1. DATOS BÁSICOS

Asignatura	La seguridad en el software base y las aplicaciones
Titulación	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones
Escuela/ Facultad	Arquitectura, Ingeniería y Diseño
Curso	Primero
ECTS	6 ECTS
Carácter	Obligatorio
Idioma/s	Castellano
Modalidad	Presencial - 0DCS001104 Online - P630001104
Semestre	Primer semestre
Curso académico	2024/2025
Docente Coordinador	Presencial: Prof. D. Pablo González Pérez Online: Prof. D. Pablo González Pérez Prof. Antonio José Sánchez Moscoso

2. PRESENTACIÓN

El estudiante aprenderá cómo se configuran y gestionan los sistemas operativos para implantar medidas de seguridad, cómo se diseñan y desarrollan aplicaciones informáticas seguras, qué medidas de protección se emplean contra virus y otros tipos de software malicioso, y por último, cómo se gestiona la seguridad en las bases de datos. El estudiante aplicará los conocimientos teóricos a prácticas de configuración de seguridad en sistemas operativos.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CG.4. Emitir juicios en función de criterios, de normas externas o de reflexiones personales.
- CG.6. Capacidad para integrarse en equipos de trabajo multidisciplinares de manera eficaz y cooperativa.

Competencias específicas:

- CE9: Ser capaces de configurar y gestionar los sistemas operativos para implantar medidas de seguridad, así como los principios de diseño y desarrollo de aplicaciones informáticas seguras y de seguridad en las bases de datos.
- CE10: Conocer las medidas de protección que se emplean contra virus y otros tipos de software malicioso.

Resultados de aprendizaje:

- RA1: El estudiante será capaz de aplicar los conceptos básicos utilizando técnicas de aprendizaje cooperativo.
- RA4: El estudiante será capaz de desarrollar procedimientos de operación para una empresa cliente sobre la configuración segura de sus sistemas operativos.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CG6, CE9, CE10	RA1
CG4, CG6, CE9, CE10	RA4

4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

1.1 CONFIGURACIÓN SEGURA DE BASES DE DATOS Y APLICACIONES
Unidad 1. La seguridad en las aplicaciones y bases de datos I

- 1.1. Análisis de puertos.
- 1.2. Análisis de vulnerabilidades.
- 1.3. Servicios. Usuarios y contraseñas.
- 1.4. Aplicaciones web. Usuarios y contraseñas

Unidad 2. La seguridad en las aplicaciones y bases de datos II

- 2.1. Introducción a las vulnerabilidades Web y OWASP.
- 2.2. Análisis automático de vulnerabilidades web.
- 2.3. Laboratorio 1. Vulnerabilidades web
- 2.4 Laboratorio 2. Vulnerabilidades web

Unidad 3. La seguridad en las aplicaciones y bases de datos III

- 3.1. Identificación y explotación de XSS.
- 3.2. Identificación y explotación de inyecciones de SQL.
- 3.3. Laboratorio 3. Ataques XSS.
- 3.4. Laboratorio 4. Ataques mediante inyección SQL

1.2 CONFIGURACIÓN SEGURA DE SISTEMAS OPERATIVOS
Unidad 4. Práctica de configuración segura de sistemas Windows

- 4.1. Introducción y revisión de configuración segura en Windows.
- 4.2. Introducción a los exploits en Windows.
- 4.3. Laboratorio 5. Configuración segura en Windows
- 4.4. Laboratorio 6. Exploits en Windows

Unidad 5. Práctica de configuración segura de sistemas Linux

- 5.1. Introducción a la seguridad en Linux.
- 5.2. Seguridad en Linux.
- 5.3. Práctica de revisión de seguridad con Lynis.
- 5.4. Práctica de bastionado de sistemas Linux - OpenSCAP.

1.3 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Unidad 6. Protección contra software malicioso

- 6.1. Introducción a los mecanismos de protección.
- 6.2. Instalación de backdoors y rootkits.
- 6.3. Detección de backdoors y rootkits

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

- Clase magistral.
- Método del caso.
- Aprendizaje cooperativo.
- Aprendizaje basado en proyectos.

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad presencial:

Actividad formativa	Número de horas
A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición	25 h
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	68,75 h
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	31,25 h
TOTAL	**150 h**

Modalidad online:

Actividad formativa	Número de horas
A1. Participación en debates y foros de discusión moderados por el profesor	32,5 h
A2. Realización de actividades aplicativas colaborativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25 h
A3. Trabajo integrador del módulo	10 h
A4. Realización de actividades aplicativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25 h
A5. Estudio independiente del alumno	32,5 h
A6. Tutoría y evaluación	25 h

A7 Participación en debates y foros de discusión moderados por el profesor	32,5 h
TOTAL	150h

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad presencial:

Sistema de evaluación	Peso
Actividades teórico-prácticas de Linux y test final de conocimiento	10%
Examen teórico de conocimientos sobre seguridad de sistemas operativos Linux	15%
Prácticas individuales sobre seguridad de sistemas operativos Linux	15%
Ejecución e implementación de los laboratorios y ejercicios prácticos propuestos	20%
Trabajo en grupo sobre seguridad en Windows	10%
Implementación y ejecución de laboratorio. Seguridad en la web, en la base de datos y en aplicaciones	15%
Ejecución e implementación de ejercicios prácticos	15%

Modalidad online:

Sistema de evaluación	Peso
Reconocimiento de software vulnerable con herramientas de auditoría	5%
Reconocimiento de arquitectura y explotación LFI	10%
Identificación y explotación de vulnerabilidad de inyección XSS y SQL	15%
Explotación de vulnerabilidades en Windows con Metasploit	10%
Configuración de Linux de forma segura	15%
Revisión de los puntos de inicio de Windows	10%
Identificación y explotación de Command Injection + Escalada de privilegios con Path Hijacking	15%
Prueba de conocimientos	20%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

Modalidad presencial:

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

En la modalidad online será necesario obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de las actividades.

En la modalidad online será necesario obtener en la prueba de conocimiento una calificación igual o superior a 5.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

Modalidad online:

En ambas convocatorias (ordinaria y extraordinaria) se permitirá la entrega tardía con un máximo de una semana a partir de la fecha de entrega fijada, con una **penalización de 0,25 puntos sobre 10 por día de retraso**. Una vez superada la semana, no se permitirá la entrega salvo casos excepcionales de fuerza mayor que deba estudiar el personal docente implicado.

Las actividades se entregarán en el campus virtual, no siendo válida la entrega por correo electrónico.

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1 hasta A7), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

Para superar la asignatura en convocatoria extraordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1 hasta A7), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Modalidad presencial:

Sistema de evaluación	FECHA
Actividades teórico-prácticas de Linux y test final de conocimiento	SEM 1
Examen teórico de conocimientos sobre seguridad de sistemas operativos Linux	SEM 2
Prácticas individuales sobre seguridad de sistemas operativos Linux	SEM 3
Ejecución e implementación de los laboratorios y ejercicios prácticos propuestos	SEM 5
Trabajo en grupo sobre seguridad en Windows	SEM 7
Implementación y ejecución de laboratorio. Seguridad en la web, en la base de datos y en aplicaciones	SEM 8
Ejecución e implementación de ejercicios prácticos	SEM 9

Modalidad online:

Sistema de evaluación	FECHA
A1. Reconocimiento de software vulnerable con herramientas de auditoría.	SEM 2
A2. Reconocimiento de arquitectura y explotación LFI	SEM 4
A3. Identificación y explotación de vulnerabilidad de inyección XSS y SQL	SEM 7
A4. Explotación de vulnerabilidades en Windows con Metasploit	SEM 8
A5. Configuración de Linux de forma segura	SEM 10
A6. Revisión de los puntos de inicio de Windows.	SEM 11
A7. Identificación y explotación de Command Injection + Escalada de privilegios con Path Hijacking	SEM 11

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

A continuación, se indica bibliografía recomendada:

M4.1. Configuración segura de sistemas operativos

- Linux essentials, Roderik W. Smith, Anaya, 2013. https://www.amazon.es/Linux-Essentials-Roderick-W-Smith/dp/1118106792
- Guías de Seguridad de Cis Security <https://www.cisecurity.org/> (consultado en Enero 2018)
- Herramienta de seguridad para Linux OpenSCAP <https://www.open-scap.org/> (consultado en Enero 2018)
- Guía de bastionado de CentOS <https://wiki.centos.org/HowTos/OS_Protection> (consultado en Enero 2018)
- Guía de Seguridad de RedHat <https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/> (consultado Enero 2018).

M4.2. Configuración segura de bases de datos y aplicaciones

- TOP 10 OWASP. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- DVWA. Aplicación de pruebas web vulnerable. http://www.dvwa.co.uk
- Guía de buenas prácticas de desarrollo web y aplicaciones de bases de datos. https://www.owasp.org/index.php/Main_Page

M4.3. Protección contra software malicioso

- UAC, AppLocker. Protecciones Windows contra software malicioso. https://support.microsoft.com/es-co/help/922708/how-to-use-user-account-control-uac-in-windows-vista
- NAP. https://docs.microsoft.com/en-us/windows/desktop/nap/network-access-protection-start-page

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo

educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.
Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tú opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.