Universidad de Alcalá

GUÍA DOCENTE

Diseño y Desarrollo de Sistemas Seguros

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20

GUÍA DOCENTE

Nombre de la asignatura:	**Diseño y Desarrollo de Sistemas Seguros**
Código:	202558
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:	Iván Marsá Maestre
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

Una estrategia fundamental para la seguridad en el software y en los componentes es el uso de principios y buenas prácticas de seguridad durante todo su ciclo de vida. La obtención de sistemas seguros implica la utilización de metodologías o procedimientos para el análisis, diseño, implementación y prueba de los sistemas que permitan tener en cuenta la seguridad como un elemento primordial, estableciendo requerimientos y controles de seguridad medibles durante todo su ciclo de desarrollo.

En esta asignatura se estudian los procesos y técnicas para garantizar la seguridad del software y los componentes a lo largo de todo su ciclo de vida, abarcando especificación de requisitos de seguridad, casos de abuso, análisis de riesgo, análisis de código, pruebas de penetración dinámicas, modelado de amenazas, operaciones de seguridad y revisiones externas, entre otras.

2. COMPETENCIAS

Competencias Generales (CG) y Básicas (CB)

Esta asignatura contribuye a alcanzar las siguientes competencias generales y básicas, tal y como se recoge en la memoria de verificación del estudio:

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.

Competencias específicas (CE)

Esta asignatura contribuye a alcanzar las siguientes competencias específicas, tal y como se recoge en la memoria de verificación del estudio:

CE8	Capacidad para aplicar técnicas de indagación de vulnerabilidades en el software y en las redes, así como ser capaz de aplicar contramedidas para esas técnicas.
CE9	Capacidad para analizar software malicioso destinado a la intrusión o exfiltración en sus aspectos estáticos y dinámicos, para componentes individuales o redes complejas

Competencias transversales (CT)

Esta asignatura contribuye a alcanzar las siguientes competencias transversales, tal y como se recoge en la memoria de verificación del estudio:

CT1	Gestión del tiempo
CT3	Trabajo en equipo
CT4	Resolución de problemas

Resultados del aprendizaje

Al término de la asignatura, 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 practicas de seguridad (S-SDLC) en el desarrollo del software.
RA3	Selección e implementación de tecnologías y metodologías de diseño y desarrollo seguro de acuerdo con los requisitos de diferentes usuarios y organizaciones.
RA4	Trabajar en equipo de forma colaborativa para la resolución de problemas relacionados con la seguridad de las comunicaciones y comunicar de manera eficaz sus conocimientos, procedimientos, resultados e ideas al respecto, tanto por escrito como de forma oral.

3. CONTENIDOS

Bloques de contenido
Modelado de amenazas. Estrategias para el modelado de amenazas. El modelo de amenazas STRIDE. Amenazas de suplantación de identidad. Amenazas de alteración. Amenazas de filtración de información. Amenazas de denegación de servicio. Amenazas de elevación de privilegios. Árboles de ataques. Bibliotecas de ataques. CAPEC. OWASP Top 10. Herramientas para el modelado de amenazas. El papel de los requisitos en las amenazas y mitigaciones. Mapeo de amenazas a gestión de riesgos y requisitos de seguridad
El ciclo de vida de desarrollo seguro. Modelos de madurez de sistemas seguros. Recursos para buenas prácticas de diseño seguro. Principios del desarrollo seguro. Principio de mínimo privilegio. Principios de privacidad. Integración del desarrollo seguro en el ciclo de desarrollo de un proyecto. Particularización para el desarrollo de software. Buenas prácticas en el diseño de arquitectura. Buenas prácticas en el diseño detallado. Buenas prácticas en la implementación. Buenas prácticas en la entrega y en el soporte.
Herramientas para el desarrollo de software seguro. Herramientas de revisión de código. Análisis de riesgo a nivel de arquitectura. Tests de penetración. Pruebas basadas en el análisis de riesgos. Casos de abuso.

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. • Análisis y valoración de fuentes primarias y secundarias. • Actividades con ordenador 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. • Análisis y valoración de fuentes primarias y secundarias. • 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, una ordinaria y otra extraordinaria para la superación de la asignatura.

Convocatoria Ordinaria (Evaluación Continua y Evaluación Final)

En la convocatoria ordinaria, se distingues 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 Máster en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del Máster 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.

Instrumentos de evaluación y Criterios de Calificación

Se plantea una evaluación continua del rendimiento del estudiante mediante el seguimiento del trabajo programado y la realización de una prueba parcial a mitad de cuatrimestre, más una prueba de conjunto a realizar al final del semestre.

- Actividades de seguimiento entregables (E): El seguimiento del trabajo del estudiante permite que el profesor conozca el grado de dedicación del estudiante respecto a las distintas actividades propuestas. A su vez, a los estudiantes les sirve para conocer si van alcanzando los objetivos marcados a lo largo del curso. Las actividades de seguimiento podrán plantearse para hacer en clase, o como trabajo personal para el alumno, y podrán temer carácter individual o grupal. Las actividades de seguimiento suponen un 40% de la calificación final.
- Prueba de evaluación Intermedia (PEI): La prueba de Evaluación Intermedia tiene un peso del 30% sobre la calificación final.
- Prueba de Evaluación Final (PEF): La Prueba de Evaluación Final tiene un peso del 30% de la calificación final, y persigue un doble objetivo: evaluar la capacidad de relación de los conceptos aprendidos y revisar los conceptos evaluados en la prueba parcial. Por ello, si se ha obtenido al menos un 20% de calificación en las actividades de seguimiento, la prueba de conjunto permitirá además mejorar la calificación final si se obtiene un resultado superior al obtenido al aplicar la media de todas las calificaciones.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT1, CT3, CT4	RA1-RA4	E	40%

CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT4	RA1-RA3	PEI	30%
CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT4	RA1-RA3	PEF	30%

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar una prueba de evaluación final (PEF) que incluye cuestiones teóricas y la realización de uno o más ejercicios, con un peso del 60% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE6, CT4, CT5	RA1-RA4	PEF	60%
CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT1, CT3, CT4	RA1-RA4	TA	40%

La convocatoria extraordinaria plantea una única prueba de evaluación extraordinaria (PEE), que incorpora cuestiones teóricas y la resolución de uno o más ejercicios, con un peso del 70% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final. Para los estudiantes que hayan seguido el proceso de evaluación continua y hayan obtenido al menos un 20% en las actividades de seguimiento, la PEE tendrá un peso del 60%, tomándose el 40% restante de calificación de las actividades de seguimiento.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT1, CT3, CT4	RA1-RA4	E	40%
CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT4	RA1-RA3	PEE	60%

CG3, CB6, CB7, CB8, CB10, CE8, CE9, CT1, CT3, CT4	RA1-RA4	TA	40%

6. BIBLIOGRAFÍA

Textos recomendados.

- Anderson, Ross. *Security engineering*. John Wiley & Sons, 2008.
- Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.
- McGraw, Gary. *Software security: building security in*. Vol. 1. Addison-Wesley Professional, 2006.
- Rerup, Neil, and Milad Aslaner. *Hands-On Cybersecurity for Architects: Plan and design robust security architectures*. Packt Publishing Ltd, 2018.
- Ransome, James, and Anmol Misra. *Core software security: Security at the source*. CRC press, 2018