

## 1. DATOS BÁSICOS

<b>Asignatura</b>	La seguridad en las comunicaciones
<b>Titulación</b>	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones
<b>Escuela/ Facultad</b>	Arquitectura, Ingeniería y Diseño
<b>Curso</b>	Primero
<b>ECTS</b>	6 ECTS
<b>Carácter</b>	Obligatorio
<b>Idioma/s</b>	Castellano
<b>Modalidad</b>	Presencial - ODCS001106
<b>Semestre</b>	Segundo semestre
<b>Curso académico</b>	2019/2020
<b>Docente coordinador</b>	Abel Lozoya de Diego

## 2. PRESENTACIÓN

El estudiante se familiarizará con los conceptos básicos de seguridad en las comunicaciones, aplicados a los casos de controles de seguridad en la red (WAN y LAN), protección del perímetro de la red, la seguridad en las redes inalámbricas, y se conocerán las tecnologías VLAN/SSL/SSH/IPSEC.

## 3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

### Competencias básicas:

- CG.2. Aprender a aplicar a entornos nuevos o poco conocidos, dentro de contextos más amplios (o multidisciplinares), los conceptos, principios, teorías o modelos relacionados con su área de estudio.
- CG.6. Capacidad para integrarse en equipos de trabajo multidisciplinares de manera eficaz y cooperativa.

### Competencias específicas:

- CE14. Conocer los conceptos avanzados de seguridad en las comunicaciones, aplicados a los casos de controles de seguridad en la red, protección del perímetro de la red y será capaz de discriminar entre las distintas tecnologías VLAN/SSL/SSH/IPSEC.
- CE20. Conocer los métodos de trabajo de las empresas consultoras de seguridad y aprender a escribir informes y procedimientos sobre las tareas básicas relacionadas con la seguridad de la organización.

### Resultados de aprendizaje:

- RA1. El estudiante será capaz de aplicar los conceptos básicos utilizando técnicas de aprendizaje cooperativo.
- RA5. Desarrollo de un procedimiento de seguridad para la red inalámbrica de la empresa cliente para la que se instala y configura la red inalámbrica.

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
CG2, CG6, CE14	RA1
CG2, CE20	RA5

## 4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

### 1.1 LA SEGURIDAD EN LAS COMUNICACIONES

#### Unidad 1. La seguridad en las Comunicaciones I

- 1.1. Introducción a la seguridad en las comunicaciones.
- 1.2. Ataques de red.
- 1.3. Introducción a los IDS.
- 1.4. Monitorización de seguridad de red.

#### Unidad 2. La seguridad en las Comunicaciones II

- 2.1. Denegación de servicio.
- 2.2. Introducción a los Honeypots.
- 2.3. Honeypot.

### 1.2 PRÁCTICA PROFESIONAL DE CONFIGURACIÓN SEGURA DE REDES INALÁMBRICAS

#### Unidad 3. Práctica de configuración segura de redes inalámbricas I

- 3.1. Introducción a las redes inalámbricas.
- 3.2. Securización de las redes inalámbricas

#### Unidad 4. Práctica de configuración segura de redes inalámbricas II

- 4.1. Ataques a redes inalámbricas I.
- 4.2. Ataques a redes inalámbricas II.

### 1.3 PRÁCTICA PROFESIONAL DE INSTALACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

#### Unidad 5. Práctica de instalación y configuración de cortafuegos I

- 5.1. Introducción a los cortafuegos.
- 5.2. Cortafuegos de código libre.
- 5.3. Despliegue, redes, zonas, interfaces y niveles de seguridad.

#### Unidad 6. Práctica de instalación y configuración de cortafuegos II

- 6.1. Configuración de políticas.
- 6.2. Alta disponibilidad.
- 6.3. Túneles VPN.

## 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	31,25 h
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	62,5 h
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	31,25 h
<b>TOTAL</b>	<b>150 h</b>

### 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
<b>TOTAL</b>	<b>150 h</b>

## 7. EVALUACIÓN

En la tabla inferior se indican las actividades evaluables y los pesos de cada una de ella.

### MODALIDAD PRESENCIAL

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Repaso de conceptos de comunicaciones y test de conocimientos	10%
Actividad 2	Trabajo individual de investigación y desarrollo en el que habrá que aplicar los conceptos básicos aprendidos a un tema de actualidad relacionados con la seguridad en las comunicaciones sobre un dispositivo	10%
Actividad 3	Trabajo en grupo de investigación y desarrollo sobre la seguridad en IoT / loE	15%
Actividad 4	Práctica. Ataques a las comunicaciones	25%
Actividad 5	Resolución de laboratorios prácticos en el aula para la configuración segura de redes inalámbricas. Examen de conocimiento práctico	10%
Actividad 6	Práctica de pivoting	10%
Actividad 7	Introducción a la plataforma y a los Firewalls virtuales	10%
Actividad 8	Instalación y aplicación de reglas de Firewall en una red LAN	10%

## MODALIDAD ONLINE

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Envenamiento de ARP	5%
Actividad 2	Honeypots	5%
Actividad 3	Debate en el foro sobre caso real de ataque de red a partir de casos publicados	15%
Actividad 4	Descripción del protocolo WPA.	10%
Actividad 5	Desarrollo de un procedimiento de seguridad para la red inalámbrica de la empresa cliente para la que se instala y configura la red inalámbrica.	15%
Actividad 6	Instalación de un sistema virtual con firewall pfsense y VPN	15%
Actividad 7	Túnel VPN con OpenVPN	10%
Actividad 8	Prueba de conocimientos	25%

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) no se permitirá la entrega tardía de las actividades puntuables. Las actividades no puntuables se podrán entregar hasta con 1 semana de retraso. Una vez superada esta fecha, 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 M6.1 tras realizar los ejercicios y prácticas online (actividad 1) y un 4 en el test de evaluación de la actividad 4.
- Obtener una nota mínima de 4 en la prueba objetiva de M6.2 (actividad 5).
- Obtener al menos un 4 en los trabajos y resoluciones de casos prácticos (actividades 3, 6, 7, 8 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

### MODALIDAD PRESENCIAL



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										

# MODALIDAD ONLINE

## CALENDARIO ACADÉMICO 2019-2020



NOVIEMBRE 2019							DICIEMBRE 2019							ENERO 2020							
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	
				1	2	3	2	3	4	5	6	7	8	6	7	8	1	2	3	4	5
4	5	6	7	8	9	10	9	10	11	12	13	14	15	13	14	15	16	17	18	19	
11	12	13	14	15	16	17	16	17	18	19	20	21	22	20	21	22	23	24	25	26	
18	19	20	21	22	23	24	23	24	25	26	27	28	29	27	28	29	30	31			
25	26	27	28	29	30		30	31													

  

FEBRERO 2020							MARZO 2020							ABRIL 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
					1	2	2	3	4	5	6	7	8	6	7	8	9	10	11	12
3	4	5	6	7	8	9	9	10	11	12	13	14	15	13	14	15	16	17	18	19
10	11	12	13	14	15	16	16	17	18	19	20	21	22	20	21	22	23	24	25	26
17	18	19	20	21	22	23	23	24	25	26	27	28	29	27	28	29	30			
24	25	26	27	28	29		30	31												

  

MAYO 2020							JUNIO 2020							JULIO 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
				1	2	3	1	2	3	4	5	6	7	1	2	3	4	5		
4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12
11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19
18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26
25	26	27	28	29	30	31	29	30						27	28	29	30	31		

  

AGOSTO 2020							SEPTIEMBRE 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D
					1	2	1	2	3	4	5	6	
3	4	5	6	7	8	9	7	8	9	10	11	12	13
10	11	12	13	14	15	16	14	15	16	17	18	19	20
17	18	19	20	21	22	23	21	22	23	24	25	26	27
24	25	26	27	28	29	30	28	29	30				
31													

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										
2	Marzo										
	Abril										
	Mayo										
	Junio										
	Julio										
	Agosto										
Septiembre											

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 la bibliografía recomendada.

### M6.1. La Seguridad en la comunicaciones

- La Segmentación de red, <https://www.cisco.com/c/en/us/about/securitycenter/framework-segmentation.html>
- Wifi Alliance: <https://www.wi-fi.org>
- IEEE EAP and 802.1x: <http://ieeexplore.ieee.org/document/1561920/>
- Wikipedia [https://en.wikipedia.org/wiki/IEEE\\_802.11](https://en.wikipedia.org/wiki/IEEE_802.11)
- Modelo OSI: [https://es.wikipedia.org/wiki/Modelo\\_OSI](https://es.wikipedia.org/wiki/Modelo_OSI)
- "Comunicaciones y Redes de Computadores". 7ª edición. William Stallings. Ed. Prentice-Hall. 2004.
- "Redes de computadores". 4ª edición. Andrew S. Tanenbaum. Ed. Prentice-Hall. 2003.

### M6.2. Práctica profesional de configuración segura de redes inalámbricas

- "Hacking Exposed Wireless" (3ª Ed): <http://www.hackingexposedwireless.com>
- "Kali Linux Wireless Penetration Testing: Beginner's Guide" (3ª Ed): <https://www.packtpub.com/networking-and-servers/kali-linux-wireless-penetration-testing-beginner%E2%80%99s-guide-third-edition>
- DinoSec Lab: <http://www.dinosec.com/es/lab.html>
- DinoSec Blog: <http://blog.dinosec.com>

### M6.3. Práctica profesional de instalación y configuración cortafuegos

- "Ataques a redes de datos IPv4 e IPv6" (3ª Ed). Chema Alonso, Juan Luis G. Rambla. Pablo González. Ed. Oxword.
- Flu Project Blog: <http://flu-project.com>
- "Linux Iptables". Gregor N. Purdy. Ed. O'Reilly. 2004.

## 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](mailto:unidad.diversidad@universidadeuropea.es) al comienzo de cada semestre.



## ANEXO – FICHAS COVID-19

Debido a las adaptaciones necesarias para la formación en online de la modalidad presencial se producen los cambios siguientes:

Actividad formativa descrita en la Guía de aprendizaje	Actividad formativa adaptada a formato a distancia
A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición	A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A3. Tutorías y evaluación	A3. Tutorías y evaluación de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A4. Estudio independiente del alumno	A4. Estudio independiente del alumno de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual

Actividad de evaluación presencial planificada según Guía		NUEVA actividad de evaluación que se propone (a distancia)	
Descripción de la actividad de evaluación presencial original	A4. Resolución de laboratorios prácticos en el aula para la configuración segura de redes inalámbricas. Examen de conocimiento práctico	Descripción de la nueva actividad de evaluación	A4. Resolución de laboratorios prácticos en el aula para la configuración segura de redes inalámbricas. Examen de conocimiento práctico de forma online
Contenido desarrollado (temas)	Los contenidos a los que da respuesta la nueva prueba han de ser los mismos. Especificar: Test sobre contenido impartido en la misma clase sobre conocimientos de redes inalámbricas		
Resultados de aprendizaje desarrollados (consultar Guía de aprendizaje de la asignatura/módulo)	Los resultados de aprendizaje a los que da respuesta la nueva prueba han de ser los mismos. Especificar: RA5. Desarrollo de un procedimiento de seguridad para la red inalámbrica de la empresa cliente para la que se instala y configura la red inalámbrica.		
Duración aproximada	30 minutos	Duración aproximada y fecha	30 minutos y 09/05/2020
Peso en la evaluación	10%	Peso en la evaluación	10%
Observaciones	Se utilizará Respondus LockDown Browser		