Universidad de Alcalá

GUÍA DOCENTE

Análisis Forense Avanzado

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20
Primer Curso - Segundo Cuatrimestre

DESCRIPCIÓN DE LA ASIGNATURA

Asignatura	**Análisis Forense Avanzado**
Código:	**202561**
Titulación en la que se imparte:	**Máster Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Automática.** **Área de Ingeniería Telemática.**
Carácter:	**Optativo**
Créditos ECTS:	**3**
Curso y cuatrimestre:	**Primer curso – Segundo Cuatrimestre**
Profesorado:	**Susel Fernández Melián** **José Luis Narbona**
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 "Análisis forense avanzado" se centra en el estudio metodologías y técnicas para analizar el escenario una vez producido un ciberataque. Se estudian herramientas software que permiten extraer información relevante de los dispositivos y discos sin alterar su contenido, con el objetivo de encontrar patrones, información oculta y esclarecer como se ha producido un determinado incidente de seguridad. Se estudian metodologías y herramientas para la gestión y respuesta ante incidentes y se analiza la historia y evolución de delitos informáticos, incluyendo clasificación de delitos informáticos y casos de ciberdelincuencia y ciberterrorismo.

2. COMPETENCIAS

Competencias Generales (CG)

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

CG3	Capacidad para aplicar herramientas a la protección, análisis y evaluación de componentes software, así como para emitir juicios sobre los atributos relacionados con la seguridad de sistemas.
CB6	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
CB7	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
CB8	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CB10	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Esta asignatura contribuye a reforzar las siguientes transversales:

CT1	Gestión del tiempo
CT3	Toma de decisiones
CT4	Orientación a la calidad

Competencias específicas (CESP)

Esta asignatura contribuye a reforzar las siguientes competencias específicas:

CE10	Saber aplicar los procesos, métodos y tecnologías del análisis forense digital.

Resultados del aprendizaje

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

RA1	Aplicar conocimientos y técnicas de seguridad de la información a la gestión de diferentes áreas de negocio, sectores o aplicaciones concretas.
RA2	Conocer y aplicar los conceptos básicos y metodologías para la realización del análisis forense 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.
RA5	Conocer metodologías y herramientas para gestión y respuesta ante incidentes.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)
Introducción al análisis forense: conceptualización y objetivos del análisis forense informático. Metodologías para realizar el análisis forense. Actividad del perito.

Adquisición de evidencias: Documentación de la escena, pasos a seguir para preservar la evidencia, cadena de custodia, clonado, hashing, reporte final.
Técnicas y herramientas para el análisis forense: tipos de análisis forense. Herramientas software aplicadas al análisis forense. Estudio de casos reales de análisis forense.
Gestión y respuesta ante incidentes: detección, definición y clasificación de incidentes. Metodologías y herramientas para la gestión de incidentes. Respuesta ante incidentes. Historia y evolución de delitos informáticos. Tipos de delitos informáticos. Ciberdelincuencia, ciberterrorismo.

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases presenciales teórico prácticas, incluyendo trabajo en ordenador: 21 horas Tutorías: 6 horas Seminarios temáticos y conferencias: 3 horas Total: 30 horas presenciales
Número de horas del trabajo propio del estudiante:	Trabajo personal del estudiante: 30 horas Trabajo en grupos de estudiantes: 15 horas
Total horas	75 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 (mejorar la comprensión de los conceptos de seguridad, detección de intrusiones, análisis de vulnerabilidades y puesta en marcha de medidas de seguridad). • Presentaciones orales y otras actividades. • Actividades de trabajo en grupo.
Tutorías individuales,	• Resolución de dudas. • Apoyo al aprendizaje autónomo.

grupales y vía web (foro, correo, etc.)	
Trabajo autónomo	• 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 Máster, 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 Máster 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 que sabe aplicar conocimientos y técnicas de seguridad de la información a la gestión de diferentes áreas de negocio, sectores o aplicaciones concretas como la criminalística.
CE2	El alumno demuestra conocer y aplicar los conceptos básicos y metodologías para la realización del análisis forense 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 técnicas de análisis forense para hacer investigación post-ataque.
CE5	El alumno demuestra conocer metodologías y herramientas para gestión y respuesta ante incidentes.

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): Consistente en la realización de cuestiones teóricas de desarrollo y/o tipo test y la realización de uno o más ejercicios.
2. Entregables (E) de trabajos personales: Consistente en la realización de tareas de trabajos personal cuyo resultado será la entrega de documentos con los resultados del trabajo.
3. Pruebas de Laboratorio: Consistente en la 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 Examen Final (PEF): Consistente en la 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 E, 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 E, PL, PEI y PEF, y se ha alcanzado, al menos, el 50% de la calificación máxima posible en las pruebas de tipo E y PL.

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1-RA3	CE1, CE2, CE3	PEI1	30%
RA1-RA5	CE1-CE5	PEF	40%
RA1, RA4, RA5	CE1, CE4, CE5	E, PL	30%

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 E, 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 E, PL, PEI y PEF, y se ha alcanzado, al menos, el 50% de la calificación máxima posible en las pruebas de tipo E 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, CE2, CE3	PEI1	30%
RA1-RA5	CE1-CE5	PEF	40%

RA1, RA4, RA5	CE1, CE4, CE5	E, PL	30%

Convocatoria Extraordinaria, Evaluación final

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

6. BIBLIOGRAFÍA

Textos 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 Sapronov, Ayman Shaaban. Publisher: Packt Publishing Release Date: June 2016. ISBN: 9781783554096.