

# 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

2023/24 - 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	2023-24

## 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 - 09:00 - 12:00 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 X - 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. Además de abarcar los conceptos de seguridad de redes físicas *on premise*, se contemplan conceptos, herramientas y políticas para hacerlo con elementos de red en entornos Cloud.

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
- Conocer mecanismos de soluciones de detección y prevención de intrusiones

- Poner en marcha soluciones de VPN
- Gestionar la seguridad en entornos de red en Cloud

## 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. Ciclo de vida de un ataque
- 2.5. Análisis forense
- 2.6. Herramientas de ataque, registro y pentesting

### 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. Firewalls

- 4.1. Tecnologías de firewalls
- 4.2. Firewalls de filtrado de paquetes
- 4.3. Firewalls con estado
- 4.4. Nuevas tendencias

### 5. Detección y prevención de Intrusiones

- 5.1. Detección de Intrusiones (IDS)

## 5.2. Prevención de Intrusiones (IPS)

## 5.3. Firmas de intrusiones

## 6. Redes Privadas Virtuales (VPNs)

### 6.1. Tipos de VPNs

### 6.2. Túneles GRE-IP

### 6.3. Fundamentos de criptografía

### 6.4. Componentes y funcionamiento de IPsec

### 6.5. VPNs sitio a sitio

### 6.6. VPNs de acceso remoto

## 7. Seguridad en Cloud

### 7.1. Introducción a cloud

### 7.2. Securizar el acceso a los recursos

### 7.3. Securizar la infraestructura

### 7.4. Securizar los datos

### 7.5. Securizar las aplicaciones

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

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



11	<b>Tema 6</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral	<b>Tema 6</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
12	<b>Tema 7</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral	<b>Tema 6 - Laboratorio de recopilación</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
13	<b>Tema 7</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral	<b>Tema 7</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
14	<b>Tema 7</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral	<b>Tema 7</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
15	<b>Tema 7</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral	<b>Tema 7 - Laboratorio de recopilación</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		<b>Ejercicio teórico-práctico (Temas 6-7)</b> EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 01:30  <b>Cuestionarios breves en clase con Woodlap. Semanas 1-15 [no recuperable]</b> ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Presencial Duración: 01:00
16		<b>Laboratorio físico</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas		
17				<b>Examen final (evaluación progresiva)</b> EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 02:00  <b>Examen final (evaluación global)</b> EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Presencial Duración: 02:00

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
9	Ejercicio teórico-práctico (Temas 1-5)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	25%	/ 10	CG16 CE1 CE4 CE5
15	Ejercicio teórico-práctico (Temas 6-7)	EP: Técnica del tipo Examen de Prácticas	Presencial	01:30	25%	/ 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	CG16 CE1 CE4 CE5
17	Examen final (evaluación progresiva)	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	40%	/ 10	CG16 CE1 CE4 CE5

#### 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	CG16 CE1 CE4 CE5
17	Examen final (evaluación global)	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	90%	/ 10	

#### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Cuestionarios breves en clase con Woodclap. Semanas 1-15 [no recuperable]	ET: Técnica del tipo Prueba Telemática	Presencial	01:00	10%	/ 10	CG16 CE1 CE4 CE5
Examen final (extraordinaria)	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	90%	/ 10	CG16 CE1 CE4 CE5

## 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 simuladores y herramientas 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 y 7 se realizará un ejercicio teórico-práctico con o sin simulador, sin nota mínima. Además, durante la semana oficial de exámenes programada por Jefatura de Estudios (semana 17), se realizará un examen final de la asignatura.

Además, durante las clases se realizarán presencialmente cuestionarios breves sobre conceptos recientemente impartidos utilizando la herramienta Woodclap 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 suma ponderada entre el 10% de los cuestionarios de clase, y el 90% restante que se obtiene del cálculo más favorable entre:

- media ponderada de ejercicio temas 1-4 (25%), ejercicio temas 5-7 (25%), examen final (40%) y cuestionarios (10%).
- examen final (90%) y cuestionarios (10%)

Para superar la asignatura, dicha nota deberá ser igual o superior a 5 sobre 10.

## Evaluación mediante prueba global

Durante la semana oficial de exámenes programada por Jefatura de Estudios (semana 17), los estudiantes realizarán el examen global. Este examen computa como examen global si su nota es mayor que la obtenida en el cálculo ponderado con los dos exámenes parciales. De esta forma el alumno tiene la opción de superar aquellos exámenes parciales que no hubiera superado en evaluación progresiva.

La nota final se calcula la fórmula indicada en el sistema de evaluación progresiva, aplicando el mejor resultado para el alumno. La nota de los cuestionarios de Woodlap se traslada tal y como se obtuvo, al ser prueba no recuperable.

## Evaluación en periodo extraordinario

La convocatoria extraordinaria de julio consistirá en la realización del examen final de la asignatura, que se computará con un peso del 90% junto con los cuestionarios de clase (10%).

## Actuación ante copias y otros comportamientos fraudulentos

Ante la comprobación de fraude académico durante el desarrollo de pruebas de evaluación, se aplicará lo recogido en el artículo 13 de la Normativa de Evaluación UPM aprobada en Consejo de Gobierno de 26 de mayo de 2022.

## 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 Security 210-260 - Complete videocourse	Recursos web	by Omar Santos, Aaron Woland, and Mason Harris. <a href="https://learning.oreilly.com/videos/ccna-security-210-260/9780134400631/9780134400631-CCNA_01_00_00">https://learning.oreilly.com/videos/ccna-security-210-260/9780134400631/9780134400631-CCNA_01_00_00</a>
CCSK Certificate of Cloud Security Knowledge All-in-One Exam Guide	Bibliografía	Graham Thompson. McGraw-Hill. <a href="https://learning.oreilly.com/library/view/ccsk-certificate-of/9781260460094/">https://learning.oreilly.com/library/view/ccsk-certificate-of/9781260460094/</a>
AWS Cloud Security - videocourse	Recursos web	By Michael Shannon. <a href="https://learning.oreilly.com/videos/aws-cloud-security/9780135174784/">https://learning.oreilly.com/videos/aws-cloud-security/9780135174784/</a>