Proyecto/Guía docente de la asignatura

Asignatura	INFORMÁTICA FORENSE		
Materia	TECNOLOGÍAS DE LA INFORMACIÓN		
Módulo	TECNOLOGÍAS ESPECÍFICAS		
Titulación	GRADO EN INGENIERÍA INFORMÁTICA		
Plan	545	**Código**	46958
Periodo de impartición	1º CUATRIMESTRE	**Tipo/Carácter**	Optativa-5 (Mención IS) Optativa-4 (Mención TI)
Nivel/Ciclo	GRADO	**Curso**	4º
Créditos ECTS	6 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	JOAQUÍN ADIEGO RODRÍGUEZ JAIME DIEZ ZURRO		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 5646 E-MAIL: jadiego@infor.uva.es		
Departamento	INFORMÁTICA (ATC, CCIA, LSI)		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La asignatura “Informática Forense” es una asignatura de carácter optativo que está programada en el primer semestre del 4º curso de la titulación de Grado en Ingeniería Informática en las menciones de Ingeniería de Software y Tecnologías de la Información.

La ubicuidad de medios informáticos, combinada con el crecimiento imparable de Internet y las redes durante los últimos años, abre un escenario de oportunidades para actos ilícitos (fraude, espionaje empresarial, sabotaje, robo de datos, intrusiones no autorizadas en redes y sistemas y un largo etcétera) a los que es preciso hacer frente entendiendo las mismas tecnologías de las que se sirven los delincuentes informáticos, con el objeto de salirles al encuentro en el mismo campo de batalla. Parte vital en el combate contra el delito es una investigación de medios digitales basada en métodos profesionales y buenas prácticas al efecto de que los elementos de evidencia obtenidos mediante la misma puedan ser puestos a disposición de los tribunales. Se debe hacer con las suficientes garantías en lo referente tanto al mantenimiento de la cadena de custodia y al cumplimiento de aspectos esenciales para el orden legal del estado de derecho, como al respeto a las leyes sobre privacidad y protección de datos y otras normativas de relevancia similar.

La Informática Forense es la disciplina que se encarga de la adquisición, el análisis y la valoración de elementos de evidencia digital hallados en ordenadores, soportes de datos e infraestructuras de red, y que pudieran aportar luz en el esclarecimiento de actividades ilegales perpetradas en relación con instalaciones de proceso de datos, independientemente de que dichas instalaciones sean el objetivo de la actividad delictiva o medios utilizados para cometerla.

1.2 Relación con otras materias

Fundamentos de Sistemas Operativos.
Estructura de Sistemas Operativos.
Garantía y Seguridad de la Información.

1.3 Prerrequisitos

Sistemas Operativos.
Seguridad.
Estructuras de Datos.

2. Competencias

2.1 Generales

Código	Descripción
C01	Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas a continuación en esta sección de la memoria, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.
G02	Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática de acuerdo con los conocimientos adquiridos según lo establecido en las competencias de formación especificadas a continuación en esta sección de la memoria.
G03	Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
G08	Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

2.2 Específicas

Código	Descripción
TI2	Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
TI7	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

2.3 Transversales

Código	Descripción
CT1	Capacidad de análisis y síntesis.
CT2	Capacidad de organizar y planificar.
CT3	Comunicación oral y escrita en la lengua propia.
CT4	Capacidad para la lectura de textos técnicos en inglés.
CT7	Toma de decisiones
CT9	Trabajo en equipo.
CT11	Responsabilidad y compromiso ético.
CT12	Liderazgo.
CT13	Capacidad de aplicar los conocimientos en la práctica.
CT14	Capacidad de aprender.
CT15	Capacidad de adaptarse a nuevas situaciones.

3. Objetivos

	Descripción
1	Ser capaz de analizar un sistema cuando ha ocurrido un acceso no autorizado, un robo de información o un mal uso de los recursos en general.
2	Conocer los aspectos legales que deben considerarse durante el análisis forense.
3	Conocer y saber utilizar las técnicas y herramientas más útiles para la realización del análisis forense.
4	Conocer las acciones legales que a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc.

4. Contenidos y/o bloques temáticos

Bloque 1: Metodología de la investigación forense en informática

Carga de trabajo en créditos ECTS: 2,4

a. Contextualización y justificación

La informática forense sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información; para ello se deberán investigar los sistemas informáticos con el fin de detectar evidencias de la vulneración de los sistemas. Cuando una empresa contrata servicios de informática forense puede perseguir objetivos preventivos, anticipándose al posible problema, u objetivos correctivos como solución una vez que la vulneración y las infracciones ya se han producido. Todo el procedimiento debe hacerse tenido en cuenta los requisitos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados, con el fin que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio. En este bloque se estudiará la problemática de la informática forense, así como sus bases legales, los distintos tipos de delitos informáticos ("cibercrimen") que se pueden cometer y las actuaciones que se pueden llevar a cabo.

b. Objetivos de aprendizaje

TI7.1	Conocer los aspectos legales que deben considerarse durante el análisis forense.
TI7.2	Conocer las acciones legales a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc.

c. Contenidos

TEMA 1: Introducción a la informática forense

TEMA 2: Análisis de dispositivos físicos

TEMA 3: Investigación en soportes de datos

d. Métodos docentes

- Véase el punto 5 de esta guía.

e. Plan de trabajo

En este primer bloque temático se estudiará la necesidad e importancia de las técnicas de informática forense, viendo cuál es su campo de aplicación y diferentes aspectos. También se comentarán los diferentes tipos de cibercrimen con el que un analista forense se puede encontrar, su marco legal y los requisitos que se deben cumplir a la hora de realizar un peritaje informático para que éste sea válido judicialmente. En la parte práctica

de este bloque, el estudiante deberá presentar un trabajo que será, generalmente, de carácter teórico/bibliográfico.

f. Evaluación

Véase el punto 7 de esta guía.

g. Bibliografía básica

- E. Casey, *Handbook of Digital Forensics and Investigation*. Academic Press. ISBN: 978-0123742674
- Francisco Lázaro Domínguez, *Introducción a la Informática Forense*. RA-MA. ISBN: 978-84-9964-209-3
- B. Nelson, *Guide to Computer Forensics and Investigations*. Cengage Learning. ISBN: 978-1435498839

.

h. Bibliografía complementaria

- Rafael López Rivera, *Peritaje Informático y Tecnológico*. ISBN: 978-8461608959
- John Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. Syngress. ISBN: 978-1597496612

i. Recursos necesarios

Campus Virtual de la UVa (https://campusvirtual.uva.es)

j. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
2,4 ECTS	Semanas 1 a 6

Bloque 2: Tecnología forense

Carga de trabajo en créditos ECTS: 3,6

a. Contextualización y justificación

Las distintas metodologías forenses incluyen la recogida segura de datos de diferentes medios y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas. En este bloque se estudiarán algunas de las tecnologías forenses que se utilizan para recabar información y obtener pruebas de delito dependiendo del entorno en el que se está trabajando.

b. Objetivos de aprendizaje

TI2.1	Ser capaz de analizar un sistema cuando ha ocurrido un acceso no autorizado, un robo de información o un mal uso de los recursos en general.
TI2.2	Conocer y saber utilizar las técnicas y herramientas más útiles para la realización del análisis forense.

c. Contenidos

TEMA 4: Análisis post-mortem

TEMA 5: Investigación de imágenes digitales

TEMA 6: Introducción a la esteganografía digital

TEMA 7: Investigación de dispositivos móviles

d. Métodos docentes

- Véase el punto 5 de esta guía.

e. Plan de trabajo

En el segundo bloque teórico se estudiarán las herramientas (principalmente de libre distribución) y técnicas que permiten llevar a cabo un análisis forense dependiendo del entorno que se desea investigar. En la parte práctica de este bloque, el estudiante deberá presentar un trabajo que podrá ser de carácter práctico y/o teórico/bibliográfico.

f. Evaluación

Véase el punto 7 de esta guía.

g. Bibliografía básica

- C. Altheide y H. Carvey, *Digital Forensics with Open Source Tools*. Syngress. ISBN: 978-1597495868
- H. Carvey, *Windows Forensic Analysis Toolkit*. Syngress. ISBN: 978-1597497275
- E. Casey, *Handbook of Digital Forensics and Investigation*. Academic Press. ISBN: 978-0123742674
- B. Nelson, *Guide to Computer Forensics and Investigations*. Cengage Learning. ISBN: 978-1435498839

h. Bibliografía complementaria

- J. Fichera y S. Bolt. *Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response*. Syngress. ISBN: 978-1597499620
- John Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. Syngress. ISBN: 978-1597496612

i. Recursos necesarios

Campus Virtual de la UVa (https://campusvirtual.uva.es)

j. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
3,6 ECTS	Semanas 7 a 15

5. Métodos docentes y principios metodológicos

Actividad	Metodología
Clase de teoría	• Cada clase de teoría está diseñada como una actividad completa y autocontenida compuesta de diversas actividades dirigidas a facilitar la adquisición de conocimientos, habilidades y competencias. • La asignatura combina la exposición de temas y realización de ejercicios por parte del profesor, con la realización de ejercicios individuales o en grupo por parte de los estudiantes. Podrá haber sesiones específicas donde los estudiantes expondrán sus soluciones propuestas. Estas sesiones serán anunciadas previamente por el profesor. • Docencia presencial: la teoría básica necesaria será expuesta en clase por el profesor de la asignatura, con ayuda de la pizarra y/o algún método de proyección, utilizando ejemplos variados tanto para introducir conceptos como para asimilar los ya introducidos. • Docencia online: parte de los contenidos se desarrollarán de manera semipresencial, haciendo uso de los recursos online y de las herramientas que se proporcionan en el Campus Virtual de la UVa. • Se suministrará al estudiante una colección de documentos o enlaces a los mismos que contienen, ocasionalmente en forma ampliada, la documentación básica relacionada con el problema a resolver en la clase. Se desarrollarán ejemplos ilustrativos de la metodología de solución de pequeños problemas relacionados con el problema principal a resolver. El estudiante debe utilizar la documentación extra para realizar las tareas encargadas. • Será importante que el estudiante intente resolver los ejercicios propuestos en la documentación entregada al comienzo del curso, y así se le hará saber. • Asimismo, si fuera el caso, los estudiantes conocerán con antelación los ejercicios que serán resueltos en cada clase práctica y el profesor solicitará su colaboración para responder diferentes cuestiones sobre los problemas.
Clase práctica	• Durante la semana previa a la sesión o sesiones de prácticas de laboratorio el estudiante estudiará de manera personal o en grupo la documentación relativa a las tareas correspondientes a las sesiones de laboratorio. Las horas presenciales de laboratorio incluirán para su desarrollo clase magistral participativa y la realización de un proyecto guiado por el profesor, que encargará y guiará el trabajo que se realizará de manera o individual o en grupos (de hasta 5 estudiantes), siguiendo un enfoque colaborativo. • Se elaborará material que estará disponible en el Campus Virtual de la UVa para que los estudiantes puedan preparar las clases prácticas. • El aprendizaje basado en problemas (PBL) o el aprendizaje basado en proyectos (PjBL) son unas estrategias de enseñanza-aprendizaje que potencia tanto la adquisición de conocimientos como el desarrollo de competencias, actitudes y valores. Tanto en PBL como en PjBL, un grupo pequeño de estudiantes se reúne, con la facilitación del profesor, con la finalidad de analizar y resolver un problema diseñado especialmente para el logro de ciertos objetivos de aprendizaje. Durante el proceso de interacción de los alumnos para entender y resolver el problema se logra, además del

	aprendizaje del conocimiento propio de la materia, que puedan elaborar un diagnóstico de sus propias necesidades de aprendizaje, que comprendan la importancia de trabajar colaborativamente, que desarrollen habilidades de análisis y síntesis de información, además de comprometerse con su proceso de aprendizaje. • Las reuniones con los estudiantes se podrán celebrar bien en el aula, bien a través de un sistema de videoconferencia, apoyándose en ambos casos en las herramientas presentes en la Campus Virtual de la UVa.
Seminarios	• Durante el curso se podrán celebrar varios seminarios, con el objeto de afianzar y completar algunos aspectos muy relacionados con la misma y para facilitar el desarrollo de algunas competencias genéricas. Estos seminarios tendrán un carácter teórico y práctico. • Los estudiantes podrán ser distribuidos en un grupo de trabajo (el número de integrantes puede variar según circunstancias), cada uno de los cuales junto con el profesor llevará a cabo los seminarios previstos. • En estos seminarios el profesor orientará la actividad de los estudiantes en relación con la asignatura, exponiendo estos sus problemas con el aprendizaje de la materia. El profesor, previamente a cada seminario, propondrá a cada grupo de trabajo la resolución de varias cuestiones o problemas que deberán ser entregadas en el mismo y sobre los que los estudiantes tendrán que debatir. • Cada estudiante entregará en cada seminario una hoja al empezar con su propuesta de solución, y otra al terminar con la nueva solución que propone y los comentarios que recojan de forma esquemática su aprendizaje en el seminario. El objetivo de esta actividad es que el estudiante reconozca su propio aprendizaje y detecte posibles errores en el mismo, así como que el profesor esté informado de la marcha del curso, lo cual puede facilitar una reorientación de actividades o la recomendación de actuaciones particulares para mejorar el aprendizaje individual. En la calificación final se tendrá en cuenta la participación en los seminarios, y las soluciones propuestas.
Tutoría	• Las tutorías individualizadas podrán ser atendidas en las seis horas oficiales que se podrán consultar en la web de la Universidad de Valladolid a principio de curso o a cualquier otra hora, previa cita con el profesor. Como alternativa, se propondrá el uso de alguna plataforma de e-learning o sistema de videoconferencia para la resolución de dudas y creación de debates relacionados con los temas que se están estudiando.
Actividades no presenciales	• Los estudiantes deben realizar una serie de actividades fuera del aula, aprendiendo a gestionar su tiempo y organizar su trabajo. Incluyen tanto encargos específicos como actividades generales: ○ Preparación de sesiones. Los estudiantes reciben el encargo de leer bibliografía y preparar dudas previamente a una sesión. Para ello se les suministrarán referencias, enlaces a documentos y/o material extra. ○ Repaso de conceptos y ejercicios de consolidación. El estudiante debe dedicar al menos dos horas por cada sesión para repasar y afianzar los conceptos presentados. Puede utilizar ejercicios y problemas extras suministrados por el profesor para comprobar su progreso. ○ Laboratorio personal. El profesor pondrá a disposición de los estudiantes el material necesario para que en su casa o en el laboratorio de la facultad puedan realizar programas o actividades similares a los que se realizan en las sesiones presenciales. El entorno, metodología y herramientas serán los mismos que se utilizan en clase. De esta forma, el estudiante podrá comprobar si la experiencia adquirida en las clases se traduce en un aumento correspondiente de su destreza en la materia.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	30	Estudio y trabajo autónomo individual	65
Laboratorios (L)	24	Estudio y trabajo autónomo grupal	25
Seminarios (S)	6		
Total presencial	**60**	**Total no presencial**	**90**

7. Sistema y características de la evaluación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Entrega práctica 1	40%	Aproximadamente semana 5
Entrega práctica 2		Aproximadamente semana 10
Entrega práctica 3		Aproximadamente semana 15
Examen final escrito	60%	Periodo de exámenes

CRITERIOS DE CALIFICACIÓN
Se usará el mismo criterio de calificación en las dos convocatorias de la asignatura. El examen escrito incluirá apartados dedicados a los conocimientos teóricos y también la resolución de problemas en los que se apliquen dichos conocimientos teóricos. La calificación obtenida por la realización de los ejercicios prácticos durante el periodo lectivo de la asignatura se conserva durante todo el curso académico, no siendo posible recuperar estos apartados prácticos fuera del periodo lectivo natural de la asignatura. Para la convocatoria extraordinaria de la asignatura, los estudiantes que no hayan superado la parte práctica podrán recuperarla entregando la resolución de un nuevo guion de prácticas.

8. Consideraciones finales

Cronograma de actividades previstas

Nota: La información mostrada en el siguiente cronograma es provisional y puede sufrir cambios. Consulte periódicamente la página web de la asignatura para acceder a información actualizada.

Semana	Contenido		Horas	
			Teoría	Lab. / Sem.
1	Bloque 1	Tema 1: Introducción a la informática forense	2	2
2		Tema 2: Análisis de dispositivos físicos	2	2
3			2	2
4			2	2
5		Tema 3: Investigación en soportes de datos	2	2
6			2	2
7	Bloque 2	Tema 4: Análisis post-mortem	2	2
8			2	2
9			2	2
10		Tema 5: Investigación de imágenes digitales	2	2
11			2	2
12		Tema 6: Introducción a la esteganografía digital	2	2
13			2	2
14		Tema 7: Investigación de dispositivos móviles	2	2
15			2	2