



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

2019/20 - Segundo semestre

## Índice

---

### Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	3
5. Descripción de la asignatura y temario.....	4
6. Cronograma.....	7
7. Actividades y criterios de evaluación.....	9
8. Recursos didácticos.....	11

## 1. Datos descriptivos

---

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	103000624 - Diseño y Seguridad de Redes
<b>No de créditos</b>	6 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Primer curso
<b>Semestre</b>	Segundo semestre
<b>Período de impartición</b>	Febrero-Junio
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	10AN - Master Universitario En Ingeniería Informatica
<b>Centro responsable de la titulación</b>	10 - Escuela Tecnica Superior de Ingenieros Informaticos
<b>Curso académico</b>	2019-20

## 2. Profesorado

---

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías *</b>
Fco. Javier Yaguez Garcia	D-4308	javier.yaguez@upm.es	L - 14:00 - 16:00 M - 11:00 - 13:00 J - 11:00 - 13:00 Establecer sesiones de tutoría mediante correo electrónico

Sonia Valentina De Frutos Cid	D-4311	sonia.frutos@upm.es	L - 11:00 - 14:00 X - 11:00 - 14:00 Establecer sesiones de tutoría mediante correo electrónico
Miguel Jimenez Gañan (Coordinador/a)	D-4311	m.jimenez@upm.es	L - 11:00 - 14:00 X - 11:00 - 14:00 Establecer sesiones de tutoría mediante correo electrónico
Guillermo Antonio Viguera Gonzalez	D-4310	guillermo.viguera@upm.es	M - 10:00 - 13:00 J - 10:00 - 13:00 Establecer 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

## 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. 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 de área local seguras
  - 6.1. Seguridad de los equipos finales
  - 6.2. Control de acceso a la red
  - 6.3. Ataques relacionados con VLANs

6.4. Ataques relacionados con STP

6.5. Ataques relacionados con DHCP

6.6. Falsificación (spoofing) de direcciones

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 extremo a extremo

7.6. VPNs de acceso remoto



## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	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 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		
3	<b>Tema 2</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral  <b>Tema 2</b> Duración: 01:30 AC: Actividad del tipo Acciones Cooperativas			
4	<b>Tema 3</b> Duración: 03:00 LM: Actividad del tipo Lección Magistral			
5	<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		
6	<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		
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</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>Examen Temas 1-5</b> EX: Técnica del tipo Examen Escrito Evaluación continua 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 7</b> Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		<b>Examen Tema 6</b> EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:30
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>Laboratorio de Integración</b> Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas		<b>Examen Tema 7</b> EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 01:30
16				
17				<b>Examen global</b> EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00  <b>Examen global</b> EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

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.

## 7. Actividades y criterios de evaluación

### 7.1. Actividades de evaluación de la asignatura

#### 7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
9	Examen Temas 1-5	EX: Técnica del tipo Examen Escrito	Presencial	01:30	20%	0 / 10	CE1 CE5 CE4 CG16
12	Examen Tema 6	EX: Técnica del tipo Examen Escrito	Presencial	01:30	20%	0 / 10	CE5 CE4 CG16 CE1
15	Examen Tema 7	EX: Técnica del tipo Examen Escrito	Presencial	01:30	20%	0 / 10	CE1 CE5 CE4 CG16
17	Examen global	EX: Técnica del tipo Examen Escrito	Presencial	02:00	40%	0 / 10	CE1 CE5 CE4 CG16

#### 7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen global	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	5 / 10	CE5 CE4 CG16

#### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
-------------	-----------	------	----------	-----------------	-------------	------------------------

Examen global	EP: Técnica del tipo Examen de Prácticas	Presencial	02:30	100%	5 / 10	CE1 CE5 CE4 CG16
---------------	--	------------	-------	------	--------	---------------------------

## 7.2. Criterios de evaluación

### Evaluación en periodo ordinario

La nota de los alumnos mediante evaluación continua se calculará en base a la realización de tres exámenes durante el curso, y un examen final que incorpora todos los temas y se realiza en la fecha establecida por Jefatura de Estudios. Estos exámenes, que no tienen nota mínima, se computan con un peso de 20%, 20%, 20% y 40% respectivamente, debiendo ser el resultado mayor o igual a 5 para superar la asignatura. Los exámenes son teórico-prácticos, con preguntas conceptuales de respuesta corta combinadas con la implementación de contramedidas y soluciones de seguridad en los escenarios planteados.

### Evaluación mediante sólo prueba final

La evaluación mediante sólo prueba final consiste en un único examen realizado en la fecha establecida por Jefatura de Estudios, cubriendo el contenido teórico y práctico completo de la asignatura. Deberá superarse con un 5 y constituye el 100% de la nota.

### Evaluación en periodo extraordinario

Aquellos alumnos que no superen la asignatura por evaluación continua (nota superior a 5 en las pruebas de evaluación en periodo ordinario) o superen la evaluación mediante sólo prueba final, o que no se hayan presentado, podrán optar a la evaluación en periodo extraordinario. Esta evaluación consiste en un único examen realizado en la fecha establecida por Jefatura de Estudios para el periodo extraordinario, cubriendo el contenido teórico y práctico completo de la asignatura. Deberá superarse con un 5 y constituye el 100% de la nota.

### 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 (RA3)

- **I2:** Comprender los peligros actuales hacia una infraestructura de red y las vulnerabilidades más relevantes (RA1)
- **I3:** Asegurar el acceso a los dispositivos de red (RA3)
- **I4:** Conocer los mecanismos de control de acceso a los dispositivos (RA2)
- **I5:** Configurar mecanismos de control de acceso en dispositivos de red (RA3)
- **I6:** Prevenir los accesos no autorizados a la red mediante Firewalls (RA3)
- **I7:** Describir los mecanismos de detección y prevención de intrusiones (RA2)
- **I8:** Describir las vulnerabilidades que afectan a los dispositivos de nivel de enlace de una infraestructura de red (RA1)
  
- **I9:** Configurar mecanismos de seguridad a nivel de enlace para mitigar los ataques más comunes (RA3)
- **I10:** Conocer los mecanismos de acceso seguro a redes empresariales a través de redes públicas (RA1)
- **I11:** Implementar accesos remotos seguros con VPN (RA3)
- **I12:** Elegir, diseñar y configurar mecanismos de seguridad en redes empresariales a múltiples niveles (RA3)

## 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. Stallng. 5th ed., Prentice Hall, 2011 
Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide	Bibliografía	C. Packet. 2nd Ed., Cisco Press, 2012
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