Universidad de Alcalá

GUÍA DOCENTE

Fundamentos de Seguridad en el Software y Componentes

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20

DESCRIPCIÓN DE LA MATERIA

Asignatura	**Fundamentos de seguridad en el software y componentes**
Código	**202554**
Titulación en la que se imparte:	**Master Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Automática.** **Área de Ingeniería Telemática.**
Carácter:	**Obligatorio**
Créditos ECTS:	**4,5**
Curso y cuatrimestre:	**Primer curso**
Profesorado:	**Susel Fernández Melián**
Horario de Tutoría:	
Idioma en el que se imparte:	**Español**

1. PRESENTACIÓN

En la actualidad, con el aumento de la conectividad a internet por parte de las aplicaciones, los sistemas de información son cada vez más vulnerables a ataques maliciosos y otros factores que ponen en riesgo la integridad, la autenticación y la disponibilidad de la información. Estos ataques pueden materializarse a través de la explotación de algunas vulnerabilidades del software tales como errores de implementación, defectos de diseño, mal manejo de errores, etc. La seguridad en el software tiene como objetivo proteger nuestros sistemas y aplicaciones utilizando prácticas de programación que consideren la seguridad desde el primer momento del ciclo de vida del software.

La asignatura "Fundamentos de seguridad en el software y componentes" forma parte del módulo de Seguridad en el Software y Componentes, que tiene como objetivo permitir al estudiante adquirir conocimientos y profundizar en materias relacionadas con la construcción de arquitecturas y componentes software de todo tipo y condición con un grado suficiente de seguridad. En esta asignatura se introducen los principales conceptos que abarca la seguridad del software y de los sistemas operativos, su importancia en la seguridad global de un sistema, las propiedades de un software seguro, así como las principales vulnerabilidades y amenazas en el software. Se introducen técnicas de análisis de malware para comprender el funcionamiento del código malicioso y evaluar los daños causados y también se tratan las particularidades de la seguridad en aplicaciones y servicios web y aplicaciones para dispositivos móviles con sus rasgos y características propios. Además, se abordan temas relacionados con la investigación de delitos informáticos como el ciberterrorismo y la ciberdelincuencia.

2. COMPETENCIAS

Competencias Generales (CG)

Esta materia 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 materia contribuye a reforzar las siguientes transversales:

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

Competencias específicas (CESP)

Esta materia contribuye a reforzar las siguientes competencias específicas:

CE8	Saber aplicar técnicas de indagación de vulnerabilidades en el software y en las redes, así como ser capaz de aplicar contramedidas para esas técnicas.
CE9	Saber analizar software malicioso destinado a la intrusión o exfiltración en sus aspectos estáticos y dinámicos, para componentes individuales o redes complejas.
CE10	Saber aplicar los procesos, métodos y tecnologías del análisis forense digital.

Resultados del aprendizaje

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

RA1	Construcción de arquitecturas software con un grado de seguridad aceptable en escenarios concretos, utilizando diferentes aproximaciones y metodologías.
RA2	Utilización de buenas prácticas de seguridad (S-SDLC) en el desarrollo del software.
RA3	Análisis y despliegue de metodologías y herramientas de análisis de malware.
RA4	Selección e implementación de tecnologías y metodologías de diseño y desarrollo seguro de acuerdo con los requisitos de diferentes usuarios y organizaciones.
RA5	Aplicación de técnicas avanzadas de análisis forense para hacer investigación post-ataque.
RA6	Uso correcto de los lenguajes y constructores para acceder a los datos.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)
Seguridad del software y los sistemas operativos: beneficios, importancia en la seguridad global de un sistema, propiedades del software seguro, metodologías aplicables a los procesos de desarrollo seguro de software. Análisis y técnicas de diseño más comunes de malware en sus diferentes categorías.
Seguridad en aplicaciones Web y móviles: particularidades de las aplicaciones y servicios web y aplicaciones para dispositivos móviles con sus rasgos y características propios.
Vulnerabilidades y amenazas: principales vulnerabilidades y amenazas en el software y en la programación de los accesos a bases de datos y a sistemas de gestión de ficheros.
Introducción al Análisis Forense: Técnicas de análisis forense. Delitos informáticos: ciberterrorismo y ciberdelincuencia.

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: 31,5 horas Tutorías: 9 horas Seminarios temáticos y conferencias: 4,5 horas Total: 45 horas presenciales
Número de horas del trabajo propio del estudiante:	Trabajo personal del estudiante: 45 horas Trabajo en grupos de estudiantes: 22,5 horas
Total horas	112,5 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, 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

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:** En 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 es capaz de diseñar arquitecturas software con un grado de seguridad aceptable en escenarios concretos, utilizando diferentes aproximaciones y metodologías.
CE2	El alumno es capaz de reconocer y aplicar buenas prácticas de seguridad en el desarrollo del software.
CE3	El alumno conoce metodologías y herramientas para el análisis de malware.

CE4	El alumno es capaz de seleccionar e implementar tecnologías y metodologías de diseño y desarrollo seguro de acuerdo con los requisitos de diferentes usuarios y organizaciones.
CE5	El alumno demuestra conocer técnicas de análisis forense para hacer investigación post-ataque.
CE6	El alumno es capaz de reconocer el uso correcto de los lenguajes y constructores para acceder a los datos.

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, RA2, RA3	CE1, CE2, CE3	PEI1	30%
RA1-RA6	CE1-CE6	PEF	40%
RA1-RA6	CE1-CE6	E, PL	30%

Convocatoria Ordinaria, Evaluación final

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1-RA6	CE1-CE6	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, RA2, RA3	CE1, CE2, CE3	PEI1	30%
RA1-RA6	CE1-CE6	PEF	40%
RA1-RA6	CE1-CE6	E, PL	30%

Convocatoria Extraordinaria, Evaluación final

Resultados de aprendizaje	Criterios de evaluación	Instrumentos de evaluación	Peso en la calificación
RA1-RA6	CE1-CE6	PEF	100%

6. BIBLIOGRAFÍA

Textos recomendados

- Building Secure Software: How to Avoid Security Problems the Right Way. Viega, John; McGraw, Gary. ISBN: 9780201721522. Addison Wesley Professional, 2001
- The art of software security assessment: identifying and preventing software vulnerabilities. Dowd, Mark; McDonald, John; Schuh, Justin. ISBN: 9780321444424. Addison-Wesley, 2007
- Core software security: security at the source. Ransome, James F. ISBN: 9781466560956. Taylor & Francis, 2013
- Software Security: Building Security In. Gary McGraw. Addison-Wesley Professional. ISBN: 9780321356703
- Black Hat Physical Device Security: Exploiting Hardware and Software. Miller, Drew; Bednarczyk, Michael. ISBN: 9781932266818. Syngress Press [Imprint], 2004
- A bug hunter's diary: a guided tour through the wilds of software security. Klein, Tobias. ISBN: 9781593273859
- Malware Analyst's: Tools and Techniques for Fighting Malicious Code. Ligh, Michael; Richard,Matthew; Adair,Steven. ISBN: 9780470613030. Wiley [Imprint], 2010
- The Basics of Digital Forensics. John Sammons. Syngress. 2012. ISBN: 9781597496629.
- System Forensics, Investigation, and Response, 3rd Edition. Easttom. Jones & Bartlett Learning. August 2017.