

1. DATOS BÁSICOS

Asignatura	Seguridad en Redes
Titulación	Grado en Ingeniería de la Ciberseguridad
Escuela/ Facultad	Escuela de Arquitectura, Ingeniería y Diseño
Curso	Tercero
ECTS	6 ECTS
Carácter	Básico
Idioma/s	Castellano
Modalidad	Online
Semestre	Segundo semestre
Curso académico	2024/2025
Docente coordinador	Enrique De Miguel Ambite

2. PRESENTACIÓN

La asignatura Seguridad en Redes está diseñada para proporcionar a los estudiantes una comprensión integral de los principios fundamentales y las técnicas aplicadas en la protección de redes de comunicaciones modernas. A lo largo del curso, los estudiantes aprenderán a describir los fundamentos de la seguridad en redes y a aplicar estrategias específicas en distintas capas del modelo OSI, desde la capa física y de acceso hasta las capas de routing y transporte. Además, explorarán pautas de seguridad avanzadas para plataformas emergentes como IoT, redes 5G y arquitecturas SASE. También se abordarán técnicas de seguridad perimetral mediante el uso de firewalls, sistemas de detección de intrusiones (IDS), y proxies. Este conocimiento permitirá a los estudiantes diseñar y gestionar infraestructuras de red seguras, adaptándose a las exigencias de entornos tecnológicos cada vez más complejos y conectados, preparando así su perfil profesional para enfrentar desafíos reales en ciberseguridad.

Esta asignatura pertenece a la Materia “Informática” dentro de la Rama de Ingeniería Ingeniería informática y de sistemas.

3. RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje	
Conocimientos	<p>CON05. Reconocer las implicaciones que para la seguridad tiene desarrollar, desplegar y utilizar aplicaciones y servicios basados en tecnologías de red, incluyendo: Internet, web, comercio electrónico, multimedia, servicios interactivos, redes sociales, computación móvil, Internet de las cosas.</p> <p><input type="checkbox"/></p> <p>Describir las bases de la seguridad en las redes de comunicaciones</p> <p><input type="checkbox"/></p> <p>Describir las técnicas y pautas de seguridad en plataformas de servicio tipo IoT, 5G o arquitecturas SASE</p> <p>CON05. Recognizing the security implications of developing, deploying, and using applications and services based on network technologies, including: Internet, web, e-commerce, multimedia, interactive services, social networks, mobile computing, Internet of Things.</p> <p>- Describing the basics of security in communication networks.</p> <p>- Describing security techniques and guidelines in IoT, 5G, or SASE service platforms.</p>
Habilidades	<p>HAB06. Aplicar las arquitecturas y modelos de ciberseguridad.</p> <p><input type="checkbox"/></p> <p>Aplicar las técnicas de seguridad en la capa física y de acceso</p> <p><input type="checkbox"/></p> <p>Aplicar las técnicas de seguridad en la capa de routing y transporte</p> <p><input type="checkbox"/></p> <p>Aplicar las técnicas de seguridad perimetral basadas en Firewall</p> <p><input type="checkbox"/></p> <p>Aplicar las técnicas de seguridad perimetral basadas en detectores de intrusión y elementos proxy</p> <p>HAB06. Applying cybersecurity architectures and models.</p> <p>- Applying security techniques at the physical and access layer.</p> <p>- Applying security techniques at the routing and transport layer.</p> <p>- Applying perimeter security techniques based on firewalls.</p> <p>- Applying perimeter security techniques based on intrusion detection systems and proxy elements.</p>
Competencias	<p><i>CP04. Seleccionar, desarrollar, desplegar y utilizar aplicaciones, servicios y protocolos seguros basados en tecnologías de red, los cuales se adecuen a los requerimientos de las aplicaciones.</i></p> <p><i>CP10. Aplicar y analizar los principios y técnicas basadas en la criptografía que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de la información, así como la autenticación y autorización de sus entidades.</i></p> <p><i>CP14. Utilizar las tecnologías de la información y de la comunicación para la búsqueda y análisis de datos, la investigación, la comunicación y el aprendizaje.</i></p> <p><i>CP18. Adaptarse a situaciones adversas, inesperadas, que causen estrés, ya sean personales o profesionales, superándolas e incluso convirtiéndolas en oportunidades de cambio positivo.</i></p>

	<p><i>CP19. Mostrar comportamientos éticos y compromiso social en el desempeño de las actividades de una profesión, así como sensibilidad a la desigualdad y a la diversidad.</i></p> <p><i>CP04. Select, develop, deploy, and use secure applications, services, and protocols based on network technologies that meet the requirements of the applications.</i></p> <p><i>CP10. Apply and analyze principles and techniques based on cryptography that ensure the confidentiality, integrity, and availability of computer systems and information, as well as the authentication and authorization of entities.</i></p> <p><i>CP14. Use information and communication technologies for data search and analysis, research, communication, and learning.</i></p> <p><i>CP18. Adapt to adverse, unexpected situations that cause stress, whether personal or professional, overcoming them and even turning them into opportunities for positive change.</i></p> <p><i>CP19. Demonstrate ethical behavior and social commitment in the performance of professional activities, as well as sensitivity to inequality and diversity.</i></p>
--	---

4. CONTENIDOS

Seguridad de los componentes de la red

Ataques a la red

Seguridad en Plataformas IoT/OT, Arquitecturas SASE,

Seguridad en 5G

Evolución tecnológica de los firewalls

Plataformas adicionales. IDS, IPS, DLP. Soluciones Proxy

- Network Component Security
- Network Attacks
- Security in IoT/OT Platforms, SASE Architectures
- Security in 5G
- Technological Evolution of Firewalls
- Additional Platforms: IDS, IPS, DLP. Proxy Solutions

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

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

- Clase magistral/ web conference
- Aprendizaje cooperativo
- Aprendizaje basado en problemas
- Aprendizaje basado en enseñanzas de taller virtual
- Entornos de simulación

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 online:

Actividad formativa	Número de horas
Clases magistrales	8
Clases virtuales	26
Elaboración de informes y escritos	10
Investigaciones y proyectos	38
Actividades síncronas en talleres/ laboratorio	12
Estudio de contenidos y documentación complementaria (trabajo autónomo)	50
Foro virtual	4
Pruebas de evaluación virtuales	2
TOTAL	150 h

7. EVALUACIÓN

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

Modalidad online:

Sistema de evaluación	Peso
Pruebas de evaluación virtuales	60 %
Caso/ Problema/cuaderno prácticas laboratorio/observación desempeño	40 %

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.

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 5,0 en la prueba de conocimiento final, para que la misma pueda hacer media con el resto de las actividades.

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 5,0 en la prueba de conocimiento final, para que la misma pueda hacer media con el resto de las actividades.

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.

8. CRONOGRAMA

En este apartado se indica el cronograma aproximado de desarrollo de las unidades de aprendizaje del curso:

Unidad	Semanas
1	1, 2, 3,
2	4, 5, 6, 7
3	8, 9, 10,
4	11, 12
5	13, 14
6	15,16
Prueba de conocimiento	17

Este cronograma podrá sufrir modificaciones por razones docentes y/o logísticas, las cuales serán notificadas al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

-"Network Security Essentials: Applications and Standards" de William Stallings

-"Network+ Guide to Networks" de Jill West, Tamara Dean y Dean Andrews

-"Network Security" de Charlie Kaufman, Radia Perlman y Mike Speciner

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.