UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE
CURSO 2016-2017

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre	Seguridad en Redes y Servicios
Código	ASI33
Titulación	Grado en Ingeniería Telemática
Curso	4º
Cuatrimestre	1º
Créditos ECTS	6 ECTS
Carácter	Obligatorio
Departamento	Telemática y Computación
Área	Ingeniería Telemática
Universidad	Universidad Pontificia Comillas
Horario	
Profesores	Francisco Javier Santos Ortega
Descriptor	

Datos del profesorado	
Profesor	
Nombre	Francisco Javier Santos Ortega
Departamento	Telemática y Computación
Área	Ingeniería Telemática
Despacho	Sala de profesores
e-mail	javiersantos@kpmg.es
Horario de Tutorías	Consultar con profesor

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura
Aportación al perfil profesional de la titulación
El objetivo de la asignatura es dotar de los conocimientos profesionales necesarios en la seguridad, tanto desde el punto de vista de la informaci6n (encriptación, cifrado, firma digital), como de la red (protocolos seguros, redes privadas, ..) Asimismo, la asignatura abarca conceptos que van desde lo más específico hasta lo más general (como la auditoria de seguridad).
Prerrequisitos
Tecnologías de Redes. Arquitecturas de Redes

Competencias - Objetivos	
Competencias Genéricas del título-curso	
CGT3	Conocimiento de materias básicas y tecnologías, que le capacite para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.
CGT4	Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad y de comunicar y transmitir conocimientos y habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del ingeniero técnico de telecomunicación.
CGT5	Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos en su ámbito específico de la telecomunicación.
CGT6	Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
CGT9	Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.
Competencias de Tecnología específica de telemática	
CETM2	Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gesti6n, senalizaci6n y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.

Resultados de Aprendizaje
Conocer las técnicas criptográficas más adecuadas en la transmisión RA1. Conocimiento sobre las diferencias entre criptografía simétrica y asimétrica. Ejemplos de algoritmos, robustez, rendimiento, y técnicas básicas de criptoanálisis. RA2. Conocimiento sobre el uso práctico de los certificados digitales, cadena de certificación, firma electrónica y funciones HASH, **Ser capaces de utilizar e implantar herramientas de supervisión y control de acceso en redes de datos.** RA3. Estar familiarizado con herramientas de análisis y captura de tráfico de red. RA4. Conocer herramientas de verificación de seguridad de cortafuegos, monitorización de la red, y detección de intrusiones. **Conocer los protocolos seguros utilizados en las redes de datos así como su idoneidad en la arquitectura global de una organización.** RA5. Conocimientos sobre el funcionamiento de protocolos http/https, ssh. RA6. Conocimientos sobre los fundamentos y casos prácticos de implementación de redes privadas virtuales VPN, túneles IPsec y acceso remoto. RA7. Saber segmentar una red, siendo capaz de analizar ventajas desde el punto de vista de rendimiento, de gestión y control del tráfico, y de la seguridad. **Conocer los estándares de gestión de la seguridad y poseer la capacidad de implantar una política de seguridad acorde a dichos estándares.** RA8. Conocer métricas de seguridad, mecanismos de gestión de la seguridad, técnicas de auditoría. RA9. Conocer la normativa y legislación relativa a la seguridad de los sistemas de información y de las comunicaciones.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

1. **INTRODUCCION A LA SEGURIDAD (6H)**
   - INTRODUCCION Y CONCEPTOS BASICOS. (4H TEORIA)
   - ANALISIS DE RIESGOS. (2H TEORIA)
2. **CRIPTOGRAFiA (14H)**
   - CRIPTOGRAFiA SIMETRICA Y CLAVE PUBLICA (4H TEORIA + 2H PRACTICAS)
   - CIFRADO IRREVERSIBLE, FUNCIONES DE RESUMEN Y ALEATORIEDAD (2H TEORIA + 2H PRACTICAS)
   - ALGORITMOS DE FIRMA DIGITAL (2H TEORIA + 2H PRACTICAS)
3. **ARQUITECTURA SEGURA DE REDES (16H)**
   - SEGREGACION DE TRAFICO. REDES PRIVADAS VIRTUALES. (2H TEORIA+2H PRACTICAS)
   - TUNELES Y CORTAFUEGOS. PROTOCOLOS SEGUROS. ACCESO REMOTO(2H TEORIA+4H PRACTICAS)
   - INFRAESTRUCTURAS DE CLAVE PUBLICA (PKI) (2H TEORIA)
   - VIRUS Y SISTEMAS ANTIVIRUS. (2H TEORIA)
4. **GESTION DE LA SEGURIDAD (16H)**
   - MONITORIZACION, SISTEMAS IDS, IPS Y DETECCION DE ANOMALiAS. (4H TEORIA + 2H PRACTICAS)
   - ESTANDARES DE GESTION DE LA SEGURIDAD. (2H TEORIA + 2H PRACTICAS)
   - CUADRO DE MANDO DE LA SEGURIDAD, METRICAS. (2H TEORIA + 2H PRACTICAS)
5. **CUMPLIMIENTO (SECURITY COMPLIANCE) (6H)**
   - NORMATIVAS DE SEGURIDAD, REGULACION, SOX, LOPD, LSSI. (2H DE TEORIA)
   - AUDITORiA Y CONTROL (2H TEORIA+2H PRACTICAS)

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Con el fin de conseguir el desarrollo de competencias propuesto, la materia se desarrollara promoviendo la participaci6n activa del alumno en las actividades de æaprendizaje tanto en las sesiones presenciales como en las no presenciales.

Metodología Presencial: Actividades

- **Lección expositiva**: El profesor desarrolla el temario explicando mediante la proyección de transparencias y el uso de la pizarra. Una vez desarrollados los conceptos teóricos, se exponen ejemplos de aplicación con la resolución de ejercicios.
- **Debates grupales, pruebas y resolución de ejercicios**: En estas sesiones se resolverán las dudas surgidas de las lecturas y actividades llevadas a cabo por los alumnos de los temas o contenidos propuestos por el profesor. También se realizarán pruebas de 15 minutos cada dos temas para facilitar el aprendizaje y realizar evaluación continua, Además, se resolverán los ejercicios propuestos por el profesor.
- **Prácticas de laboratorio**: La asignatura comprende la realización de 10

sesiones de 2 horas en el laboratorio de comunicaciones. Las prácticas a desarrollar requieren la preparación previa de las mismas mediante la lectura del enunciado y de la documentación elaborada por el profesor. Adicionalmente, se deberán determinar los procedimientos a realizar en el laboratorio para la realización de la práctica.

- **Tutorías**: Se realizarán tutorías en grupo e individualmente para resolver las dudas de los alumnos sobre la materia impartida y para orientar al alumno en su proceso de aprendizaje.

Metodología no presencial: Actividades

1 Estudio de los contenidos expuestos por el profesor
2 Realización de los ejercicios propuestos por el profesor
3 Preparación de las prácticas del laboratorio de comunicaciones. Elaboración del documento de prácticas del laboratorio de comunicaciones, que inl`cluyen los procedimientos, informes, resultados comentarios de cada una de las prácticas realizadas.

RESUMEN HORAS DE TRABAJO DEL ALUMNO					
HORAS PRESENCIALES					
Lección magistral		Debate y ejercicios	Prácticas laboratorio		Exámenes y pruebas
24		6	20		8
HORAS NO PRESENCIALES					
Lectura y estudio de sesiones de teoría	Prácticas de la asignatura	Resolución de problemas	Preparación de prácticas	Realización documento de prácticas	Preparación de exámenes
22	18	8	15	15	14
				CRÉDITOS ECTS:	6 (150 horas)

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	PESO
Examen Final de Teoría	– Comprensión de conceptos. – Aplicación de conceptos para la resolución de problemas. – Análisis e interpretación de los resultados obtenidos en la resolución de problemas	50%

Práctica Final de Laboratorio	– Comprensión de conceptos. – Aplicación de conceptos al diseño y gestión de redes	20%
Realización de pruebas intermedias de seguimiento y ejercicios	– Comprensión de conceptos. – Aplicación de conceptos para la resolución de problemas. – Análisis e interpretación de los resultados obtenidos en la resolución de problemas	15%
Documento de prácticas del Laboratorio de Comunicaciones	– Comprensión de conceptos. – Aplicación de conceptos para la resolución de problemas. – Carácter técnico y exactitud de la documentación entregada	15%

Calificaciones

La calificaci6n en la convocatoria ordinaria de la asignatura se obtendrá como:

- La nota del examen final de teoría supondrá un 50% de la calificaci6n final en la asignatura.
- Un 20% de la calificaci6n será la de una práctica final de la asignatura.
- Un 15% sera la calificaci6n de las pruebas intermedias de seguimiento.
- Un 15% sera la calificaci6n del documento de prácticas del laboratorio.

La calificación en la convocatoria extraordinaria:

- La nota del examen final de teoría supondrá un 50% de la calificaci6n de esta convocatoria extraordinaria y un 20% de la calificaci6n sera la practica final en la convocatoria extraordinaria. En caso de haberse aprobado alguna de los dos partes mencionadas en la convocatoria ordinaria, la nota obtenida puede guardarse para la convocatoria extraordinaria.
- Un 15% sera la calificaci6n de las pruebas de seguimiento.
- Un 15% sera la calificaci6n del documento de prácticas del laboratorio.

Para aprobar la asignatura los alumnos tienen que tener al menos 5 puntos sobre 10 en el examen final de teoría y en la práctica final de laboratorio, tanto en la convocatoria ordinaria como en la extraordinaria.

PLAN DE TRABAJO Y CRONOGRAMA

Actividades No presenciales	Fecha de realización	Fecha de entrega
Lectura y estudio de los contendidos teóricos en los apuntes de la asignatura	Después de cada clase	
Ejercicios	Después de la clase en la que son propuestos	Siguiente día de clase de teoría
Preparación de las practicas de laboratorio	Dos días antes de cada practica	
Entregas parciales del documento de practicas	Después de cada practica	Semana posterior a la realización de la practica
Preparación de Examen Final de Teoría	Diciembre	
Practica final de la asignatura	Octubre/Noviembre/Diciembre	

BIBLIOGRAFÍA Y RECURSOS

Bibliografía básica
• Fundamentos de seguridad en redes: aplicaciones y estandares. William Stalings. Pearson Prentice Hall. ISBN: 84-205-4002-1
Bibliografía complementaria
• Criptored. www.criptored.upm.es • Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. CRC Press. ISBN: 0-8493-8523-7 • Criptografía y Seguridad en Computadores. J. Manuel Lucena.