ANX-PR/CL/001-02

GUÍA DE APRENDIZAJE

ASIGNATURA

Diseño y seguridad de redes

CURSO ACADÉMICO - SEMESTRE

2015-16 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Diseño y seguridad de redes
Titulación	10AN - Master Universitario en Ingenieria Informatica
Centro responsable de la titulación	E.T.S. de Ingenieros Informaticos
Semestre/s de impartición	Segundo semestre
Módulo	Tecnologias informaticas
Materia	Diseño y gestion de sistemas distribuidos y redes
Carácter	Obligatoria
Código UPM	103000624
Nombre en inglés	Network Design And Security

Datos Generales

Créditos	6	**Curso**	1
Curso Académico	2015-16	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Master Universitario en Ingenieria Informatica no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Master Universitario en Ingenieria Informatica no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

Otros Conocimientos Previos Recomendados

El coordinador de la asignatura no ha definido otros conocimientos previos recomendados.

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

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

Resultados de 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

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Barcia Vazquez, Nicolas Benigno	D-4309	nicolas.barcia@upm.es	M - 12:00 - 14:00 X - 15:00 - 17:00 J - 15:00 - 17:00
Frutos Cid, Sonia	D-4311	sonia.frutos@upm.es	L - 11:00 - 13:00 M - 11:00 - 13:00 X - 11:00 - 13:00
Yaguez Garcia, Fco. Javier	D - 4308	javier.yaguez@upm.es	M - 12:00 - 14:00 X - 15:00 - 17:00 J - 15:00 - 17:00
Lopez Gomez, Genoveva	D-4308	genoveva.lopez@upm.es	M - 12:00 - 14:00 X - 15:00 - 17:00 J - 15:00 - 17:00
Soriano Camino, Francisco Javier	D- 4309	javier.soriano@upm.es	L - 13:00 - 14:30 X - 13:00 - 14:30 V - 10:00 - 13:00
Jimenez Gañan, Miguel **(Coordinador/a)**	D-4311	m.jimenez@upm.es	L - 11:00 - 13:00 M - 15:00 - 17:00 J - 15:00 - 17:00

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

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

Temario

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. Redes de área local seguras
   3.1. Seguridad de los equipos finales
   3.2. Consideraciones de seguridad del Nivel 2
   3.3. Configurar seguridad en el Nivel 2
   3.4. Seguridad de redes wireless, VoIP y de almacenamiento (SAN)

4. Tecnologías de firewall

   4.1. Listas de control de acceso (ACLs)

   4.2. Tecnologías de firewall

   4.3. Control de acceso basado en contexto (CBAC)

   4.4. Políticas de firewall basado en zonas

5. Dispositivos de red seguros y AAA

   5.1. Acceso seguro a los dispositivos

   5.2. Monitorizar y gestionar dispositivos

   5.3. Autenticación, Autorización y registro de Auditoría

   5.4. Autenticación AAA local

   5.5. Autenticación AAA basada en servidor

   5.6. Autorización y registro de Auditoría AAA basada en servidor

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

Cronograma

Horas totales: 70 horas y 30 minutos

Horas presenciales: 65 horas y 30 minutos (42%)

Peso total de actividades de evaluación continua: 100%

Peso total de actividades de evaluación sólo prueba final: 100%

Semana	Actividad Prensencial en Aula	Actividad Prensencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	**Tema 1** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 2	**Tema 2** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
Semana 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** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 4	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 5	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Autoevaluación Tema 3** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 6	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 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** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 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** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Actividad no presencial

Semana 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)** Duración: 02:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua Actividad presencial **Autoevaluación del Tema 5** Duración: 01:00 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 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** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 11	**Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 7** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 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** Duración: 01:00 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 13	**Tema 8** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 8** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
Semana 14				**Autoevaluación Tema 8** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial **Práctica de integración final** Duración: 04:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad presencial **Entrega de la Práctica 2** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Actividad no presencial
Semana 15	**Tema 9** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 9** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		

Semana 16				**Autoevaluación Tema 9** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 17				**Examen final teórico** Duración: 01:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad presencial **Examen práctico (parte 2)** Duración: 02:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua Actividad presencial **Examen práctico** Duración: 04:00 EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Actividad presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
3	Autoevaluación Tema 2	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14
5	Autoevaluación Tema 3	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CE4, CE5, CG14, CG16
7	Autoevaluación Tema 4	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
8	Entrega de Práctica 1	00:00	Evaluación continua y sólo prueba final	TI: Técnica del tipo Trabajo Individual	No	10%		CE5, CG14, CG16, CE1, CE4
9	Examen Práctico (parte 1)	02:00	Evaluación continua	EP: Técnica del tipo Examen de Prácticas	Sí	20%	5 / 10	CE1, CE4, CE5, CG16
9	Autoevaluación del Tema 5	01:00	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CG14, CG16, CE5
10	Autoevaluación Tema 6	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CE4, CE5, CG14, CG16
12	Autoevaluación Tema 7	01:00	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CE4, CE5, CG14, CG16
14	Autoevaluación Tema 8	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CE4, CE5, CG14, CG16
14	Práctica de integración final	04:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	Sí	10%		CE1, CE4, CG16
14	Entrega de la Práctica 2	00:00	Evaluación continua y sólo prueba final	TI: Técnica del tipo Trabajo Individual	No	10%		CE1, CG16, CE4, CG14, CE5
16	Autoevaluación Tema 9	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE1, CE4, CE5, CG14, CG16
17	Examen final teórico	01:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	Sí	30%	7 / 10	CE4, CE5, CG14
17	Examen práctico (parte 2)	02:00	Evaluación continua	EP: Técnica del tipo Examen de Prácticas	Sí	20%	5 / 10	CE1, CE4, CG16
17	Examen práctico	04:00	Evaluación sólo prueba final	EP: Técnica del tipo Examen de Prácticas	Sí	50%	5 / 10	CE5, CG16, CE1, CE4

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)

Recursos Didácticos

Descripción	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