Guía Docente

Curso Académico 2025/26

Datos Generales

Asignatura: REDES III.

Titulación: GRADO EN CIBERSEGURIDAD.

Carácter: OBLIGATORIA.

Créditos ECTS: 6 ECTS.

Curso: 2º

Distribución temporal: 2º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Carlos Ochoa.

Presentación de la asignatura:

Asignatura teórica para profundizar en los conocimientos sobre redes, protocolos, capas, seguridad y sistemas de redes que permita posteriormente al alumno adquirir, entender y poner en contexto los aprendizajes ligados a la ciberseguridad.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)

Contenidos o conocimientos (C)	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C4	Ejecutar técnicas de desarrollo y penetración analizando las mejoras técnicas, soluciones y buenas prácticas.
	C12	Conocer la nube, su seguridad y sus aplicaciones.
Competencias (CO)	CO1	Usar y programar ordenadores, sistemas operativos, redes, bases de datos y el entorno de la nube para su aplicación en la ciberseguridad.
	CO4	Realizar diseños de ingeniería aplicados a la ciberseguridad.
	CO6	Utilizar de forma segura los lenguajes de programación más utilizados para su implementación en situaciones reales.
	CO8	Analizar y ejecutar test de penetración en sistemas informáticos.
Destrezas o habilidades (H)	H1	Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad

		académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

1. Protección del perímetro: Firewall y DMZ.
2. Seguridad en redes avanzadas.
3. Prevención y detección de intrusos.
4. Redes privadas virtuales: IPSEC y TLS.
5. Seguridad en redes inalámbricas.

*(*El contenido desarrollado está disponible en la Programación Docente de la asignatura publicada en el Campus Virtual de la Universidad).*

Metodologías Docentes y Actividades Formativas

Metodologías docentes utilizadas en esta asignatura son:

MD1	Método expositivo.
MD2	Estudio de casos.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	23	100
AF9: Clase en laboratorio.	17	100
AF3: Realización de trabajos (individuales y/o grupales).	11	20

AF4: Tutorías (individuales y/o grupales).	5	0
AF5: Estudio independiente y trabajo autónomo del estudiante.	85	0
AF6: Pruebas de evaluación.	9	100
Total	**150**	

Evaluación: Sistemas y Criterios de Evaluación

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. mín.	Pond. Máx
SE1 Evaluación de la asistencia y participación del estudiante.	0	5
SE2 Evaluación de trabajos.	10	30
SE3 Pruebas de evaluación y/o exámenes.	50	80

El estudiantado posee dos opciones de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con una convocatoria/año.
- En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiante acogerse a la evaluación única (examen único).
- No se permite el cambio del sistema de evaluación escogido por el estudiante a lo largo del curso.
- El estudiante que desee acogerse a la evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio del curso.
- Si el estudiante no asiste un 80% a las clases presenciales no podrá presentarse a la convocatoria ordinaria y pasará automáticamente a convocatoria extraordinaria.
- Las faltas de asistencia deben justificarse al profesor responsable de la asignatura.

- De manera excepcional, el docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del estudiante, etc. la posibilidad de permitir que el estudiante continué en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.
- El estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.
- El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.
    - 0-4,9: Suspenso (SS).
    - 5,0-6,9: Aprobado (AP).
    - 7,0-8,9: Notable (NT).
    - 9,0-10: Sobresaliente (SB).
- La mención de «Matrícula de Honor» podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».
- Será considerado no presentado (NP) el estudiante matriculado que no realice ninguna actividad evaluativa.
- Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas orto tipográficas en la calificación final.
- El plagio está prohibido tanto en los trabajos como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:
    - Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor para analizar las posibles fuentes de plagio y evaluar si están justificadas.
    - Cualquier trabajo con un índice de similitud superior al 30% no será evaluado.

Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- "Seguridad perimetral, monitorización y ataques en redes" de Antonio Ángel Ramos Varón y Carlos Alberto Barbero Muñoz.
- "Fundamentos de seguridad en redes" de William Stallings.
- "Firewalls and Internet Security: Repelling the Wily Hacker: Repelling the Wily Hacker" de William R. Cheswick.

Bibliografía Complementaria

- "Procesos y herramientas para la seguridad de redes" de Gabriel Díaz Orueta, Ignacio Alzórriz Armendáriz, Elio Sancristóbal Ruiz, Manuel Alonso Castro Gil.
- “Hacking Wireless: Seguridad de Redes Inalámbricas” de Andrew A. Vladimirov.
- “IPsec Virtual Private Network Fundamentals” de James S. Tiller.
- “IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks” de Naganand Doraswamy y Dan Harkins.
- "Applied Network Security" de Arthur Salmon, Warun Levesque, Michael McLafferty.

Otros Recursos de Aprendizaje Recomendados

- "Seguridad en redes" de Rubén Bustamante Sánchez.
- "Manual de seguridad en redes" de varios autores.