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

2021/22 - Segundo semestre

Índice

Guía de Aprendizaje

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 Ingenieria Informatica
Centro responsable de la titulación	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Curso académico	2021-22

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	L - 10:00 - 13:00 X - 10:00 - 13:00 Solicitar sesiones de tutoría mediante correo electrónico
Miguel Jimenez Gañan (Coordinador/a)	D-4311	m.jimenez@upm.es	X - 10:00 - 13:00 V - 10:00 - 13:00 Solicitar sesiones de tutoría mediante correo electrónico

Victor Ramperez Martin	D-4310	v.ramperez@upm.es	M - 12:00 - 14:00 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 Ingenieria Informatica 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 asginatura 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

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial 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 2** Duración: 01:30 AC: Actividad del tipo Acciones Cooperativas			
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 3** Duración: 03:00 LM: Actividad del tipo Lección Magistral	**Tema 3** 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 4** 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 3 y 4** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Examen Temas 1-4** EX: Técnica del tipo Examen Escrito 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 5** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Tema 5** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
11	**Tema 6** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Tema 5** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		
12	**Tema 7** Duración: 01:30 LM: Actividad del tipo Lección Magistral	**Tema 7** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Examen Temas 5 y 6** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:30
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 de Integración** Duración: 03:00 AC: Actividad del tipo Acciones Cooperativas		**Examen Tema 7** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:30
16				
17				**Examen Global** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00 **Examen Global** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final No presencial Duración: 02:30

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 continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
8	Examen Temas 1-4	EX: Técnica del tipo Examen Escrito	Presencial	01:30	15%	0 / 10	CE1 CE5 CE4 CG16
12	Examen Temas 5 y 6	EX: Técnica del tipo Examen Escrito	Presencial	01:30	15%	0 / 10	CE1 CE4 CG16
15	Examen Tema 7	EX: Técnica del tipo Examen Escrito	Presencial	01:30	15%	0 / 10	CE1 CE5 CE4 CG16
17	Examen Global	EX: Técnica del tipo Examen Escrito	Presencial	02:00	55%	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	No Presencial	02:30	100%	5 / 10	CE1 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 contínua 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 15%, 15%, 15% y 55% 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 contínua (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 regirá 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

9. Adendas

- Se modifica el porcentaje de las pruebas de evaluación en evaluación continua: * se reducie el peso del examen final del 55% al 45%, * se añade un elemento evaluable nuevo, con un peso total del 10%, sin nota mínima. Este elemento evaluable consiste en consultas interactivas que se realizarán en clase, a lo largo de todo el curso, recibiendo feedback inmediato y restringidas a los asistentes. La participación no es obligatoria y las pruebas no respondidas computarían como 0 en la media de ellas. La modificación sólo afecta a la evaluación continua en convocatoria ordinaria, no modificando la evaluación en periodo extraordinario ni mediante sólo prueba final. Corrección de errores: en las condiciones para evaluación en periodo extraordinario, una de las condiciones es "... o superen la evaluación mediante sólo prueba final ...", siendo la redacción correcta "... o NO superen la evaluación mediante sólo prueba final ...".