1. DATOS BÁSICOS

Asignatura	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	2019/2020
Docente coordinador	Presencial: Dr. Diego Gachet Online: Dr. Diego Gachet

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

Tipo de 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

Tipo de 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: 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
TOTAL	**150 h**

7. EVALUACIÓN

Para desarrollar las competencias y alcanzar los resultados de aprendizaje indicados, deberás realizar las actividades que se indican en la tabla inferior:

MODALIDAD PRESENCIAL

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Actividades teórico-prácticas de Linux y test final de conocimiento	10%
Actividad 2	Examen teórico de conocimientos sobre seguridad de sistemas operativos Linux	15%
Actividad 3	Prácticas individuales sobre seguridad de sistemas operativos Linux	15%
Actividad 4	Ejecución e implementación de los laboratorios y ejercicios prácticos propuestos	20%
Actividad 5	Trabajo en grupo sobre seguridad en Windows	10%
Actividad 6	Implementación y ejecución de laboratorio. Seguridad en la web, en la base de datos y en aplicaciones	15%
Actividad 7	Ejecución e implementación de los laboratorios y ejercicios prácticos	15%

MODALIDAD ONLINE

Actividad evaluable	Actividad de aprendizaje	Peso (%)
A1	Reconocimiento de software vulnerable con herramientas de auditoría	5%

A2	Reconocimiento de arquitectura y explotación LFI	5%
A3	Identificación y explotación de vulnerabilidad de inyección XSS y SQL	5%
A4	Explotación de vulnerabilidades en Windows con Metasploit	5%
A5	Debate Foro sobre vulnerabilidad	15%
A6	Configuración de Linux Centos de forma segura	10%
A7	Fortificación y OpenScap	15%
A8	Revisión de los puntos de inicio de Windows	5%
A9	Web vulnerable a LFI y SQL Injection	10%
A10	Prueba de conocimientos	20%

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

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 esta 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.

MODALIDAD PRESENCIAL

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener al menos un 70% en el test de conocimiento de M4.1 tras realizar los ejercicios y prácticas online (actividad 1).
- Obtener una nota mínima de 4 en las pruebas objetivas de M4.1 y M4.2 (actividades 2 y 7).
- Obtener al menos un 4 en las prácticas y en el trabajo (actividades 3, 4, 5, 6 y 9)
- Obtener una media ponderada de todas las actividades igual o superior a 5.

7.2. Convocatoria extraordinaria

Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor (correspondientes a las partes no entregadas o suspensas ya sean las mismas actividades u otras equivalentes a éstas). La nota de cada actividad deberá ser igual o mayor que 3 y la de las pruebas objetivas igual o mayor que 4. La media ponderada de todas las actividades de evaluación deberá ser igual o mayor a 5.

MODALIDAD ONLINE

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de todas las actividades que figuran en la tabla igual o superior a 5, y obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

- Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor, cuya nota media ponderada debe ser igual o superior a 5, y obtener en las pruebas de conocimiento una calificación igual o superior a 5.

8. CRONOGRAMA

SEMESTRE	MES	M1	M2	M3	M4	M5	M6	M7	M8	M9.2	M10
1	Octubre										
	Noviembre										
	Diciembre										
	Enero										
	Febrero										
	Marzo										
2	Abril										
	Mayo										
	Junio										
	Julio										

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

MODALIDAD ONLINE

CALENDARIO ACADÉMICO 2019-2020

Universidad Europea
LAUREATE INTERNATIONAL UNIVERSITIES

NOVIEMBRE 2019

L	M	M	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

DICIEMBRE 2019

L	M	M	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

ENERO 2020

L	M	M	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

FEBRERO 2020

L	M	M	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

MARZO 2020

L	M	M	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

ABRIL 2020

L	M	M	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

MAYO 2020

L	M	M	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

JUNIO 2020

L	M	M	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

JULIO 2020

L	M	M	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

AGOSTO 2020

L	M	M	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

SEPTIEMBRE 2020

L	M	M	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Periodo no lectivo
Entrega TFM
Defensa TFM
Inicio Curso
Festivos

Calendario sujeto a cambios en relación con las festividades: los días festivos serán fijados por el Estado y la Comunidad Autónoma correspondiente

SEMESTRE	MES	M1	M2	M3	M4	M5	M6	M7	M8	M9.B	M10
1	Octubre										
	Noviembre										
	Diciembre										
	Enero										
	Febrero										
	Marzo										
2	Abril										
	Mayo										
	Junio										
	Julio										
	Agosto										
	Septiembre										

9. BIBLIOGRAFÍA

A continuación, se indica la 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)
- Guia 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).
- **WINDOWS**

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

Estudiantes con necesidades específicas de apoyo educativo:

Las adaptaciones o ajustes curriculares para estudiantes con necesidades específicas de apoyo educativo, a fin de garantizar la equidad de oportunidades, serán pautadas por la Unidad de Atención a la Diversidad (UAD).

Será requisito imprescindible la emisión de un informe de adaptaciones/ajustes curriculares por parte de dicha Unidad, por lo que los estudiantes con necesidades específicas de apoyo educativo deberán contactar a través de: unidad.diversidad@universidadeuropea.es al comienzo de cada semestre.