Guía Docente
Curso Académico 2026/27

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 carlos.ochoa@euneiz.com

Aula(s): Aula informatizada

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)[1]

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.

[1] La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	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
    1.1. Firewalls
        1.1.1. Tipos de firewalls (basados en red, host, estado, aplicación)
        1.1.2. Reglas y filtrado de tráfico
        1.1.3. Configuración y gestión
    1.2. DMZ (Zona Desmilitarizada)
        1.2.1. Concepto y propósito
        1.2.2. Diseño y segmentación de redes
        1.2.3. Implementación de servicios en la DMZ
2. Seguridad en redes avanzadas
    2.1. Principios de seguridad en redes
        2.1.1. Confidencialidad, integridad y disponibilidad (CIA)
        2.1.2. Control de acceso y autenticación
    2.2. Ataques en redes avanzadas
        2.2.1. Ataques de denegación de servicio (DoS/DDoS)
        2.2.2. Suplantación de identidad (spoofing)
        2.2.3. Ataques de intermediario (MITM)
    2.3. Estrategias de mitigación
        2.3.1. Endurecimiento de redes (hardening)
        2.3.2. Segmentación de redes y VLANs
        2.3.3. Auditoría y monitoreo continuo
3. Prevención y detección de intrusos
    3.1. Sistemas de prevención de intrusos (IPS)
        3.1.1. Funcionamiento y tipos
        3.1.2. Implementación en redes
    3.2. Sistemas de detección de intrusos (IDS)
        3.2.1. Monitoreo de tráfico en tiempo real

3.2.2. Firma y detección basada en comportamiento
3.3. Técnicas de análisis de tráfico
3.3.1. Captura de paquetes con herramientas como Wireshark
3.3.2. Correlación de eventos de seguridad
4. Redes privadas virtuales: IPSEC y TLS
4.1. Introducción a las VPNs
4.1.1. Tipos de VPNs (site-to-site, remote access)
4.1.2. Beneficios y desafíos
4.2. Seguridad en VPNs con IPSEC
4.2.1. Modo túnel y modo transporte
4.2.2. Protocolos AH y ESP
4.2.3. Intercambio de claves con IKE
4.3. Seguridad en VPNs con TLS
4.3.1. Uso en conexiones seguras (SSL/TLS VPN)
4.3.2. Implementación en aplicaciones web
5. Seguridad en redes inalámbricas
5.1. Protocolos de seguridad en Wi-Fi
5.1.1. WEP, WPA, WPA2 y WPA3
5.1.2. Autenticación con 802.1X
5.2. Ataques en redes inalámbricas
5.2.1. Rogue AP y Evil Twin
5.2.2. Ataques de desautenticación
5.2.3. Sniffing y ataques de fuerza bruta
5.2.4. Medidas de protección
5.3. Configuración segura de routers
5.3.1. Filtrado MAC y segmentación de red
5.3.2. Redes ocultas y SSID seguro

Metodologías Docentes y Actividades Formativas[2]

Metodologías docentes utilizadas en esta asignatura son:

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

[2] Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	23	100
AF2: Clase prácticas.	17	100
AF3: Realización de trabajos (individuales y/o grupales).	11	20
AF3: Tutorías (individuales y/o grupales).	5	0
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	85	0
AF6: Pruebas de evaluación.	9	100
Total	**150**	**--**

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

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

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

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.

- Evaluación única con 2 convocatorias/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 estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de 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 de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continue en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la 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/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas 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/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas…)
Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio de Ciberseguridad

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[3]

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

[3] Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.