Datos Descriptivos

ASIGNATURA:	Diseño y Seguridad de Redes
MATERIA:	Sistemas y servicios distribuidos
CRÉDITOS EUROPEOS:	6 ECTS
CARÁCTER:	Obligatoria
TITULACIÓN:	Máster Universitario en Ingeniería Informática
CURSO/SEMESTRE	Segundo semestre
ESPECIALIDAD:	

CURSO ACADÉMICO	**2013-2014**		
PERIODO IMPARTICION	**Septiembre- Enero**	**Febrero - Junio**	
		X	
IDIOMA IMPARTICIÓN	**Sólo castellano**	**Sólo inglés**	**Ambos**
	X		

DEPARTAMENTO:	LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DEL SOFTWARE

PROFESORADO		
NOMBRE Y APELLIDO (C = Coordinador)	**DESPACHO**	**Correo electrónico**
Miguel Jiménez Gañán (C)	4311	mjimenez@fi.upm.es
Nicolás Barcia Vázquez	4309	nicolas@fi.upm.es
Rafael Fernández Gallego	4310	rfernandez@fi.upm.es
Carlos Fernández del Val	4310	cfernandez@fi.upm.es
Sonia de Frutos Cid	4311	sfrutos@fi.upm.es
Genoveva López Gómez	4308	glopez@fi.upm.es
Fco. Javier Soriano Camino	4309	jsoriano@fi.upm.es
Javier Yagüez García	4308	jyaguez@fi.upm.es

CONOCIMIENTOS PREVIOS REQUERIDOS PARA PODER SEGUIR CON NORMALIDAD LA ASIGNATURA	
ASIGNATURAS SUPERADAS	
OTROS RESULTADOS DE APRENDIZAJE NECESARIOS	

Objetivos de Aprendizaje

COMPETENCIAS Y NIVEL ASIGNADAS A LA ASIGNATURA		
Código	**COMPETENCIA**	**NIVEL**
CG14	Conocimiento y comprensión de la informática necesaria para la creación de modelos de información, y de los sistemas y procesos complejos (EURO-INF)	Comprensión
CG16	Capacidad de trabajar de forma independiente en su campo profesional (EURO-INF)	Comprensión
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	Aplicación
CE4	Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos	Aplicación
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	Aplicación

Código	**RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA**
RA1. -	Conocer los principios básicos de la seguridad de red y las principales amenazas de seguridad que afectan a las infraestructuras de red
RA2. -	Conocer las herramientas y mecanismos disponibles para prevenir y detectar intrusiones y accesos no autorizados
RA3. -	Diseñar e implementar soluciones de seguridad de red

Contenidos y Actividades de Aprendizaje

CONTENIDOS ESPECÍFICOS (TEMARIO)		
TEMA / CAPITULO	**APARTADO**	**Indicadores Relacionados**
Tema 0: Fundamentos de red	Introducción a CISCO IOS	T1
	Encaminamiento estático y dinámico	T1
	Protocolos de nivel de enlace y VLANs	T1
	Uso de Packet Tracer	T1
Tema 1: Amenazas a la seguridad de la red	Principios fundamentales de una red segura	T2
	Virus, gusanos y caballos de Troya	T2
	Metodologías de ataques	T2
	Fundamentos de criptografía	T2
Tema 2: Dispositivos de red seguros	Acceso seguro a los dispositivos	T3
	Asignación de roles administrativos	T3
	Monitorizar y gestionar dispositivos	T3
	Características automatizadas de seguridad	T3
	Práctica de laboratorio	T3
Tema 3 Autenticación, Autorización Registro de Auditoría (AAA)	Propósito de AAA	T4
	Autenticación AAA local	T4
	AAA basado en servidores	T4
	Autenticación AAA basada en servidor	T4
	Autorización y registro de Auditoría AAA basada en servidor	T4
	Práctica de laboratorio	T5
Tema 4: Implementar Tecnologías de Firewall	Listas de control de acceso (ACLs)	T6
	Tecnologías de firewall	T6
	Control de acceso basado en contexto (CBAC)	T6
	Políticas de firewall basadas en zonas	T6
	Configuración de firewalls ASA	T6
	Práctica de laboratorio	T6
Tema 5: Implementar prevención de intrusiones	Tecnologías de prevención de intrusiones	T7
	Firmas de intrusiones	T7
	Implementar Sistemas de Prevención de Intrusiones (IPS)	T8
	Verificar y monitorizar IPS	T8
	Práctica de laboratorio	T8

Tema 6: Redes de Área Local Seguras	Seguridad de los equipos finales	T9
	Consideraciones de seguridad del Nivel 2	T9
	Configurar seguridad en el Nivel 2	T10
	Seguridad de redes Wireless, VoIP y de almacenamiento (SAN)	T10
	Práctica de laboratorio	T10
Tema 7: Implementación de Redes Privadas Virtuales (VPN)	VPNs	T11
	VPNs usando GRE	T11
	Componentes y funcionamiento de VPNs IPsec	T11
	Implementar VPNs IPsec extremo-a-extremo	T12
	Implementar VPNs IPsec de acceso remoto	T12
	Configuración de VPNs con ASA	T12
	Práctica de laboratorio	T12
Tema 8: Diseño de redes seguras	Principios de un diseño de red seguro	T13
	Arquitectura software	T13
	Seguridad de las operaciones	T13
	Comprobación de la seguridad de la red	T13
	Planificación de continuidad y recuperación de desastres	T13
	Ciclo de vida de desarrollo del sistema	T13
	CASO DE ESTUDIO: Desarrollo de una política de seguridad completa	T13

BREVE DESCRIPCIÓN DE LAS MODALIDADES ORGANIZATIVAS UTILIZADAS Y METODOS DE ENSEÑANZA EMPLEADOS	
CLASES DE TEORIA	Las clases constarán de una parte teórica, en la que el profesor presenta los conceptos principales de la asignatura. En estas clases también se realizan ejercicios prácticos.
CLASES PRÁCTICAS	Las clases se complementan con ejercicios prácticos realizados en laboratorio bajo la supervisión del profesor para ayudar a su comprensión y reforzar los conocimientos aprendidos en las clases de teoría
PRACTICAS	El alumno realizará, de forma autónoma, prácticas propuestas a lo largo del curso, que abarcan los contenidos prácticos de varios temas, para resolverlas de forma integrada
TRABAJOS AUTONOMOS	El alumno realizará ejercicios prácticos propuestos en cada tema. Además, el alumno podrá de forma opcional realizar tests teóricos de evaluación en cada tema, que le permitan comprobar el grado de asimilación de los contenidos teóricos.
TUTORÍAS	Se utiliza este método para resolver dudas puntuales a un alumno de forma personalizada

RECURSOS DIDÁCTICOS	
BIBLIOGRAFÍA	K. Baker, S. Morris: "CCNA Security 640-554 Official Cert Guide", Cisco Press, 2012.
	C. Paquet: "Implementin Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide". 2nd Ed. Cisco Press, 2012.
	W. Stalling: "Cryptography Network Security. Principles and Practice". 5th Ed. Prentice Hall, 2011.
RECURSOS WEB	Cisco Networking Academy (http://www.netacad.com)
EQUIPAMIENTO	Aula informática
	Equipamiento y simuladores de red CISCO
	Laboratorio de red CISCO

Cronograma de trabajo de la asignatura

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación	Otros
Semana 1 3-7 Feb	Tema 0 (4 horas)	Tema 0 (2 horas)	Estudio autónomo (5 horas)			
Semana 2 10-14 Feb	Tema 1 (4 horas)		Estudio autónomo (5 horas)			
Semana 3 17-21 Feb	Tema 2 (2 horas)	Tema 2 (2 horas)	Estudio autónomo (4 horas)		Test Tema 2 (1 hora)	
Semana 4 24-28 Feb	Tema 3 (3 horas)	Tema 3 (1 horas)	Estudio autónomo (5 horas)			
Semana 5 4-7 Mar		Tema 3 (2 horas)	Estudio autónomo (6 horas)		Test Tema 3 (1 hora)	
Semana 6 10-14 Mar	Tema 4 (2 horas)	Tema 4 (2 horas)	Estudio autónomo (5 horas)			
Semana 7 24-28 Mar	Tema 4 (2 horas)	Tema 4 (2 horas)	Estudio autónomo (4 horas)		Test Tema 4 (1 hora)	

Semana	Actividades Aula	Laboratorio	Trabajo Individual	Trabajo en Grupo	Actividades Evaluación	Otros
Semana 8 31 Mar-4 Abr	Tema 5 (2 horas)	Tema 5 (2 horas)	Estudio autónomo (3 horas)		Test Tema 5 (1 hora)	Práctica 1 (2 horas)
Semana 9 3-7 Abr	Tema 6 (3 horas)	Tema 6 (1 horas)	Estudio autónomo (3 horas)			Práctica 1 (3 horas)
Semana 10 3-7 Feb		Tema 6 (2 horas)	Estudio autónomo (6 horas)		Test Tema 6 (1 hora)	
Semana 11 3-7 Feb	Tema 7 (2 horas)		Estudio autónomo (6 horas)			
Semana 12 3-7 Feb	Tema 7 (2 horas)	Tema 7 (2 horas)	Estudio autónomo (4 horas)			
Semana 13 3-7 Feb		Tema 7 (2 horas)	Estudio autónomo (4 horas)		Test Tema 7 (1 hora)	Práctica 2 (3 horas)
Semana 14 3-7 Feb	Tema 8 (2 horas)	Tema 8 (2 horas)	Estudio autónomo (4 horas)			Práctica 2 (2 horas)
Semana 15 3-7 Feb	Tema 8 (2 horas)	Tema 8 (2 horas)	Estudio autónomo (4 horas)		Examen final (3,5 horas)	

Sistema de evaluación de la asignatura

EVALUACION		
Ref	**INDICADOR DE LOGRO**	**Relacionado con RA:**
T1	Manejar de forma básica los dispositivos de red con CLI y realizar configuraciones de nivel de enlace y nivel de red	RA3
T2	Comprender los peligros actuales hacia una infraestructura de red y las vulnerabilidades más relevantes	RA1
T3	Asegurar el acceso a los dispositivos de red	RA3
T4	Conocer los mecanismos de Autenticación, Autorización y Contabilización	RA2
T5	Configurar mecanismos de Autenticación, Autorización y Contabilización en dispositivos de red	RA3
T6	Prevenir los accesos no autorizados a la red mediante Listas de Control de Accesos y Firewalls	RA3
T7	Describir los mecanismos de detección y prevención de intrusiones	RA2
T8	Configurar mecanismos de Prevención de Intrusiones en dispositivos de red	RA3
T9	Describir las vulnerabilidades que afectan a los dispositivos de nivel de enlace de una infraestructura de red	RA1
T10	Configurar mecanismos de seguridad a nivel de enlace	RA3
T11	Conocer los mecanismos de acceso seguro a redes empresariales a través de redes públicas	RA1
T12	Implementar accesos remotos seguros	RA3
T13	Diseñar la seguridad de redes empresariales integrando mecanismos de seguridad a múltiples niveles	RA3

La tabla anterior puede ser sustituida por la tabla de rúbricas.

EVALUACION SUMATIVA			
BREVE DESCRIPCION DE LAS ACTIVIDADES EVALUABLES	**MOMENTO**	**LUGAR**	**PESO EN LA CALIFICACIÓN**
Práctica 1 Temas 3-4	Semanas 8- 9		15%
Práctica 2 Temas 6-7	Semanas 13-14		15%
Práctica de integración final	Semanas 14-15	Aula de examen	30%
Examen final		Aula de examen	40%

CRITERIOS DE CALIFICACIÓN

La nota de los alumnos se calculará en base a la resolución de las dos prácticas 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 la tabla de evaluación sumativa.

Es necesario superar el ejercicio práctico y el examen de teoría para aprobar la asignatura. El examen de teoría deberá superarse con un porcentaje superior al 70%.

De forma adicional, se valorará la realización de los tests opcionales a la finalización de los temas 2, 3, 4, 5, 6 y 7, computándose hasta un punto extra sobre la nota obtenida según la tabla de evaluación sumativa (un punto sobre 10).