: Actividad del tipo Lección Magistral</p>	
15				
16				
17				<p>Evaluación final EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Presencial Duración: 03:00</p>

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.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Evaluación Temas 1 y 2	EX: Técnica del tipo Examen Escrito	Presencial	03:00	20%	/ 10	CG 13 CE TEL01 CG 02 CG 03 CG 10 CG 14 CG 04
13	Evaluación Tema 3	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	80%	0 / 10	CE SC06 CE SO01 CE TEL01 CG 02 CG 03 CG 10 CG 14 CG 04 CG 13 CE B2

6.1.2. 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	CE B2 CE SC06 CE SO01 CE TEL01 CG 02 CG 03 CG 10 CG 14 CG 13 CG 04

6.1.3. 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 13 CE B2 CE SC06 CE SO01 CE TEL01 CG 02 CG 03 CG 10 CG 14 CG 04

6.2. 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 relacionadas con los contenidos estudiados en las clases teóricas.

En el itinerario de evaluación continua se realizarán dos 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 también reflejada en dicho cronograma. Todas las pruebas se realizarán en el aula asignada a esta asignatura 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 también reflejada en dicho cronograma. Esta prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

Itinerario de evaluación convocatoria extraordinaria.

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 también reflejada en dicho cronograma. Esta prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

7. Recursos didácticos

7.1. 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, OxWord	Bibliografía	
Técnicas de Análisis Forense informático para Peritos Judiciales profesionales?. Pilar Vila Avendaño, OxWord	Bibliografía	
Hacking Windows: Ataques a sistemas y redes Microsoft. Carlos García, Valentín Martín y Pablo González. OxWord	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	

Máquinas virtuales	Equipamiento	
--------------------	--------------	--

8. Otra información

8.1. Otra información sobre la asignatura

La situación sanitaria causada por la pandemia COVID-19 obliga a restringir el aforo de las aulas y por ello se ha decidido que el modelo de docencia de este semestre sea híbrido o mixto. Se establecerán turnos de presencialidad dentro de los grupos, de forma que cada semana un turno asistirá a clase en el aula (columna "actividad en el aula" del cronograma), mientras el resto de los turnos se conectarán a la clase de forma telemática (columna "tele-enseñanza"). Y cada semana será un turno diferente el que acuda al aula. Si cambian las condiciones sanitarias y se pudieran impartir clases presenciales con normalidad, todos los estudiantes acudirán a las aulas a recibir las clases indicadas en la columna "actividad en el aula". Si, por el contrario, empeoraran las condiciones sanitarias, todos los alumnos pasarían a conectarse a las clases en remoto de la columna "tele-enseñanza".