



Universidad
de Alcalá

GUÍA DOCENTE

Pericia Informática

**Grado en Criminalística: Ciencias y
Tecnologías Forenses**

Universidad de Alcalá

Curso Académico 2022/23
3º Curso – 2º Cuatrimestre

Aprobada en Junta de Facultad 30/05/2022

DESCRIPCIÓN DE LA MATERIA

Asignatura:	Pericia Informática
Titulación en la que se imparte:	Grado en Criminalística: Ciencias y Tecnologías Forenses
Departamento y Área de Conocimiento:	Automática. Área de Ingeniería Telemática.
Carácter:	Obligatorio
Créditos ECTS:	6
Curso y cuatrimestre:	Tercer Curso, Segundo Cuatrimestre
Profesorado	Susel Fernández Melián (Coordinadora) José Luis Narbona Moreno Antonio García Herráiz
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

Los ataques informáticos aprovechan vulnerabilidades en los sistemas y aplicaciones, para llegar a comprometer a los usuarios finales o a los sistemas completos. Cada vez se descubren nuevas vulnerabilidades y los atacantes son conscientes de que a las organizaciones les lleva tiempo establecer una protección adecuada, lo que ha hecho que los incidentes de seguridad hayan experimentado un notable incremento en los últimos años. Esto se traduce en la necesidad de desarrollar y mantener una capacidad forense digital como parte de un marco de gestión de riesgos global. Se requiere el estudio de técnicas que posibiliten realizar una identificación, preservación, análisis y presentación de datos una vez producido el ataque, que a su vez permita evaluar las consecuencias, el autor, las causas, la metodología empleada y establecer un plan de recuperación y continuidad del negocio tras el incidente.

La asignatura “Pericia Informática” se centra en el análisis del escenario una vez producido un ciberataque. Se valoran casos concretos, conceptos legales y se estudian metodologías y herramientas para la adquisición de videncias y cadena de custodia, así como para la gestión y respuesta ante incidentes, especialmente en Windows.

2. COMPETENCIAS

Competencias Generales (CG)

Esta asignatura contribuye a reforzar las siguientes competencias generales y básicas:

CG1	Capacidad crítica y autocrítica, cuestionando las situaciones y los medios de investigación.
CG2	Habilidad para trabajar de manera autónoma, organizada y planificando la búsqueda de información, análisis y síntesis de la misma, diseño, gestión del tiempo y ejecución de una tarea de forma personal o autónoma.
CG3	Habilidad para trabajar en equipo, integrarse y comunicarse con expertos de otras áreas y en distintos contextos.
CG4	El estudiante será capaz de gestionar la información, consultando bases de datos y publicaciones relevantes y especializadas provenientes de fuentes diversas.
CB2	Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
CB4	Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
CB5	Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Esta materia contribuye a reforzar las siguientes transversales:

CT1	Habilidad para conocer y utilizar los mecanismos básicos de uso de comunicación bidireccional entre profesores y estudiantes, foros, chats, etcétera.
CT2	Capacidad para valorar situaciones, tomar decisiones y diseñar la planificación de tareas de investigación o aplicadas a emprender.

Competencias específicas (CE)

Esta materia contribuye a reforzar las siguientes competencias específicas:

CE5	Capacidad para evaluar un escenario forense y planificar un peritaje desde un enfoque técnico-científico multidisciplinar y reconocer e indicar el perfil profesional de quien debe realizar una determinada peritación en el seno de un equipo de trabajo multidisciplinar.
CE20	Capacidad para utilizar las técnicas y tecnologías de la informática para la recuperación de información digital y el seguimiento de actividades en entornos digitales, así como la utilización de herramientas informáticas para el análisis y la investigación de la seguridad informática/telemática y la ciber-delincuencia.

Resultados del aprendizaje

Al término de la materia, el alumno habrá alcanzado los siguientes resultados de aprendizaje:

RA1	Conocer y aplicar los conceptos básicos y metodologías para la realización del análisis forense informático
RA2	Conocer los aspectos fundamentales de la actividad del perito informático
RA3	Conocer la cadena de custodia y los pasos a seguir para documentar una escena y preservar la evidencia
RA4	Conocer técnicas y herramientas de análisis forense para hacer investigación post-ataque en Windows.
RA5	Conocer los principales delitos informáticos y los aspectos legales que afectan el análisis forense digital

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)
Fundamentos del análisis forense informático: Introducción, conceptos técnicos y legales del análisis forense. Objetivos y guías para realizar el análisis forense. Actividad del perito.
Adquisición y análisis de evidencias: Documentación de la escena, pasos a seguir para preservar la evidencia, cadena de custodia, clonado, hashing, reporte final.
Análisis forense en Windows: Sistemas de ficheros, hibernación, registros, eventos, navegación, papelera de reciclaje, metadatos. Herramientas software aplicadas al análisis forense en Windows.
Incidentes de seguridad: Gestión y respuesta ante Incidentes. Visión general de los principales delitos informáticos.

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases en grupo grande: 28 horas Clases en grupo reducido: 28 horas Evaluación final: 2 horas Total: 58 horas presenciales
Número de horas del trabajo propio del estudiante:	Preparación de las clases, aprendizaje autónomo, preparación de ejercicios, pruebas y prácticas, preparación de la prueba final: Total: 92 horas
Total horas	150 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Presenciales	<ul style="list-style-type: none"> Exposiciones en clase, de carácter teórico práctico. Resolución de problemas. Sesiones prácticas de laboratorio: orientadas a consolidar los conceptos presentados previamente, así como a familiarizar al estudiante con las herramientas y metodologías de apoyo al estudio de la materia y futuro desempeño profesional. Presentaciones orales y otras actividades. Actividades de trabajo en grupo.
Tutorías individuales, grupales y vía web (foro, correo, etc.)	<ul style="list-style-type: none"> Resolución de dudas. Apoyo al aprendizaje autónomo.
Trabajo autónomo	<ul style="list-style-type: none"> Lectura crítica de recursos docentes.

- Resolución de ejercicios, prácticas o casos, de manera individual o colaborativa
- Elaboración de trabajos e informes

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación

Procedimientos

El alumno dispone de dos convocatorias para superar la asignatura: una ordinaria y otra extraordinaria.

- **Convocatoria Ordinaria:** En la convocatoria ordinaria el alumno será evaluado mediante el proceso de Evaluación Continua. En situaciones excepcionales, debidamente justificadas, podrá acogerse a un sistema de evaluación mediante Examen Final. Para ello debe solicitarlo por escrito al Director del centro, en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de Evaluación Continua. En este caso, el Director del centro comunicará la resolución en un máximo de 15 días. Si el alumno no recibe respuesta en ese plazo de tiempo, se considera estimada la solicitud.
- **Convocatoria extraordinaria:** La convocatoria extraordinaria consistirá en una evaluación similar al proceso de evaluación final de la convocatoria ordinaria.

Criterios de evaluación

Atendiendo a las competencias descritas en el apartado 2, la evaluación del alumno se basará en el grado de adquisición de las mismas que demuestre, de acuerdo a los siguientes criterios de evaluación:

CE1	El alumno demuestra conocer y aplicar los conceptos básicos y metodologías para la realización del análisis forense informático.
CE2	El alumno demuestra conocer los aspectos fundamentales de la actividad del perito informático.
CE3	El alumno demuestra conocer la cadena de custodia y los pasos a seguir para documentar una escena y preservar la evidencia.
CE4	El alumno demuestra conocer y aplicar técnicas y herramientas de análisis forense para hacer investigación post-ataque en Windows.
CE5	El alumno demuestra conocer los principales delitos informáticos y los aspectos legales que afectan el análisis forense digital.

Instrumentos de calificación

Esta sección describe los instrumentos de evaluación que serán aplicados a cada uno de los criterios de evaluación definidos previamente.

1. Pruebas de Evaluación Intermedia (PEI): Realización de cuestiones teóricas de desarrollo y/o tipo test y la realización de uno o más ejercicios.
2. Seminarios (S): Realización de tareas de trabajo personal de investigación cuyo resultado será la entrega de documentos escritos y la presentación oral de los mismos.
3. Pruebas de Laboratorio: Realización de pequeñas pruebas teórico/prácticas y el seguimiento, por parte del profesor, del trabajo realizado en las sesiones de Grupo Pequeño (PL).
4. Prueba de Evaluación Final (PEF): Realización de una prueba escrita que integre todos los conocimientos de la asignatura. Los alumnos con derecho al sistema de evaluación mediante Examen Final realizarán una prueba con la misma estructura que los de evaluación continua.

Criterios de Calificación

Esta sección cuantifica los criterios de calificación para la superación de las competencias de asignatura.

Convocatoria Ordinaria, Evaluación Continua

Los alumnos realizarán una prueba PEF y se mantendrán las notas de las pruebas de tipo S, PL, PEI con los pesos indicados en la tabla. Se permite mejorar la calificación final si en la PEF se obtiene un resultado mejor al logrado en el acumulado de todas las pruebas de tipo S, PL, PEI y PEF, y se ha alcanzado, al menos, el 50% de la calificación máxima posible en las pruebas de tipo S y PL.

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1-RA3	CE1-CE3	PEI1	30%
RA1-RA5	CE1-CE5	PEF	40%
RA1-RA5	CE1-CE5	S	10%
RA1-RA5	CE1-CE5	PL	20%

Convocatoria Ordinaria, Evaluación final

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1- RA5	CE1-CE5	PEF	100%

Convocatoria Extraordinaria, Evaluación Continua

En la convocatoria extraordinaria/evaluación continua los alumnos realizarán una prueba PEF y se mantendrán las notas de las pruebas de tipo S, PL, PEI con los pesos indicados en la tabla. Se permite mejorar la calificación final si en la PEF se obtiene un resultado mejor al logrado en el acumulado de todas las pruebas de tipo S, PL, PEI y PEF, y se ha alcanzado, al menos, el 50% de la calificación máxima posible en las pruebas de tipo S y PL. La relación entre los criterios, instrumentos y calificación es la siguiente:

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1-RA3	CE1-CE3	PEI1	30%
RA1-RA5	CE1-CE5	PEF	40%
RA1-RA5	CE1-CE5	S	10%
RA1-RA5	CE1-CE5	PL	20%

Convocatoria Extraordinaria, Evaluación final

Resultados de aprendizaje	de	Criterios de evaluación	Instrumentos de evaluación	de	Peso en la calificación
RA1- RA5		CE1-CE5	PEF		100%

6. BIBLIOGRAFÍA

Libros recomendados.

- The Basics of Digital Forensics. John Sammons. Syngress. 2012. ISBN: 9781597496629.
- System Forensics, Investigation, and Response, 3rd Edition. Easttom. Jones & Bartlett Learning. August 2017.
- Digital Archaeology: The Art and Science of Digital Forensics. Michael W. Graves. Addison-Wesley Professional. 2013. SBN: 9780132853774.
- Practical Windows Forensics. Konstantin Saponov, Ayman Shaaban. Publisher: Packt Publishing Release Date: June 2016. ISBN: 9781783554096.
- Técnicas de Análisis Forense informático para peritos Judiciales profesionales. Pilar Vila Avendaño. ISBN: 978-84-697-7700-8.