Universidad de Alcalá

GUÍA DOCENTE

Evidencias Digitales en la Prevención del Delito.

Grado en Criminalística: Ciencias y Tecnologías Forenses

Universidad de Alcalá

Curso Académico 2022/23

4º Curso – 2º Cuatrimestre

Aprobada en Junta de Facultad 30/05/2022

DESCRIPCIÓN DE LA MATERIA

Asignatura:	**Evidencias Digitales en la Prevención del Delito**
Código	**652044**
Titulación en la que se imparte:	**Grado en Criminalística: Ciencias y Tecnologías Forenses**
Departamento y Área de Conocimiento:	**Ciencias de la Computación.** **Área de Ciencia de la Computación e Inteligencia Artificial** **Área de Lenguajes y Sistemas Informáticos.**
Carácter:	**Optativa**
Créditos ECTS:	**6**
Curso y cuatrimestre:	**Cuarto Curso, Segundo Cuatrimestre**
Profesorado	**Manuel Sánchez Rubio** **José Javier Martínez Herráiz (Coordinador)**
Horario de Tutoría:	**Por determinar**
Idioma en el que se imparte:	**Español**

Aprobada en Junta de Facultad 30/05/2022

1. PRESENTACIÓN

En esta asignatura se estudian las técnicas y herramientas para llevar a cabo investigaciones policiales en el ámbito de las redes sociales, mensajerías de todo tipo y la internet profunda.

Los principios básicos, tecnologías y técnicas sobre el funcionamiento y análisis de datos en aplicaciones enfocadas a la comunicación e intercambio de información (mensajería instantánea, correo electrónico, compartición de archivos p2p, redes de intercambio de archivos): reconocimiento, búsqueda, autenticación e identificación de evidencias.

Existen una serie de características que definen a la ciberdelincuencia y que la distinguen de la que podemos calificar como delincuencia tradicional y es aquí donde se centran las líneas principales de la asignatura.

Entre esas particularidades, se pueden encontrar las siguientes:

- Son delitos de fácil comisión. De forma genérica y dejando de lado los delitos puramente tecnológicos que necesitan una mayor elaboración, la preparación y ejecución de la mayoría de los ciberdelitos no conlleva apenas dificultad.
- Con relativa frecuencia estos tipos delictivos tienen un elemento internacional, al situarse geográficamente el autor y su/s víctima/s en distintos países.
- Una misma acción delictiva puede causar un número muy elevado de víctimas , sin que tengan una relación directa ni entre ellas ni con el autor. Como ejemplo podemos citar la Botnet Mariposa, compuesta por más de 12 millones de ordenadores comprometidos.
- Los resultados del delito pueden manifestarse bien de manera instantánea, como es el caso de las estafas o distribución de contenidos ilícitos, a pesar de la distancia geográfica existente, o bien mucho tiempo después (por ejemplo con la distribución de malware).
- En algunos casos, el hecho del delito pasa completamente desapercibido para la víctima, que no es consciente de haberlo sido.
- Existe una importante cifra negra de delitos, tanto por no ser las víctimas conscientes de serlo o porque, siéndolo, prefieren no presentar denuncia.
- Los indicios de la comisión de un delito informático suelen hallarse en servidores informáticos, donde no se almacenan por períodos prolongados de tiempo.
- Además, son fácilmente modificables y/o destruibles. Estas características hacen complicada la investigación policial y judicial.

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 las diferentes etapas en la cadena de custodia de las evidencias digitales.
RA2	Conocer y utilizar herramientas para el análisis de archivos en diferentes entornos.
RA3	Conocer y utilizar técnicas y herramientas para la obtención de datos en correo, mensajería instantánea, redes P2P e internet profunda.
RA4	Conocer y aplicar las técnicas de obtención de datos en la prevención de delitos.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)
Evidencias periciales: Etapas, cadena de custodia de las evidencias digitales y delitos de falsedad en la pericia.
Análisis de evidencias: Esquemas de análisis, archivos en distintos sistemas operativos
Obtención de datos: mail, mensajería instantánea, Deep web, intercambio de archivos P2P.
Prevención de captura de datos ilícitos: redes sociales, phising, keyloggers, troyanos

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	• 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.)	• Resolución de dudas. • Apoyo al aprendizaje autónomo.
Trabajo autónomo	• Lectura crítica de recursos docentes. • Resolución de ejercicios, prácticas o casos, de manera individual o colaborativa • Elaboración de trabajos e informes

Si las autoridades sanitarias consideraran necesaria la suspensión de la actividad docente presencial o las circunstancias de la asignatura lo requieren, la docencia, o parte de la misma, continuaría con la metodología online hasta que se levantara la suspensión, momento en el que se volvería a la modalidad presencia

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 las diferentes etapas en la cadena de custodia de las evidencias digitales.
CE2	El alumno demuestra conocer y utilizar herramientas para el análisis de archivos en diferentes entornos.
CE3	El alumno demuestra conocer y utilizar técnicas y herramientas para la obtención de datos en correo, mensajería instantánea, redes P2P e internet profunda.
CE4	El alumno demuestra conocer y saber aplicar las técnicas de obtención de datos en la prevención de delitos.

Instrumentos de calificación

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

1. 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.
2. Pruebas de Laboratorio (PL): Realización de pequeñas pruebas teórico/prácticas y el seguimiento, por parte del profesor, del trabajo realizado en las sesiones de Grupo Pequeño.
3. Prueba de Evaluación Final (PEF): Realización de un trabajo que integre todos los conocimientos de la asignatura. La evaluación se realizará a través de un informe escrito y una presentación oral. 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-RA4	CE1-CE4	PEF	40%
RA1-RA4	CE1-CE4	S	20%
RA1-RA4	CE1-CE4	PL	40%

Convocatoria Ordinaria, Evaluación final

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1- RA4	CE1-CE4	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-RA4	CE1-CE4	PEF	40%
RA1-RA4	CE1-CE4	S	20%
RA1-RA4	CE1-CE4	PL	40%

Convocatoria Extraordinaria, Evaluación final

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1- RA4	CE1-CE4	PEF	100%

6. BIBLIOGRAFÍA

Libros recomendados.

- Brown, C. L. T. (2010). Computer evidence. Collection and preservation. Boston: Course Technology PTR.
- The Basics of Digital Forensics. John Sammons. Syngress. 2012. ISBN: 9781597496629.
- NIST. (2006). Performing the Forensic Process. En Guide to integrating forensic techniques into incident response.
- 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.
- Técnicas de Análisis Forense informático para peritos Judiciales profesionales. Pilar Vila Avendaño. ISBN: 978-84-697-7700-8.

La Universidad de Alcalá garantiza a sus estudiantes que, si por exigencias sanitarias las autoridades competentes impidieran la presencialidad total o parcial de la actividad docente, los planes docentes alcanzarían sus objetivos a través de una metodología de enseñanza-aprendizaje y evaluación en formato online, que retornaría a la modalidad presencial en cuanto cesaran dichos impedimentos.

Aprobada en Junta de Facultad 30/05/2022