

**Proyecto/Guía docente de la asignatura**

Asignatura	Ciberseguridad		
Materia	Formación optativa		
Módulo			
Titulación	Máster en Ingeniería de Telecomunicación		
Plan	736	Código	55268
Periodo de impartición	1.º cuatrimestre (2.º bimestre)	Tipo/Carácter	Optativa
Nivel/Ciclo	Máster	Curso	2.º
Créditos ECTS	3 ECTS		
Lengua en que se imparte	Español		
Profesor/es responsable/s	Federico Simmross Wattenberg		
Datos de contacto (E-mail, teléfono...)	e-mail: fedsim@tel.uva.es Teléfono: 983 42 30 00 ext. 5539		
Departamento	Teoría de la Señal y Comunicaciones e Ingeniería Telemática		
Fecha de revisión por el Comité de Título	10 de julio de 2026		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Podría decirse que uno de los objetivos principales de la Ingeniería de Telecomunicación es conseguir que las comunicaciones a distancia que forman su naturaleza misma sean seguras. En un mundo digitalizado y global, la amenaza bajo la que se encuentran tanto dichas comunicaciones como los sistemas que las procesan y las almacenan es constante, y es necesario monitorizar continuamente y tomar medidas activas para que la integridad, disponibilidad y confidencialidad de los datos no se vea afectada.

En la asignatura «Ciberseguridad» (CIB) se pretende proporcionar a los alumnos unos conocimientos adecuados, mediante una orientación práctica, sobre diversos aspectos que deben tenerse en cuenta a la hora de configurar y mantener los sistemas que tienen presencia en Internet, y son, por lo tanto, susceptibles de ser atacados en cualquier momento.

1.2 Relación con otras materias

Esta asignatura está relacionada con las asignaturas *Computación en la nube y virtualización* y *Desarrollo de aplicaciones telemáticas distribuidas*, de la materia *Infraestructuras, redes y servicios* en cuanto a que las aplicaciones que allí se desarrollan y los entornos en los que en ellas se trabaja son candidatos de primer orden a proteger mediante los conocimientos y técnicas impartidas en *Ciberseguridad*.

1.3 Prerrequisitos

No existen requisitos previos para cursar esta asignatura. Sin embargo, es muy recomendable tener conocimientos básicos de administración y gestión de sistemas en red y cierta soltura con el manejo de una terminal UNIX. Para el caso de los alumnos procedentes del *Grado en Ingeniería de Tecnologías Específicas de Telecomunicación, mención en Telemática*, esta recomendación queda plenamente satisfecha tras haber superado las asignaturas *Administración y gestión de redes de comunicaciones* y *Seguridad en redes de comunicaciones*. De forma análoga, para los alumnos procedentes del *Grado en Ingeniería de Tecnologías de Telecomunicación*, esta recomendación se cumple tras superar la asignatura *Administración y gestión de redes y servicios telemáticos*. Para los alumnos que han de completar la materia *Complementos de Telemática para Graduados en Tecnologías Específicas de Telecomunicación, mención en Sistemas de Telecomunicación y mención en Sistemas Electrónicos* es muy recomendable haber superado la asignatura *Fundamentos de administración y gestión de redes de comunicaciones*.

2. Competencias

2.1 Generales

- G1. Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería de telecomunicación.
- G5. Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería de Telecomunicación siguiendo criterios de calidad y medioambientales.
- G8. Capacidad para la aplicación de los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar conocimientos.
- G9. Capacidad para comprender la responsabilidad ética y la deontología profesional de la actividad de la profesión de Ingeniero de Telecomunicación.
- G10. Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de las telecomunicaciones.
- G11. Capacidad para saber comunicar (de forma oral y escrita) las conclusiones -y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- G12. Poseer habilidades para el aprendizaje continuado, autodirigido y autónomo.
- G13. Conocimiento, comprensión y capacidad para aplicar la legislación necesaria en el ejercicio de la profesión de Ingeniero de Telecomunicación.

2.2 Específicas

- TEL1. Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
- TEL2. Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.
- TEL3. Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.

3. Objetivos

Una vez superada la asignatura los alumnos deberían ser capaces de:

- Conocer las primitivas básicas disponibles en sistemas de seguridad y las principales técnicas de defensa utilizadas en tareas de ciberseguridad.
- Comprender las ventajas e inconvenientes de diferentes sistemas de cifrado.
- Entender los componentes, fundamentos y aplicaciones de la tecnología *Blockchain*.
- Ser capaz de aplicar buenas prácticas de configuración e implementación de sistemas TIC desde el punto de vista de la seguridad y de analizar la seguridad de dichos sistemas.



4. Contenidos y/o bloques temáticos

Bloque 1: Ciberseguridad

Carga de trabajo en créditos ECTS: 3

a. Contextualización y justificación

Véase el apartado 1.1.

b. Objetivos de aprendizaje

Véase el apartado 3.

c. Contenidos

- Generación de claves y certificados. Autenticación y claves de sesión.
- Despliegue de sistemas de comunicación seguros: HTTPS, SSH e IPsec.
- Despliegue de cortafuegos de funcionalidad avanzada.
- Configuración segura y detección de puntos débiles en sistemas UNIX.
- Concepto de *blockchain*.

d. Métodos docentes

- Clase magistral participativa.
- Resolución de problemas.
- Aprendizaje basado en problemas.
- Aprendizaje cooperativo.
- Estudio de casos.

e. Plan de trabajo

Véase el Anexo I.

f. Evaluación

- Informes de laboratorio, realizados por los alumnos individualmente y entregados a través del Campus Virtual.
- Exposición oral de un trabajo relacionado con los contenidos de la asignatura.

g Material docente

g.1 Bibliografía básica

- W. Stallings, *Cryptography and Network Security*, Pearson Education, 6th Edition, 2014.
- W. Stallings y L. Brown, *Computer Security. Principles and practice*, 3rd Edition, Pearson Education, 2015.

g.2 Bibliografía complementaria

- E. Nemeth, G. Snyder, T.R. Hein y B. Whaley, *UNIX and Linux System Administration Handbook*, 4th Edition, Prentice Hall, 2011.
- E.D. Comer, *Internetworking with TCP/IP vol.1: principles, protocols and architecture*. 5th edition, Prentice Hall, 2006.

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), ...)

- Página de la asignatura en el Campus Virtual.

h. Recursos necesarios

Serán necesarios los siguientes recursos, todos ellos facilitados por la Universidad de Valladolid o el profesor:

- Entorno de trabajo en la plataforma Moodle ubicado en el Campus Virtual.
- Entorno de trabajo en el laboratorio de la asignatura.
- Bibliografía disponible en la biblioteca de la Universidad.
- Documentación de apoyo.

i. Temporalización

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Ciberseguridad	3 ECTS	Semanas 9 a 16 del primer cuatrimestre

5. Métodos docentes y principios metodológicos

Véase el apartado 4.d.

6. Tabla de dedicación del estudiantado a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA ⁽¹⁾	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	14	Estudio y trabajo autónomo individual	30
Laboratorios (L)	10	Estudio y trabajo autónomo grupal	15
Prácticas en aula, seminarios, tutorías y evaluación	6		
Total presencial	30	Total no presencial	45
TOTAL presencial + no presencial			75

(1) Actividad presencial a distancia es aquella en la que un grupo sigue una videoconferencia de forma síncrona a la clase impartida por el profesor.

7. Sistema y características de la evaluación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Informes de laboratorio	80%	Es condición necesaria (pero no suficiente) para superar la asignatura que la calificación de cada uno de los informes sea igual o superior al 4 puntos sobre 10.
Exposición oral	20%	Es condición necesaria (pero no suficiente) para superar la asignatura que la calificación en este apartado sea igual o superior a 4 puntos sobre 10.

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**
 - En caso de que no se alcance el mínimo exigido para promediar, la calificación final será el mínimo obtenido en los informes/exposición oral.
- **Convocatoria extraordinaria:**
 - La evaluación se realizará del mismo modo que en la convocatoria ordinaria.
- **Verificación de autoría:** la calificación final de cualquier actividad evaluable (exámenes parciales, examen final o prácticas de laboratorio) está supeditada a la autoría original del estudiante. El profesorado se reserva el derecho de convocar a cualquier estudiante a una prueba oral complementaria para explicar o justificar los procedimientos y resultados entregados. La no comparecencia injustificada o la incapacidad para justificar el trabajo supondrá la calificación de 0 puntos en la prueba correspondiente, impidiendo superar el umbral mínimo exigido en dicha actividad evaluable.



8. Consideraciones finales

El Anexo I mencionado en la guía, donde se describe la planificación detallada, se entregará al comienzo de la asignatura

