Escuela Técnica Superior de
Ingeniería de Telecomunicación

UPCT

GUÍA DOCENTE DE LA ASIGNATURA:

SEGURIDAD EN REDES

(NETWORK SECURITY)

Titulación/es: Grado en Ingeniería Telemática

1. Datos de la asignatura

Nombre	SEGURIDAD EN REDES				
Materia*	SEGURIDAD EN REDES				
Módulo*	TECNOLOGÍA ESPECÍFICA: TELEMÁTICA				
Código	505104001/505108008				
Titulación	GRADO EN INGENIERÍA TELEMÁTICA				
Plan de estudios	2010				
Centro	Escuela Técnica Superior de Ingeniería de Telecomunicación				
Tipo	TET (Tecnología Específica: Telemática)				
Periodo lectivo		**Cuatrimestre**	1º	**Curso**	4º
Idioma	Español				
ECTS	6	**Horas / ECTS**	30	**Carga total de trabajo (horas)**	180

*** Todos los términos marcados con un asterisco están definidos en *Referencias para la actividad docente en la UPCT y Glosario de términos:***

http://repositorio.bib.upct.es/dspace/bitstream/10317/3330/1/isbn8469531360.pdf

2. Datos del profesorado

Profesor responsable	MARÍA DOLORES CANO BAÑOS		
Departamento	TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES		
Área de conocimiento	INGENIERÍA TELEMÁTICA		
Ubicación del despacho	Despacho 17, 1ª Planta ETSI Telecomunicación		
Teléfono	968 32 5953	**Fax**	968 32 5973
Correo electrónico	mdolores.cano@upct.es		
URL / WEB			
Horario de atención / Tutorías	Martes de 9:15 a 12:15 Miércoles de 9:15 a 12:15		
Ubicación durante las tutorías	Despacho 17, 1ª Planta ETSI Telecomunicación		

Titulación	Doctora en Ingeniería de Telecomunicación por la Universidad Politécnica de Cartagena
Vinculación con la UPCT	Profesora Titular de Universidad
Año de ingreso en la UPCT	2000
Nº de quinquenios (si procede)	3
Líneas de investigación (si procede)	Grupo de investigación Ingeniería Telemática. Provisión de QoS/QoE (Quality of Service/ Quality of user Experience) en redes de comunicación Provisión de Seguridad en redes de comunicaciones Innovación en educación
Nº de sexenios (si procede)	2
Experiencia profesional (si procede)	Participación en contratos de investigación con empresas del sector TIC
Otros temas de interés	Fulbright Posdoctoral en Columbia University, EEUU

Profesor	JOSEMARÍA MALGOSA SANAHUJA		
Departamento	TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES		
Área de conocimiento	INGENIERÍA TELEMÁTICA		
Ubicación del despacho	Despacho 39, 2ª Planta ETSI Telecomunicación		
Teléfono	968 32 5370	**Fax**	968 32 5973
Correo electrónico	josem.malgosa@upct.es		
URL / WEB	http://ait.upct.es		
Horario de atención / Tutorías	Martes de 9h a 12h y jueves de 16h a 19h. Otros horarios bajo petición de los alumnos		
Ubicación durante las tutorías	Despacho 39, 2ª Planta ETSI Telecomunicación		

Titulación	Doctor en Ingeniería de Telecomunicación por la Universidad de Zaragoza
Vinculación con la UPCT	Profesor Titular de Universidad
Año de ingreso en la UPCT	1999
Nº de quinquenios (si procede)	5
Líneas de investigación (si procede)	Grupo de Investigación de Ingeniería Telemática de la UPCT. Redes overlay (peer-to-peer), Software Defined Networking (SDN)
Nº de sexenios (si procede)	2
Experiencia profesional (si procede)	Contratos de investigación con empresas relevantes del sector TIC: Indra, Broadcom, Cynara, Integra, GMV, Inforges
Otros temas de interés	Investigador visitante en: University College Dublin (UCD), Irlanda

3. Descripción de la asignatura

3.1. Descripción general de la asignatura

La seguridad en redes de telecomunicación es un tema complejo y que despierta a la vez gran curiosidad en el mundo de la ingeniería. Nuevas amenazas, tanto desde dentro como desde fuera de las redes, aparecen constantemente, sobre todo con los imparables avances de las nuevas tecnologías, y al mismo ritmo, se crean nuevos protocolos, algoritmos, o procedimientos para defendernos de esas amenazas. Podemos decir que la seguridad se basa en cuatro grandes pilares que son: confidencialidad, integridad, disponibilidad y autenticación. Es en base a estos elementos, que se ha estructurado el contenido de esta materia para dotar al alumno de la capacidad de aplicar las técnicas en que se basan.

3.2. Aportación de la asignatura al ejercicio profesional

La asignatura Seguridad en Redes cubre una parte vital en la formación del estudiante del Grado en ingeniería Telemática, que es la seguridad en las redes de telecomunicaciones; perfil muy demandado además en el ámbito profesional. Con el objetivo de presentar a los alumnos un temario suficientemente amplio como para cubrir las diferentes áreas dentro de la seguridad y a la vez, que los alumnos sean capaces de entender en profundidad los conceptos básicos que involucra, el temario se ha dividido en tres grandes bloques. El primer bloque, más breve, sirve como introducción a la temática de la seguridad y las políticas de seguridad, de uso obligado en organismos públicos y privados. En el segundo bloque se da a conocer al alumno la criptografía como una de las herramientas para aumentar la seguridad en las redes de comunicaciones. Tras hacer una clasificación de los diferentes sistemas de cifrado en sistemas en bloque, en flujo, simétricos y asimétricos, y estudiar su funcionamiento general, se pasa a revisar en detalle ejemplos actuales de estos algoritmos de cifrado (AES, curva elíptica, etc.). Finalmente, en el tercer bloque se presentan en primer lugar las herramientas básicas de autenticación (funciones hash y códigos MAC, su finalidad y casos prácticos actuales como por ejemplo HMAC), protocolos de autenticación para redes cableadas e inalámbricas, la firma digital y los certificados digitales, así como la protección de contenidos. Para finalizar este bloque, se presentan con profundidad los protocolos de seguridad que se emplean en distintas capas de la arquitectura TCP/IP en Internet, desde el nivel de aplicación hasta el nivel de red, los cortafuegos y las redes privadas virtuales, como herramientas eficientes para mejorar la seguridad de la red.

3.3. Relación con otras asignaturas del plan de estudios

La asignatura Seguridad en Redes se imparte durante el primer cuatrimestre del cuarto curso del Grado en Ingeniería Telemática. Se trata de una asignatura de alto contenido especializado sobre la temática de la seguridad en las redes de comunicaciones actuales. Aunque existe una clara relación de la asignatura Seguridad en Redes con el resto de materias impartidas anteriormente en la titulación, se trata de la primera asignatura que cubre esta temática.

3.4. Incompatibilidades de la asignatura definidas en el plan de estudios

No existen incompatibilidades.

3.5. Recomendaciones para cursar la asignatura

Se recomienda haber cursado las asignaturas: Redes y Servicios de Telecomunicaciones, y Conmutación.

3.6. Medidas especiales previstas

El alumno/a que se encuentre en alguna de las siguientes situaciones debe contactar con el profesor responsable de la asignatura: alumnos/as con discapacidad, alumnos extranjeros, otros casos.

4. Competencias y resultados del aprendizaje

4.1. Competencias básicas* del plan de estudios asociadas a la asignatura

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

4.2. Competencias generales del plan de estudios asociadas a la asignatura

Véase apartado 4.4

4.3. Competencias específicas* del plan de estudios asociadas a la asignatura

T1 Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas estas como sistemas de captacion, transporte, representacion, procesado, almacenamiento, gestion y presentacion de informacion multimedia, desde el punto de vista de los servicios telematicos.

T2 Capacidad para aplicar las tecnicas en que se basan las redes, servicios y aplicaciones telematicas, tales como sistemas de gestion, señalizacion y conmutacion, encaminamiento y enrutamiento, seguridad (protocolos criptograficos, tunelado, cortafuegos, mecanismos de cobro, de autenticacion y de proteccion de contenidos), ingenieria de trafico (teoria de grafos, teoria de colas y teletrafico) tarificacion y fiabilidad y calidad de servicio, tanto en entornos fijos, moviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonia y datos.

4.4. Competencias transversales del plan de estudios asociadas a la asignatura

TR1 - Comunicarse oralmente y por escrito de manera eficaz
TR5 - Aplicar a la práctica los conocimientos adquiridos

4.5. Resultados** del aprendizaje de la asignatura

1. Saber identificar y aplicar una política de seguridad y un sistema de cifrado.
2. Saber identificar y distinguir vulnerabilidades, amenazas y ataques en un sistema de

telecomunicación, siendo capaces de seleccionar los métodos de defensa adecuados ante dichas amenazas.

3. Entender y evaluar el funcionamiento de los sistemas de cifrado más comunes y saber seleccionar el sistema de cifrado más adecuado a un escenario de trabajo.
4. Conocer la finalidad y el funcionamiento de los métodos de autenticación y de los protocolos de autenticación.
5. Entender la finalidad y el funcionamiento de la firma digital, los certificados digitales y las autoridades de certificación.
6. Saber describir el funcionamiento de los protocolos de seguridad más comunes en Internet.
7. Saber seleccionar en función del ámbito de trabajo los protocolos de seguridad más eficaces.
8. Entender la utilidad de una red privada virtual y de un cortafuegos.
9. Saber seleccionar la topología de cortafuegos y/o el sistema de túneles más adecuados al ámbito de trabajo.
10. Saber aplicar de forma práctica los conocimientos adquiridos (por ejemplo, configuración de equipos, etc.).

** **Véase también la *Guía de apoyo para la redacción, puesta en práctica y evaluación de los resultados del aprendizaje,* de ANECA:**

http://www.aneca.es/content/download/12765/158329/file/learningoutcomes_v02.pdf

5. Contenidos

5.1. Contenidos del plan de estudios asociados a la asignatura

Conceptos básicos de seguridad. Criptografía. Seguridad en Internet. Cortafuegos y VPN. Mecanismos de cobro, autenticación y protección de contenidos.

5.2. Programa de teoría (unidades didácticas y temas)

BLOQUE 1. INTRODUCCIÓN A LA SEGURIDAD EN LAS REDES DE COMUNICACIONES.

Conceptos básicos. Definición y tipos de ataques, vulnerabilidades y amenazas. Conceptos básicos como confidencialidad, integridad, disponibilidad y autenticación.

Política de seguridad. Definición y características de una política de seguridad.

BLOQUE 2. CRIPTOGRAFÍA.

Cifrado en bloque. Estudiar el funcionamiento de los principales algoritmos de cifrado en bloque, simétricos y asimétricos (por ejemplo: AES; DES, RSA, curva elíptica, Diffie-Hellman, etc.).

Cifrado en flujo. Estudiar el funcionamiento de los principales algoritmos de cifrado en flujo (por ejemplo: RC4, A5, etc.)

BLOQUE 3. SEGURIDAD EN INTERNET

Autenticación. Sistemas y protocolos de autenticación, certificados y firma digital, protección de contenidos.

Seguridad a nivel de aplicación y a nivel de transporte. Descripción, ventajas y desventajas. Casos de estudio.

Seguridad a nivel de red y a nivel de enlace. Descripción, ventajas y desventajas. Casos de estudio.

Redes privadas virtuales y cortafuegos. Descripción, ventajas y desventajas. Casos de estudio.

5.3. Programa de prácticas (nombre y descripción de cada práctica)

PRACTICA 1: Funciones hash aplicadas a la autenticación de usuarios. El uso más frecuente de funciones hash es para firmar documentos y para autenticar usuarios. En esta práctica se ejemplificará el uso que hace el sistema operativo Linux de los hash DES, MD5, SHA-256 y SHA-512 para autenticar usuarios. En otra práctica se estudiará el uso de los hash para firmar documentos.

PRACTICA 2: Usos cotidianos de la criptografía. En esta práctica se experimentará con distintas técnicas criptográficas que se utilizan de forma cotidiana. En concreto se estudiará: La transferencia segura de archivos entre máquinas remotas (scp), cifrar y descifrar con sistemas simétricos, cifrar y descifrar con sistemas asimétricos, la conexión remota segura (ssh), técnicas esteganográficas, la verificación de un hash (openssl), la generación de contraseñas seguras, el acceso a portales a través de certificados digitales, el escaneo de puertos TCP/UDP abiertos, la firma electrónica, el envío de correos electrónicos firmados y encriptados mediante el estándar openPGP

PRACTICA 3: Configuración de un portal seguro. De entre todos los modelos basados en

la arquitectura cliente-servidor, el portal web es el más conocido y utilizado. Por ello, es muy importante saber configurar un portal web seguro (https), basado en tecnología PKI (Public key infrastructure).

PRACTICA 4: Configuración de un firewall. Un firewall es el dispositivo de red diseñado para filtrar el tráfico de paquetes que circulan por él. Los firewalls se utilizan con frecuencia para evitar que los paquetes generados por usuarios de Internet no autorizados puedan acceder a redes corporativas (intranets). Todos los paquetes que entren o salgan de la intranet pasan a través del firewall, que examina cada paquete y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Prevención de riesgos

La Universidad Politécnica de Cartagena considera como uno de sus principios básicos y objetivos fundamentales la promoción de la mejora continua de las condiciones de trabajo y estudio de toda la Comunidad Universitaria.
Este compromiso con la prevención y las responsabilidades que se derivan atañe a todos los niveles que integran la Universidad: órganos de gobierno, equipo de dirección, personal docente e investigador, personal de administración y servicios y estudiantes.
El Servicio de Prevención de Riesgos Laborales de la UPCT ha elaborado un "Manual de acogida al estudiante en materia de prevención de riesgos" que puedes encontrar en el Aula Virtual, y en el que encontraras instrucciones y recomendaciones acerca de cómo actuar de forma correcta, desde el punto de vista de la prevención (seguridad, ergonomía, etc.), cuando desarrolles cualquier tipo de actividad en la Universidad. También encontrarás recomendaciones sobre cómo proceder en caso de emergencia o que se produzca algún incidente.
En especial, cuando realices prácticas docentes en laboratorios, talleres o trabajo de campo, debes seguir todas las instrucciones del profesorado, que es la persona responsable de tu seguridad y salud durante su realización. Consúltale todas las dudas que te surjan y no pongas en riesgo tu seguridad ni la de tus compañeros.

5.4. Programa de teoría en inglés (unidades didácticas y temas)

UNIT 1. INTRODUCCTION TO NETWORK SECURITY.
Network security fundamentals. Security policy.

UNIT 2. CRYPTOGRAPHY.
Block encryption/decryption algorithms (e.g., AES; DES, RSA, elliptic curves, Diffie-Hellman, etc.)
Flow encryption/decryption algorithms (e.g., RC4, A5, etc.)

UNIT 3. INTERNET SECURITY
Authentication. Protocols and systems, digital certificates, content protection, etc.
Security at application and transport layers. Descriptions, advantages, and limitations. Study cases.
Security at network and link layers. Descriptions, advantages, and limitations. Study cases.
Virtual private networks and firewalls. Descriptions, advantages, and limitations. Study cases.

5.5. Objetivos del aprendizaje detallados por unidades didácticas

La asignatura Seguridad en Redes de Comunicaciones tiene como objetivo familiarizar al alumno con los diferentes mecanismos y servicios de seguridad que deben ofrecer las actuales redes de telecomunicación.

Objetivo del aprendizaje en BLOQUE 1: Familiarizar al alumno con la temática de la

seguridad y las políticas de seguridad, de uso obligado en organismos públicos y privados.

Objetivos del aprendizaje en BLOQUE 2: Comprender las bases teóricas de la criptografía y los métodos de cifrado.

Objetivos del aprendizaje en BLOQUE 3: Entender los servicios de autenticación, firma digital, gestión de claves y control de acceso. Comprender la utilidad e importancia de la seguridad, a través de su inclusión en diversos protocolos y aplicaciones (redes privadas virtuales, comercio electrónico o servidores web, entre otras).

6. Metodología docente

6.1. Metodología docente*

Actividad*	Técnicas docentes	Trabajo del estudiante	Horas
Clase de teoría	Clase expositiva empleando el método de la lección. Resolución de dudas planteadas por los estudiantes.	Presencial: Toma de apuntes. Planteamiento de dudas.	**21**
		No presencial: Estudio de la materia.	**51**
Resolución de ejercicios, problemas y actividades	Se plantean ejercicios y se da un tiempo para que el estudiante intente resolverlo (individual o en grupo). Se resuelve con ayuda de la pizarra y/o material audiovisual, en ocasiones, con la participación de estudiantes. Incluye también actividades en clase y/o a través de Aula Virtual consistentes en la realización de un entregable para cuya elaboración el alumno (o grupo de alumnos) debe ser capaz de buscar, filtrar y elaborar la información disponible en distintos medios (incluye **exposición oral** de resultados).	Presencial: Participación activa. Resolución de ejercicios. Planteamiento de dudas.	**9**
		No presencial: Estudio de la materia. Resolución de ejercicios, problemas y/o actividades propuestas por el profesor de forma individual o en grupo según corresponda.	**34,5**
Prácticas de laboratorio	Se trabaja con los estudiantes en el laboratorio, planteándoles tareas prácticas (p.e., implementación, configuración, programación, etc.) relacionadas con la seguridad en redes de telecomunicación. Al finalizar la sesión se realizará un control tipo test para evaluar los conocimientos adquiridos en la realización de la práctica.	Presencial: Realización de las actividades y ejercicios planteados en el boletín de prácticas.	**24**
		No presencial: Lectura del boletín de prácticas y estudio de la materia. Preparación para valoración de la labor de prácticas.	**34,5**
Asistencia seminarios, conferencias, etc.	Se plantean problemáticas actuales y con conocimientos muy específicos (tanto en el aula como online), en las que la intervención activa del alumnado es fundamental.	Presencial: asistencia y participación activa en el evento	**1,5**
		No presencial: asistencia a seminarios/tutoriales online sobre los que se solicitarán actividades (redacción de opiniones, planteamiento de dudas, críticas, etc.)	**1,5**
Realización de pruebas de evaluación	Evaluación escrita (examen oficial).	Presencial: Asistencia al examen oficial.	**3**
			180

6.2. Resultados (4.5) / actividades formativas (6.1) (opcional)

	Resultados del aprendizaje (4.5)									
Actividades formativas (6.1)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Clase de teoría	x	x	x	x	x	x	x	x	x	x
Resolución de ejercicios, problemas y actividades	x	x	x	x	x	x	x	x	x	x
Prácticas de laboratorio				x		x			x	x
Asistencia a seminarios, conferencias, etc.			x			x		x		x
Realización de pruebas de evaluación	x	x	x	x	x	x	x	x	x	x

7. Metodología de evaluación

7.1. Metodología de evaluación*

Actividad	Tipo		Sistema y criterios de evaluación*	Peso (%)	Resultados (4.5) evaluados
	Sumativa*	Formativa*			
Prueba escrita: Teoría/Ejercicios/Problemas	x		Preguntas breves y/o problemas y/o cuestiones tipo test (conceptos, definiciones, etc.). Evalúan, principalmente, conocimientos y razonamientos teóricos y prácticos.	50%	De 1 a 10
Evaluación continua de las prácticas	x	x	Al finalizar la sesión se realizará un control tipo test para evaluar los conocimientos adquiridos en la realización de la práctica	10%	10
Examen de prácticas	x		Preguntas breves y/o problemas y/o cuestiones tipo test (conceptos, definiciones, etc.). Evalúan, principalmente, conocimientos y razonamientos prácticos.	20%	10
Actividades propuestas por el profesor en clase u otros medios (p.e. Aula Virtual)	x	x	Problemas y ejercicios propuestos por el profesor para resolver en clase o en casa, de forma individual o en grupo. Permiten evaluar tanto la evolución del aprendizaje como ciertas habilidades, por ejemplo, las relacionadas con la búsqueda de información, síntesis y comprensión de la información, comprensión de la información en una lengua extranjera, presentación oral pública, iniciativa, etc.	20%	De 1 a 10
Prueba escrita/oral: Complementaria (3)	x		Sólo disponible cuando se cumplan los criterios establecidos en la normativa vigente. Se evalúa el porcentaje de la nota final que no haya podido ser evaluada por los medios ordinarios contemplados en la guía docente.	20%	De 1 a 10

Comentarios adicionales:

(1) Para poder aprobar la asignatura es necesario haber obtenido una calificación de APTO en la asistencia a las prácticas, que son de carácter obligatorio.

(2) Asimismo, para promediar el alumno deberá sacar un mínimo de cinco puntos tanto en 1) "Prueba escrita: Teoría/Ejercicios/Problemas" como en 2) "Examen de Prácticas".

(3) Tal como prevé el artículo 5.4 del Reglamento de las pruebas de evaluación de los títulos oficiales de grado y de máster con atribuciones profesionales de la UPCT, el estudiante en el que se den las circunstancias especiales recogidas en el Reglamento, y previa solicitud justificada al Departamento y admitida por este, tendrá derecho a una prueba global de evaluación. Esto no le exime de realizar los trabajos obligatorios que estén recogidos en la guía docente de la asignatura.

7.2. Mecanismos de control y seguimiento (opcional)

Para el control y seguimiento de los resultados de los alumnos y la calidad de la asignatura se hará uso tanto del histórico de resultados de cursos académicos anteriores (p.e. encuestas de calidad, etc.) como de los resultados obtenidos durante el curso activo a través de las dos actividades formativas propuestas “Actividades propuestas por el profesor en clase u otros medios” y “Entrega de cuestionarios de prácticas”, aportando la correspondiente realimentación a los alumnos. Asimismo, las tutorías servirán de herramienta de seguimiento, aunque en este caso bajo la demanda del alumno por no ser de carácter obligatorio sino voluntario.

8 Bibliografía y recursos

8.1. Bibliografía básica*

Cryptography and Network Security: Principles and Practice (5th Edition), W. Stallings, Prentice Hall, 2010, ISBN-10: 0136097049.
Network Security Essentials: Applications and Standards (4th Edition), W. Stallings, Prentice Hall, 2010, ISBN-10: 0136108059.

8.2. Bibliografía complementaria*

"Firewalls and Internet Security: Repelling the Wily Hacker", W. R. Cheswick, S. M. Bellovin, A. D. Rubin, 2nd Edition, Addison Wesley, 2003, ISBN 020163466X.
"Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption", W. Ford, M. S. Baum, 2nd Edition, Prentice Hall, 1997, ISBN 0130272760.
"Protect Your Privacy: The Pgp User's Guide", W. Stallings, Prentice Hall, 1994, ISBN 0131855964.
"Security Technologies for the World Wide Web", R.Oppliger, Artech House, 2000, ISBN 1580530451.
"Seguridad y comercio electrónico en la web", Simson Garfinkel, Gene Spafford, Osborne McGranw-Hill/Internamericana de España, ISBN 970-10-2142-8.
"Network Security, Private Communications in a Public World", C. Kaufman, R. Perlman, M. Speciner, C. Kaufman, Prentice Hall, 2002, ISBN 0130460192.
"Building and Managing Virtual Private Networks", D. Kosiur. John Wiley & Sons, 1998.
Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Bruce Schneier, Wiley, 1996, ISBN-10: 0471117099.

8.3. Recursos en red y otros recursos

Aula virtual de la asignatura accesible para todos los alumnos matriculados.
Trabajos de investigación y/o divulgativos proporcionados por el profesor.