ANX-PR/CL/001-02
GUÍA DE APRENDIZAJE

ASIGNATURA

Diseño y seguridad de redes

CURSO ACADÉMICO - SEMESTRE

2014-15 - Segundo semestre

FECHA DE PUBLICACIÓN

Diciembre - 2014

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
Carácter	Obligatoria
Código UPM	103000624

Datos Generales

Créditos	6	**Curso**	1
Curso Académico	2014-15	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Superadas

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 - Conocimiento y comprensión de la informática necesaria para la creación de modelos de información, y de los sistemas y procesos complejos (EURO-INF)

CG16 - Capacidad de trabajar de forma independiente en su campo profesional (EURO-INF)

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
Fernandez Gallego, Rafael	D - 4310	r.fernandez@upm.es	L - 13:00 - 14:30 X - 13:00 - 14:30 V - 10:00 - 13:00
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 - 13:00 - 17:00
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
Fernandez Del Val, Carlos	D-4310	carlos.fernandez.delval@upm.es	M - 12:00 - 14:00 X - 12:00 - 14:00 J - 12:00 - 14:00
Soriano Camino, Francisco Javier	D- 4309	javier.soriano@upm.es	L - 13:00 - 14:30 X - 13:00 - 14:30
Jimenez Ga?an, 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 tutorias 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. 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. 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. Detección y prevención de Intrusiones

   5.1. Tecnologías de prevención de intrusiones

   5.2. Firmas de intrusiones

   5.3. Implementar Sistemas de Prevención de Intrusiones (IPS)

   5.4. Verificar y monitorizar IPS

6. Redes de área local seguras

   6.1. Seguridad de los equipos finales

   6.2. Consideraciones de seguridad del Nivel 2

   6.3. Configurar seguridad en el Nivel 2

   6.4. Seguridad de redes wireless, VoIP y de almacenamiento (SAN)

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. Diseño de redes seguras

   8.1. Principios de un diseño de red seguro

   8.2. Arquitectura software

   8.3. Seguridad de las operaciones

   8.4. Comprobación de la seguridad de la red

   8.5. Planificación de continuidad y recuperación de desastres

   8.6. Ciclo de vida del desarrollo del sistema

9. Dispositivos físicos de seguridad

   9.1. Introducción a Adaptive Security Appliance (ASA)

   9.2. Firewall con ASA

   9.3. VPN con ASA

Cronograma

Horas totales: 73 horas

Horas presenciales: 68 horas (43.6%)

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: 01:00 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: 01:00 LM: Actividad del tipo Lección Magistral	**Presentación de la Práctica 1** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 5** Duración: 01:00 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: 01:00 LM: Actividad del tipo Lección Magistral **Tema 6** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Tema 5** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 6** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 5** Duración: 00:30 ET: Técnica del tipo Prueba Telemática 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		**Evaluación sobre práctica 1** Duración: 02:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua y sólo prueba final Actividad 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		**Autoevaluación Tema 7** Duración: 01:00 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 12	**Tema 8** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Presentación de la Práctica 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 8** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		
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		**Evaluación sobre la Práctica 2** Duración: 02:00 EP: Técnica del tipo Examen de Prácticas Evaluación continua y sólo prueba final Actividad presencial
Semana 14	**Tema 9** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 9** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Autoevaluación Tema 8** Duración: 00:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad no presencial
Semana 15				**Autoevaluación Tema 9** 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 y sólo prueba final Actividad presencial
Semana 16				

Semana 17				**Examen final teórico** Duración: 01:30 ET: Técnica del tipo Prueba Telemática Evaluación continua y sólo prueba final Actividad presencial **Examen final práctico** Duración: 02:30 TI: Técnica del tipo Trabajo Individual Evaluación continua y 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	01:00	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1
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	Autoevaluación Tema 5	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
9	Evaluación sobre práctica 1	02:00	Evaluación continua y sólo prueba final	EP: Técnica del tipo Examen de Prácticas	Sí	20%		CG16, CE1
10	Autoevaluación Tema 6	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
11	Autoevaluación Tema 7	01:00	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
13	Evaluación sobre la Práctica 2	02:00	Evaluación continua y sólo prueba final	EP: Técnica del tipo Examen de Prácticas	Sí	20%		CE5, CG14, CG16
14	Autoevaluación Tema 8	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
15	Autoevaluación Tema 9	00:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	No		7 / 10	CE5, CG14, CG16, CE1, CE4
15	Práctica de integración final	04:00	Evaluación continua y sólo prueba final	TG: Técnica del tipo Trabajo en Grupo	Sí	15%		CG16, CE1, CE4
17	Examen final teórico	01:30	Evaluación continua y sólo prueba final	ET: Técnica del tipo Prueba Telemática	Sí	30%	7 / 10	CE5, CG14, CE4
17	Examen final práctico	02:30	Evaluación continua y sólo prueba final	TI: Técnica del tipo Trabajo Individual	Sí	15%	5 / 10	CG16, CE1, CE4

Criterios de Evaluación

La nota de los alumnos se calculará en base a la realización de las 2 prácticas con sus exámenes de forma individual, 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 de prácticas son una prueba presencial de configuración de un escenario similar al que se proponga 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.

Es necesario superar el examen final práctico y el examen final de teoría para aprobar la asignatura. 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.

Recursos Didácticos

Descripción	Tipo	Observaciones
CCNA Security 640-554 Official Cert Guide	Bibliografía	K. Baker, S. Morris. Cisco Press. 2012
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