la

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		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 5646 E-MAIL: jadiego@infor.uva.es		
Horario de tutorías	Véase www.uva.es → Centros → Campus de Valladolid → Escuela Técnica Superior de Ingeniería Informática → Tutorías		
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
G03	Capacidad de análisis y síntesis
G04	Capacidad de organizar y planificar
G05	Comunicación oral y escrita en la lengua propia
G06	Conocimiento de una segunda lengua (preferentemente inglés)
G08	Habilidades de gestión de la información
G09	Resolución de problemas
G10	Toma de decisiones
G11	Capacidad crítica y autocrítica
G12	Trabajo en equipo
G14	Responsabilidad y compromiso ético
G15	Liderazgo
G16	Capacidad de aplicar los conocimientos en la práctica
G17	Habilidades de investigación
G18	Capacidad de aprender
G19	Capacidad de adaptarse a nuevas situaciones
G20	Capacidad de generar nuevas ideas
G21	Habilidad para trabajar de forma autónoma

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.

3. Objetivos

Código	Descripción
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.
TI7.1	Conocer los aspectos legales que deben considerarse durante el análisis forense.
TI2.2	Conocer y saber utilizar las técnicas y herramientas más útiles para la realización del análisis forense.
TI7.2	Conocer las acciones legales que a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc.

4. 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
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	25
Laboratorios (L)	24		
Prácticas externas, clínicas o de campo			
Seminarios (S)	6		
Tutorías grupales (TG)			
Evaluación (fuera del periodo oficial de exámenes)			
Total presencial	**60**	**Total no presencial**	**90**

5. 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 que a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc.

c. Contenidos

TEMA 1: Introducción: el análisis forense

TEMA 2: La investigación forense en informática

TEMA 3: La investigación de intrusiones en sistemas

d. Métodos docentes

- Véase ***Anexo: Métodos Docentes***

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 alumno 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

http://www.infor.uva.es/~jadiego

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 digitales 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: Obtención de datos

TEMA 5: Análisis forense en Windows

TEMA 6: Análisis forense en Unix/Linux y Macintosh

TEMA 7: Otros tipos de análisis forense

d. Métodos docentes

- Véase ***Anexo: Métodos Docentes***

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 alumno 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

http://www.infor.uva.es/~jadiego

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Metodología de la investigación forense en informática	2,4 ECTS	Semanas 1 a 6
Bloque 2: Tecnología forense	3,6 ECTS	Semanas 7 a 15

7. Sistema de calificaciones – Tabla resumen

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

8. Anexo: Métodos docentes

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 alumnos. Podrá haber sesiones específicas donde los alumnos expondrán sus soluciones propuestas. Estas sesiones serán anunciadas previamente por el profesor. • 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. • Se suministrará al alumno 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 alumno debe utilizar la documentación extra para realizar las tareas encargadas. • Será importante que el alumno intente resolver los ejercicios propuestos en la documentación entregada al comienzo del curso, y así se le hará saber. • Asimismo, 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 alumno 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 (2/3 alumnos), siguiendo un enfoque colaborativo.

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 alumnos 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 alumnos 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 alumnos tendrán que debatir. • Cada alumno 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 alumno 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 para la resolución de dudas y creación de debates relacionados con los temas que se están estudiando.
Actividades no presenciales	• Los alumnos 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: o Preparación de sesiones. Los alumnos 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. o Repaso de conceptos y ejercicios de consolidación. El alumno 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. o Laboratorio personal. El profesor pondrá a disposición de los alumnos el material necesario para que en su casa (si disponen de ordenador) o en el laboratorio de la facultad puedan realizar programas 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 alumno podrá comprobar si la experiencia adquirida en las clases se traduce en un aumento correspondiente de su destreza en la materia.

9. Anexo: 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: el análisis forense	2	2
2	Bloque 1	Tema 2: La investigación forense en informática	2	2
3	Bloque 1	Tema 2: La investigación forense en informática	2	2
4	Bloque 1	Tema 2: La investigación forense en informática	2	2
5	Bloque 1	Tema 3: La investigación de intrusiones en sistemas	2	2
6	Bloque 1	Tema 3: La investigación de intrusiones en sistemas	2	2
7	Bloque 2	Tema 4: Obtención de datos	2	2
8	Bloque 2	Tema 4: Obtención de datos	2	2
9	Bloque 2	Tema 4: Obtención de datos	2	2
10	Bloque 2	Tema 5: Análisis forense en Windows	2	2
11	Bloque 2	Tema 5: Análisis forense en Windows	2	2
12	Bloque 2	Tema 6: Análisis forense en Unix/Linux y Macintosh	2	2
13	Bloque 2	Tema 6: Análisis forense en Unix/Linux y Macintosh	2	2
14	Bloque 2	Tema 7: Otros tipos de análisis forense	2	2
15	Bloque 2	Tema 7: Otros tipos de análisis forense	2	2