



Universidad
de Alcalá

GUÍA DOCENTE

Ingeniería inversa del software

Máster Universitario en Ciberseguridad

Universidad de Alcalá

Curso Académico 2019/20

GUÍA DOCENTE

Nombre de la asignatura:	Ingeniería inversa del software
Código:	202564
Titulación en la que se imparte:	Máster Universitario en Ciberseguridad
Departamento y Área de Conocimiento:	Ciencias de la Computación. Áreas de Lenguajes y Sistemas Informáticos/ Ciencias de la Computación e Inteligencia Artificial
Carácter:	Optativa
Créditos ECTS:	3
Curso y cuatrimestre:	Anual
Profesorado:	José Javier Martínez Herráiz
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

La ingeniería inversa del software nos permite determinar cómo hace funcionar una determinada aplicación para así obtener tanta información como sea posible y necesaria. Se trata de un método de resolución que aporta profundizar en el estudio de su funcionamiento, para obtener mejor comprensión, que podrá ser enfocado a la modificación y mejora.

Esta actividad nos va a permitir descubrir cómo funciona un aplicativo o una determinada función con el requisito importante de que no se dispone de su código fuente.

Conocer estos procesos, aportará una valiosa información, para la correcta comprensión del diseño inicial, que permitirá ayudar a conocer el origen de un determinado software y evaluar sus capacidades, al objeto de tomar las acciones de respuesta necesarias y adecuadas.

2. COMPETENCIAS

Competencias Generales (CG) y Básicas (CB)

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

1. 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.
2. CG4: Capacidad para seleccionar, implantar, desplegar y mantener soluciones de monitorización, defensa e inteligencia en ciberseguridad, combinando diferentes elementos hardware, software y humanos.
3. 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.
4. 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.
5. 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.

Competencias específicas (CE)

Esta asignatura contribuye a reforzar las siguientes competencias específicas:

1. CE1 Capacidad para aplicar conocimientos a la gestión de equipos, centros y departamentos responsables de la seguridad informática, incluyendo la auditoría de esos sistemas basada en un análisis de riesgos y el establecimiento de políticas.
2. CE4 Capacidad para aplicar, escoger y valorar diferentes controles de seguridad, ya sean basados en hardware, software y/o procedimentales.

Resultados del aprendizaje

Por lo anterior, los resultados de aprendizaje esperados son los siguientes:

- RA1: Saber extraer, almacenar, integrar y procesar datos externos de la Web o de darknets, así como de diferentes fuentes de inteligencia especializadas, para su uso como información para la protección y la investigación de inteligencia.
- RA2: Conocer y saber aplicar técnicas de inteligencia computacional y aprendizaje automático a los datos recogidos por sistemas como los mencionados.

3. CONTENIDOS

Bloques de contenido	Total de créditos
Parte I. Análisis estático. Herramientas más comunes en el desarrollo y puesta a punto de un laboratorio de ingeniería inversa para poder averiguar cómo funciona un software sin llegar a ejecutarlo.	1 ECTS
Parte II. Reconstrucción de código. La reconstrucción del código estará asociado a la obtención y estudio de los métodos y patrones y a la búsqueda de vulnerabilidades, necesario para recuperar código fuente perdido, duplicado y para entender al completo un algoritmo.	1 ECTS
Parte III. Análisis dinámico. Describir e identificar las herramientas, malware, sus funcionalidades y automatización.	1 ECTS

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:	

Total horas	75 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases teórico-prácticas	Las clases presenciales serán de carácter teórico-práctico.
Lectura crítica de recursos docentes	Se proporcionarán recursos para el trabajo personal.
Resolución de ejercicios y prácticas	El trabajo personal y grupal se centrará en la resolución de ejercicios y prácticas guiadas.
Elaboración de trabajos	La evaluación será de carácter práctico, mediante la elaboración de trabajos de análisis de datos.

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación¹

Procedimientos

El alumno dispone de dos convocatorias, una ordinaria y otra extraordinaria para la superación de la asignatura.

Convocatoria Ordinaria (Evaluación Continua y Evaluación Final)

En la convocatoria ordinaria, se distinguen dos posibles vías para la evaluación: Evaluación Continua (EC) y Examen Final (EF). El alumno será evaluado preferentemente mediante el proceso descrito de evaluación continua. Para acogerse al proceso de examen final, el alumno debe solicitarlo por escrito al Director del master en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del master comunicará la resolución en un máximo de 15 días. En caso de no haber recibido respuesta, se considera estimada esta solicitud.

Convocatoria Extraordinaria

La convocatoria extraordinaria consistirá en una prueba similar al examen final.

¹ Es importante señalar los procedimientos de evaluación: por ejemplo evaluación continua, final, autoevaluación, co-evaluación. Instrumentos y evidencias: trabajos, actividades. Criterios o indicadores que se van a valorar en relación a las competencias: dominio de conocimientos conceptuales, aplicación, transferencia conocimientos. Para el sistema de calificación hay que recordar la **Normativa del Consejo de Gobierno del 16 de Julio de 2009**: la calificación de la evaluación continua representará, **al menos, el 60%**. Se puede elevar este % en la guía.

Instrumentos de evaluación y Criterios de Calificación

Se plantea una evaluación continua del rendimiento del estudiante mediante Pruebas de evaluación Continua (PEC) de acuerdo a la siguiente Tabla.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CE1, CB7	RA1	Prueba presencial	30%
CE1, CE4, CG3, CG4, CB7, CB10	RA1/RA2	Prueba presencial	30%
CE1, CE4, CG3, CG4, CB6, CB7, CB10	RA1/RA2	Trabajo en equipo	40%

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar un examen final presencial.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
Todas	Todos	Examen presencial	100%

La convocatoria extraordinaria plantea una única prueba de consistente igualmente en un examen final presencial.

6. BIBLIOGRAFÍA

Bibliografía Básica

1. Eilam E. (2005). **Reversing: Secrets of Reverse Engineering**. Addison Wesley Professional.
2. Davis, M., Bodmer, S., and Lemasters. A. (2010). **Hacking Exposed™ Malware & Rootkits: Security Secrets & Solutions**. McGraw-Hill.
3. Graff, M. G., and van Wyk, K. R. (2003). **Secure Coding: Principles & Practices**. O'Reilly.
4. Howard, M., and LeBlanc, D. (2003). **Writing Secure Code**. Microsoft Press.
5. Howard, M., and Lipner, S. (2006). **The Security Development Lifecycle: SDL: A Process for Developing Demonstrably Secure Software**. Microsoft Press.