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

2017/18 - 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 en el que se imparte	Escuela Tecnica Superior de Ingenieros Informaticos
Curso académico	2017-18

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Sonia Frutos Cid	D-4311	sonia.frutos@upm.es	L - 11:00 - 14:00 X - 11:00 - 14:00
Nicolas Benigno Barcia Vazquez	D-4309	nicolas.barcia@upm.es	M - 15:00 - 17:00 X - 14:00 - 16:00 J - 15:00 - 17:00

Fco. Javier Yaguez Garcia	D - 4308	javier.yaguez@upm.es	L - 12:00 - 14:00 M - 15:00 - 17:00 X - 12:00 - 14:00
Miguel Jimenez Gañan (Coordinador/a)	D-4311	m.jimenez@upm.es	L - 11:00 - 14:00 V - 11:00 - 14:00

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

3. Competencias y resultados de aprendizaje

3.1. Competencias que adquiere el estudiante al cursar la asignatura

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

CG14 - Capacidad de trabajar y comunicarse también en contextos internacionales

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

3.2. Resultados del aprendizaje al cursar la asignatura

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

4. Descripción de la asignatura y temario

4.1. 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 AAA en entornos de red
- Implementar diversas soluciones de firewall en redes empresariales
- Resolver problemas de seguridad que pueden afectar a redes Ethernet
- Implementar soluciones de detección y prevención de intrusiones
- Poner en marcha soluciones de VPN

4.2. Temario de la asignatura

1. Fundamentos de red
    1.1. Introducción a CISCO IOS
    1.2. Encaminamiento estático y dinámico
    1.3. Protocolos de nivel de enlace y VLAN
    1.4. Uso de Packet Tracer
2. Amenazas a la seguridad de la red
    2.1. Principios fundamentales de una red segura
    2.2. Virus, gusanos y caballos de Troya
    2.3. Metodologías de ataques
    2.4. Fundamentos de criptografía
3. Dispositivos de red seguros y AAA
    3.1. Acceso seguro a los dispositivos
    3.2. Monitorizar y gestionar dispositivos
    3.3. Autenticación, Autorización y registro de Auditoría
    3.4. Autenticación AAA local
    3.5. Autenticación AAA basada en servidor
    3.6. Autorización y registro de Auditoría AAA basada en servidor
4. Redes de área local seguras
    4.1. Seguridad de los equipos finales
    4.2. Consideraciones de seguridad del Nivel 2
    4.3. Configurar seguridad en el Nivel 2
    4.4. Seguridad de redes wireless, VoIP y de almacenamiento (SAN)
5. Tecnologías de firewall
    5.1. Listas de control de acceso (ACLs)
    5.2. Tecnologías de firewall
    5.3. Control de acceso basado en contexto (CBAC)
    5.4. Políticas de firewall basado en zonas

6. Detección y prevención de Intrusiones
   6.1. Tecnologías de prevención de intrusiones
   6.2. Firmas de intrusiones
   6.3. Implementar Sistemas de Prevención de Intrusiones (IPS)
   6.4. Verificar y monitorizar IPS
7. Redes Privadas Virtuales (VPNs)
   7.1. VPNs
   7.2. VPNs usando GRE
   7.3. Componentes y funcionamiento de VPNs IPsec
   7.4. Implementar VPNs IPsec extremo-a-extremo
   7.5. Implementar VPNs IPsec de acceso remoto
8. Dispositivos físicos de seguridad
   8.1. Introducción a Adaptive Security Appliance (ASA)
   8.2. Firewall con ASA
   8.3. VPN con ASA
9. Diseño de redes seguras
   9.1. Principios de un diseño de red seguro
   9.2. Arquitectura software
   9.3. Seguridad de las operaciones
   9.4. Comprobación de la seguridad de la red
   9.5. Planificación de continuidad y recuperación de desastres
   9.6. Ciclo de vida del desarrollo del sistema

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Tema 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
2	**Tema 2** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 2** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30
4	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
5	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 3** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 01:00
6	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
7	**Tema 5** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 5** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 4** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30
8	**Tema 5** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 5** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Entrega de Práctica 1** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Duración: 00:00
9	**Tema 6** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 6** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Examen Práctico (parte 1)** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 02:00 **Autoevaluación del Tema 5** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30
10	**Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 7** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 6** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30

11	**Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 7** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
12	**Tema 8** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 8** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 7** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 01:00
13	**Tema 8** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 8** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
14				**Autoevaluación Tema 8** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30 **Práctica de integración final** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 04:00 **Entrega de la Práctica 2** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Duración: 00:00
15	**Tema 9** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
16				**Autoevaluación Tema 9** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 00:30
17				**Examen final teórico** ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Duración: 01:30 **Examen práctico (parte 2)** EP: Técnica del tipo Examen de Prácticas Evaluación continua Duración: 02:00 **Examen práctico** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Duración: 04:00

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.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
3	Autoevaluación Tema 2	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14
5	Autoevaluación Tema 3	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	%	7 / 10	CE5 CG14 CG16 CE1 CE4
7	Autoevaluación Tema 4	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
8	Entrega de Práctica 1	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
9	Examen Práctico (parte 1)	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	20%	5 / 10	CE5 CG16 CE1 CE4
9	Autoevaluación del Tema 5	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1
10	Autoevaluación Tema 6	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
12	Autoevaluación Tema 7	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	%	7 / 10	CE5 CG14 CG16 CE1 CE4

14	Autoevaluación Tema 8	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
14	Práctica de integración final	TG: Técnica del tipo Trabajo en Grupo	Presencial	04:00	10%	/ 10	CG16 CE1 CE4
14	Entrega de la Práctica 2	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
16	Autoevaluación Tema 9	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
17	Examen final teórico	ET: Técnica del tipo Prueba Telemática	Presencial	01:30	30%	7 / 10	CE5 CG14 CE4
17	Examen práctico (parte 2)	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	20%	5 / 10	CG16 CE1 CE4

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
3	Autoevaluación Tema 2	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14
5	Autoevaluación Tema 3	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	%	7 / 10	CE5 CG14 CG16 CE1 CE4
7	Autoevaluación Tema 4	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4

8	Entrega de Práctica 1	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
9	Autoevaluación del Tema 5	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1
10	Autoevaluación Tema 6	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
12	Autoevaluación Tema 7	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	%	7 / 10	CE5 CG14 CG16 CE1 CE4
14	Autoevaluación Tema 8	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
14	Entrega de la Práctica 2	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
16	Autoevaluación Tema 9	ET: Técnica del tipo Prueba Telemática	No Presencial	00:30	%	7 / 10	CE5 CG14 CG16 CE1 CE4
17	Examen final teórico	ET: Técnica del tipo Prueba Telemática	Presencial	01:30	30%	7 / 10	CE5 CG14 CE4
17	Examen práctico	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	50%	5 / 10	CE5 CG16 CE1 CE4

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Entrega de la Práctica 1	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
Entrega de la Práctica 2	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	10%	/ 10	CE5 CG14 CG16 CE1 CE4
Examen final teórico	ET: Técnica del tipo Prueba Telemática	Presencial	01:30	30%	7 / 10	CE5 CG14 CE4
Examen práctico	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	50%	5 / 10	CE5 CG16 CE1 CE4

6.2. Criterios de evaluación

Evaluación en periodo ordinario

La nota de los alumnos se calculará en base a la realización de las 2 prácticas de forma individual, a dos exámenes prácticos, a la realización del ejercicio práctico de integración en clase, y al examen de teoría de la asignatura, con los pesos indicados en cada actividad de evaluación.

Los exámenes prácticos se realizan después de la entrega de cada práctica, y se basan en un escenario y problemática similar a los propuestos a los alumnos en cada una de las prácticas. Se evaluará la resolución de un caso práctico y una serie de cuestiones breves sobre cómo se ha llegado a dicha solución. La nota mínima de 5 corresponde a la media de ambos exámenes prácticos, siendo 4 el mínimo para computar cada parte.

El examen de teoría deberá superarse con un porcentaje superior al 70%.

Se propondrán al alumno tests de autoevaluación en cada uno de los temas, de pueda que pueda comprobar su propia evaluación en cada uno de los temas antes de realizar el examen de teoría. Se podrán realizar de forma reiterada y a distancia, tratando de promover una autoevaluación por parte del alumno. Su realización es opcional pero recomendada.

Evaluación en periodo extraordinario

La evaluación en periodo extraordinario consiste en la realización del examen de teoría en caso de no haberse superado, la reentrega opcional de las prácticas en caso de haber obtenido una nota inferior a 5 puntos, y la realización de un único examen práctico en caso de no haber obtenido una media de los exámenes prácticos superior o igual a 5. Este examen práctico computará como la suma de las dos partes del examen práctico más la práctica de integración en clase, con un total del 50% de la nota de la asignatura y deberá superarse con una nota mayor o igual a 5.

Evaluación mediante sólo prueba final

La evaluación mediante sólo prueba final se realizará con el mismo examen teórico, y un único examen práctico que deberá superarse con una nota mayor o igual a 5 y computará como la suma de las dos partes más el peso de la práctica de integración (50%).

En este mecanismo de evaluación las prácticas se deberán entregar en la fecha establecida para la evaluación en periodo ordinario.

Indicadores de logro

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

- **I1**: Manejar de forma básica los dispositivos de red con CLI 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 Autenticación, Autorización y Contabilización (RA2)
- **I5**: Configurar mecanismos de Autenticación, Autorización y Contabilización en dispositivos de red (RA3)
- **I6**: Prevenir los accesos no autorizados a la red mediante Listas de Control de Accesos y Firewalls (RA3)
- **I7**: Describir los mecanismos de detección y prevención de intrusiones (RA2)
- **I8**: Configurar mecanismos de Prevención de Intrusiones en dispositivos de red (RA3)
- **I9**: Describir las vulnerabilidades que afectan a los dispositivos de nivel de enlace de una infraestructura de red (RA1)
- **I10**: Configurar mecanismos de seguridad a nivel de enlace para mitigar los ataques má?s comunes (RA3)
- **I11**: Conocer los mecanismos de acceso seguro a redes empresariales a trave?s de redes públicas (RA1)
- **I12**: Implementar accesos remotos seguros con VPN (RA3)
- **I13**: Diseñar la seguridad de redes empresariales integrando mecanismos de seguridad a múltiples niveles (RA3)

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
CCNA Security 210-260 Official Cert Guide	Bibliografía	Omar Santos, John Stuppi. Cisco Press. 2015
Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide	Bibliografía	C. Packet. 2nd Ed., Cisco Press, 2012
Cryptography Network Security. Principles and Practice	Bibliografía	W. Stalling. 5th ed., Prentice Hall, 2011
Cisco Networking Academy	Recursos web	Matriculación en el curso oficial de Cisco CCNA Security en la academia online de CISCO
Kits de laboratorio CCNA-S	Equipamiento	2 kits de laboratorio oficiales CISCO CCNA Security
Simuladors de red	Otros	Software de simulación de red para poner en práctica los conceptos aprendidos
CCNA Security Course Booklet Version 2	Bibliografía	2015. Cisco Press