1. DATOS BÁSICOS

Asignatura	La seguridad en las comunicaciones
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 - 0DCS001106 Online - P630001106
Semestre	Segundo semestre
Curso académico	2024/2025
Docentes	Presencial: D. Pablo González Pérez Online: D. Pablo González Pérez Dr. José Luis Martínez Martínez

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

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.

Unidad 3. Seguridad en redes inalámbricas

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

Unidad 4. Cconfiguración segura de redes inalámbricas II

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

Unidad 5. Insnstalación 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. I nstalación 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:

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
TOTAL	**150h**

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: 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	**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
A1-Ejercicio sobre Seguridad de las comunicaciones - MiTM - VPN - Conceptos basicos de seguridad de redes	35%
Resolución de laboratorios prácticos en el aula para la configuración segura de redes inalámbricas. Examen de conocimiento práctico	15%
Práctica de pivoting	15%
Introducción a la plataforma y a los Firewalls virtuales	15%
Instalación y aplicación de reglas de Firewall en una red LAN	20%

Modalidad online:

Sistema de evaluación	Peso
A1. Envenamiento de ARP	5%
A2. Honeypots	5%
A3. Debate en el foro sobre caso real de ataque de red a partir de casos publicados	15%
A4. Descripción del protocolo WPA.	10%
A5. Configuración segura de red inalámbrica corporativa.	15%
A6. Instalación de un sistema virtual con firewall pfsense y VPN	25%
A7. Prueba de conocimientos	25%

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 ncesario 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 actividades.

En la modalidad online será ncesario 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:

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 A6), 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 A6), 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:

Actividades evaluables	Fecha
A1-Ejercicio sobre Seguridad de las comunicaciones - MiTM - VPN - Conceptos basicos de seguridad de redes	Sem 3
Resolución de laboratorios prácticos en el aula para la configuración segura de redes inalámbricas. Examen de conocimiento práctico	Sem 5
Práctica de pivoting	Sem 7
Introducción a la plataforma y a los Firewalls virtuales	Sem 10
Instalación y aplicación de reglas de Firewall en una red LAN	Sem 12

Modalidad online:

Actividades evaluables	Fecha
A1. Envenamiento de ARP	Sem 2
A2. Honeypots	Sem 3
A3. Debate en el foro sobre caso real de ataque de red a partir de casos publicados	Sem 5
A4. Descripción del protocolo WPA.	Sem 6
A5. Configuración segura de red inalámbrica corporativa.	Sem 8
A6. Instalación de un sistema virtual con firewall pfsense y VPN	Sem 11
A7. Prueba de conocimientos	Sem 12

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:

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
- 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. 0xword.
- Flu Project Blog: http://flu-project.com
- "Linux Iptables". Gregor N. Purdy. Ed. 0'Reilly. 2004.

10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y 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.