



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros
Informaticos

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

103000624 - Diseño Y Seguridad De Redes

PLAN DE ESTUDIOS

10AN - Master Universitario En Ingenieria Informatica

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	2
5. Descripción de la asignatura y temario.....	3
6. Cronograma.....	6
7. Actividades y criterios de evaluación.....	8
8. Recursos didácticos.....	11

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	103000624 - Diseño y Seguridad de Redes
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	10AN - Master Universitario en Ingeniería Informática
Centro responsable de la titulación	10 - Escuela Técnica Superior De Ingenieros Informaticos
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Sonia Valentina De Frutos Cid	D-4311	sonia.frutos@upm.es	M - 12:00 - 15:00 J - 09:00 - 12:00 Solicitar sesiones de tutoría mediante correo electrónico
Miguel Jimenez Gañan (Coordinador/a)	D-4311	m.jimenez@upm.es	L - 10:00 - 13:00 M - 10:00 - 13:00 Solicitar sesiones de tutoría mediante correo electrónico

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Master Universitario en Ingeniería Informática no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Redes de Computadores, direccionamiento IPv4, routing estático, switching, VLANs y arquitectura TCP/IP

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE1 - Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.

CE4 - Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.

CE5 - Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios

CG16 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática

4.2. Resultados del aprendizaje

RA33 - Conocer los principios básicos de la seguridad de red y las principales amenazas de seguridad que afectan a las infraestructuras de red

RA34 - Conocer las herramientas y mecanismos disponibles para prevenir y detectar intrusiones y accesos no autorizados

RA35 - Diseñar e implementar soluciones de seguridad de red

RA79 - Diseñar, planificar y gestionar redes de computadores

RA80 - Comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

La cada vez mayor exposición de las redes, tanto domésticas como empresariales, a una Internet globalmente conectada impone unos requisitos de seguridad cada vez mayores. Además, la información sensible y relevante que se transporta por las redes empresariales convierte a dichas redes en un elemento imprescindible dentro de la estrategia empresarial, así como un objetivo para posibles atacantes. Es por ello que la red y su seguridad debe tenerse muy en cuenta, tanto desde su concepción y diseño, como durante su gestión y operación.

La asignatura enseña a los estudiantes los conceptos clave de la seguridad de red, y cómo llevar a cabo políticas de seguridad que permitan mitigar sus potenciales riesgos. También les aporta las habilidades necesarias para configurar, monitorizar y solucionar problemas que puedan surgir en cuanto a la red y su seguridad. Finalmente, la asignatura permite a los alumnos para la superación del examen de certificación Cisco CCNA Security.

Los objetivos concretos de la asignatura son los siguientes:

- Describir las amenazas de seguridad a las que se enfrentan las infraestructuras de red modernas
- Gestionar la seguridad de los propios dispositivos de red
- Implementar políticas de control de acceso en entornos de red
- Implementar diversas soluciones de firewall en redes empresariales
- Resolver problemas de seguridad que pueden afectar a redes de área local
- Conocer mecanismos de soluciones de detección y prevención de intrusiones

- Poner en marcha soluciones de VPN

5.2. Temario de la asignatura

1. Fundamentos de red

- 1.1. Nivel de red: direccionamiento y encaminamiento
- 1.2. Protocolos de nivel de enlace y VLAN
- 1.3. Entornos de red simulados para la gestión de dispositivos

2. Amenazas a la seguridad de la red

- 2.1. Principios fundamentales de una red segura
- 2.2. Tipos de malware
- 2.3. Tipos de ataques
- 2.4. Metodologías de ataques

3. Control de acceso a dispositivos

- 3.1. Gestión de identidades
- 3.2. Autenticación, Autorización y registro de Auditoría
- 3.3. Modelos de control de acceso
- 3.4. Sistemas centralizados

4. Redes de área local seguras

- 4.1. Seguridad de los equipos finales
- 4.2. Control de acceso a la red
- 4.3. Vulnerabilidades relacionadas con la conmutación en un switch
- 4.4. Vulnerabilidades relacionadas con VLANs
- 4.5. Vulnerabilidades relacionadas con STP
- 4.6. Vulnerabilidades relacionadas con DHCP
- 4.7. Falsificación (spoofing) de direcciones

5. Firewalls

- 5.1. Tecnologías de firewalls

- 5.2. Firewalls de filtrado de paquetes
- 5.3. Firewalls con estado
- 5.4. Nuevas tendencias
- 6. Detección y prevención de Intrusiones
 - 6.1. Detección de Intrusiones (IDS)
 - 6.2. Prevención de Intrusiones (IPS)
 - 6.3. Firmas de intrusiones
- 7. Redes Privadas Virtuales (VPNs)
 - 7.1. Tipos de VPNs
 - 7.2. Túneles GRE-IP
 - 7.3. Fundamentos de criptografía
 - 7.4. Componentes y funcionamiento de IPsec
 - 7.5. VPNs sitio a sitio
 - 7.6. VPNs de acceso remoto

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	Tema 1 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 1 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
2	Tema 2 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 1 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
3	Tema 2 Duración: 01:30 LM: Actividad del tipo Lección Magistral Tema 3 Duración: 01:30 LM: Actividad del tipo Lección Magistral			
4	Tema 3 Duración: 03:00 LM: Actividad del tipo Lección Magistral	Tema 3 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
5	Tema 4 Duración: 03:00 LM: Actividad del tipo Lección Magistral	Tema 4 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
6	Tema 4 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 4 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
7	Tema 5 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 4 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
8	Tema 5 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Temas 5 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		Ejercicio teórico-práctico (Temas 1-4) EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 01:30
9	Tema 5 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 5 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
10	Tema 6 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 5 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		

11	Tema 7 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 7 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		Ejercicio teórico-práctico (Temas 5 y 6) EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 01:30
12	Tema 7 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 7 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
13	Tema 7 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 7 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
14	Tema 7 Duración: 01:30 LM: Actividad del tipo Lección Magistral	Tema 7 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
15		Laboratorio físico Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas		Cuestionarios breves en clase con Wooclap. Semanas 1-15 [no recuperable] ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Presencial Duración: 01:00
16				
17				Ejercicio teórico-práctico (Tema 7) EP: Técnica del tipo Examen de Prácticas Evaluación continua y sólo prueba final Presencial Duración: 01:30 Recuperación ejercicio teórico-práctico (Temas 1-4) EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Presencial Duración: 01:00 Recuperación ejercicio teórico-práctico (Temas 5-6) EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final No presencial Duración: 01:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
8	Ejercicio teórico-práctico (Temas 1-4)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	30%	4 / 10	CE1 CE5 CE4 CG16
11	Ejercicio teórico-práctico (Temas 5 y 6)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	30%	4 / 10	CG16 CE1 CE4
15	Cuestionarios breves en clase con Wooclap. Semanas 1-15 [no recuperable]	ET: Técnica del tipo Prueba Telemática	Presencial	01:00	10%	/ 10	CE1 CE5 CE4 CG16
17	Ejercicio teórico-práctico (Tema 7)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	30%	4 / 10	CE1 CE5 CE4 CG16

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
15	Cuestionarios breves en clase con Wooclap. Semanas 1-15 [no recuperable]	ET: Técnica del tipo Prueba Telemática	Presencial	01:00	10%	/ 10	CE1 CE5 CE4 CG16
17	Ejercicio teórico-práctico (Tema 7)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	30%	4 / 10	CE1 CE5 CE4 CG16
17	Recuperación ejercicio teórico-práctico (Temas 1-4)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	30%	4 / 10	CE1 CE5 CE4 CG16

17	Recuperación ejercicio teórico-práctico (Temas 5-6)	EP: Técnica del tipo Examen de Prácticas	No Presencial	01:00	30%	4 / 10	CE1 CE4 CG16
----	---	--	---------------	-------	-----	--------	--------------------

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Recuperación ejercicio teórico-práctico (Temas 1-4)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	30%	4 / 10	CE5 CE4 CG16 CE1
Recuperación ejercicio teórico-práctico (Temas 5-6)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	30%	4 / 10	CE1 CE4 CG16
Recuperación ejercicio teórico-práctico (Tema 7)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:00	30%	4 / 10	CE5 CE4 CG16 CE1
Cuestionarios breves en clase con Wooclap. Semanas 1-15 [no recuperable]	ET: Técnica del tipo Prueba Telemática	Presencial	01:00	10%	/ 10	CE1 CE5 CE4 CG16

7.2. Criterios de evaluación

Sistema de evaluación progresiva

La asignatura está organizada en 7 temas. Durante el desarrollo de cada tema se realizarán en el aula informática diferentes supuestos prácticos con el simulador Packet Tracer de Cisco para obtener los conocimientos que luego permitirán evaluar las competencias adquiridas por los alumnos (aprendizaje basado en competencias).

La asignatura seguirá un proceso de evaluación progresiva, de modo que al finalizar los temas 4, 6 y 7 se realizará un ejercicio teórico-práctico con o sin simulador. El tercer examen se realizará durante la semana 17. Para superar cada tema es necesario superar cada ejercicio teórico-práctico con más de un 4 sobre 10.

Además, durante las clases se realizarán presencialmente cuestionarios breves sobre conceptos recientemente impartidos utilizando la herramienta Wooclap o similar. Estos cuestionarios computan un 10% de la nota de la

asignatura y son no recuperables, puesto que evalúan la progresión diaria de los alumnos en clase. Los alumnos que, por causa justificada, no puedan acudir a las clases, dispondrán de un mecanismo alternativo para obtener esta misma evaluación.

La nota final de la asignatura será la media ponderada de las notas de los temas 1, 2, 3 y 4 (30%), tema 5 (30%), tema 6 y 7 (30%) y de las notas de los cuestionarios de Wooclap (10%), debiendo ser mayor o igual que 5 para superar la asignatura.

Evaluación mediante prueba global

Durante la semana oficial de exámenes programada por Jefatura de Estudios (semana 17), los estudiantes realizarán el tercer ejercicio teórico-práctico y podrán recuperar los dos primeros ejercicios teórico-prácticos no superados en evaluación progresiva (nota menor que 5).

La nota final se calcula la fórmula indicada en el sistema de evaluación progresiva, aplicando el máximo entre las pruebas recuperadas y las notas obtenidas durante la evaluación progresiva. La nota de los cuestionarios de Wooclap se traslada tal y como se obtuvo, al ser prueba no recuperable.

Evaluación en periodo extraordinario

La convocatoria extraordinaria de julio consistirá en la recuperación de los ejercicios teórico-prácticos no superados.

La nota final se calcula la fórmula indicada en el sistema de evaluación progresiva, aplicando el máximo entre las pruebas recuperadas y las notas obtenidas durante la evaluación progresiva o global. La nota de los cuestionarios de Wooclap se traslada tal y como se obtuvo, al ser prueba no recuperable.

Actuación ante copias y otros comportamientos fraudulentos

Ante la comprobación de fraude académico en una prueba de evaluación, se calificará con la puntuación de cero al estudiante o estudiantes implicados en la calificación final de la convocatoria correspondiente a la celebración de la prueba (ordinaria o extraordinaria). Además, en función de la gravedad del caso, el Tribunal de la asignatura podrá acordar la realización de un examen especial y equivalente para evaluar los resultados de aprendizaje de la asignatura en la siguiente convocatoria oficial.

Indicadores de logro

La evaluación de la asignatura se registrará por los siguientes indicadores de logro:

- **I1:** Manejar de forma básica dispositivos de red mediante consolas de gestión, y realizar configuraciones de nivel de enlace y nivel de red (RA35, RA79)
- **I2:** Comprender los peligros actuales hacia una infraestructura de red y las vulnerabilidades más relevantes (RA33, RA80)
- **I3:** Asegurar el acceso a los dispositivos de red (RA35, RA79)
- **I4:** Conocer los mecanismos de control de acceso a los dispositivos (RA34)
- **I5:** Configurar mecanismos de control de acceso en dispositivos de red (RA35, RA79)
- **I6:** Prevenir los accesos no autorizados a la red mediante Firewalls (RA35, RA79)
- **I7:** Describir los mecanismos de detección y prevención de intrusiones (RA34)
- **I8:** Describir las vulnerabilidades que afectan a los dispositivos de nivel de enlace de una infraestructura de red (RA33)

- **I9:** Configurar mecanismos de seguridad a nivel de enlace para mitigar los ataques más comunes (RA35, RA79)
- **I10:** Conocer los mecanismos de acceso seguro a redes empresariales a través de redes públicas (RA33, RA80)
- **I11:** Implementar accesos remotos seguros con VPN (RA35, RA79)
- **I12:** Elegir, diseñar y configurar mecanismos de seguridad en redes empresariales a múltiples niveles (RA35, RA79)

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
CCNA Security 210-260 Official Cert Guide	Bibliografía	Omar Santos, John Stuppi. Cisco Press. 2015
Cryptography Network Security. Principles and Practice	Bibliografía	W. Stalling. 5th ed., Prentice Hall, 2011
Simuladores de red	Otros	Software de simulación de red para poner en práctica los conceptos aprendidos
Equipamiento físico de laboratorio de redes	Equipamiento	Routers y switches para la realización de prácticas con equipos reales. Este equipamiento se corresponde con kits de laboratorio oficiales CISCO CCNA Security

CCNA 200-301 Official Cert Guide, Volume 1	Bibliografía	Wendell Odom. Cisco Press. 2019
CCNA 200-301 Official Cert Guide, Volume 2	Bibliografía	Wendell Odom. Cisco Press. 2019
31 Days Before Your CCNA Security Exam: A Day-By-Day Review Guide for the IINS 210-260 Certification Exam	Bibliografía	Patrick Gargano. Cisco Press. 2016
CCNA Security 210-260 - Complete videocourse	Recursos web	by Omar Santos, Aaron Woland, and Mason Harris. https://learning.oreilly.com/videos/ccna-security-210-260/9780134400631/9780134400631-CCNA_01_00_00