



## FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Seguridad y Normativa
Código	DTC-GITT-413
Título	<a href="#">Grado en Ingeniería en Tecnologías de Telecomunicación por la Universidad Pontificia Comillas</a>
Impartido en	Grado en Ingeniería en Tecnologías de Telecom. y Grado en Análisis de Negocios/Business Analytics [Cuarto Curso] Grado en Ingeniería en Tecnologías de Telecomunicación [Cuarto Curso]
Nivel	Reglada Grado Europeo
Cuatrimestre	Semestral
Créditos	7,5 ECTS
Carácter	Obligatoria (Grado)
Departamento / Área	Departamento de Telemática y Computación
Responsable	Rafael Palacios Hielscher
Horario	Mañana
Horario de tutorías	Acordar con los profesores

Datos del profesorado	
<b>Profesor</b>	
Nombre	Francisco Javier Santos Ortega
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	jsortega@icai.comillas.edu
<b>Profesor</b>	
Nombre	Mary Luz Mouronte López
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	mmouronte@icai.comillas.edu
<b>Profesores de laboratorio</b>	
<b>Profesor</b>	
Nombre	Rafael Palacios Hielscher
Departamento / Área	Departamento de Telemática y Computación
Despacho	Alberto Aguilera 25 [Dirección]
Correo electrónico	Rafael.Palacios@iit.comillas.edu

## DATOS ESPECÍFICOS DE LA ASIGNATURA

<b>Contextualización de la asignatura</b>
<b>Aportación al perfil profesional de la titulación</b>



En el perfil profesional del graduado en ingeniería de telecomunicación la asignatura de Seguridad y Normativa contribuye en varios aspectos relevantes:

- Conocer la normativa específica que aplica al sector de las comunicaciones y la normativa asociada a seguridad y protección de la información.
- Conocer no sólo la legislación y normativa nacional sino también la internacional, y más concretamente la europea.
- Se desarrolla la capacidad de aplicar dicha normativa a los entornos donde las telecomunicaciones prestan servicio.
- Desarrollar conciencia de seguridad de las información. Las implicaciones que pueden tener las brechas de seguridad, acceso ilegítimo a información sensible, la denegación de servicios, etc.

## Prerequisitos

Conocimientos básicos de redes, servicios web, protocolo http.

## Competencias - Objetivos

### Competencias

#### GENERALES

<b>CG02</b>	Conocimiento, comprensión y capacidad para aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico de Telecomunicación.
<b>CG05</b>	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.
<b>CG06</b>	Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
<b>CG08</b>	Conocer y aplicar elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como de legislación, regulación y normalización en las telecomunicaciones.

#### ESPECÍFICAS

<b>CETM02</b>	Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización 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.
<b>CRT15</b>	Conocimiento de la normativa y la regulación de las telecomunicaciones en los ámbitos nacional, europeo e internacional.

### Resultados de Aprendizaje

<b>RA1</b>	Conocer las técnicas criptográficas más adecuadas en la transmisión
<b>RA2</b>	Ser capaces de utilizar e implantar herramientas de supervisión y control de acceso en redes de datos.
<b>RA3</b>	Conocer los protocolos seguros utilizados en las redes de datos así como su idoneidad en la arquitectura global de una



	organización
<b>RA4</b>	Conocer los estándares de gestión de la seguridad y poseer la capacidad de implantar una política de seguridad acorde a dichos estándares
<b>RA5</b>	Conocer el marco regulatorio de las telecomunicaciones en España y en la Unión Europea.
<b>RA6</b>	Interpretar y aplicar la normativa de las telecomunicaciones y la informática en los ámbitos nacional, europeo e internacional y los casos en los que aplica.
<b>RA7</b>	Conocer estándares de seguridad, métricas de cumplimiento de seguridad, y normativa específica.

## BLOQUES TEMÁTICOS Y CONTENIDOS

### Contenidos – Bloques Temáticos

#### 1 POLÍTICAS Y NORMATIVA DE TELECOMUNICACIONES EN LA UE

- Como es y como se rige la UE (Unión Europea). Normativa de la UE.

#### 2 NORMATIVA DE TELECOMUNICACIONES EN ESPAÑA

- LOT (Ley Ordenación de las Telecomunicaciones).
- Liberalización RDL 6/1996 y Ley Liberalización de Telecomunicaciones (LLT) 2/1997.
- Ley General de Telecomunicaciones (LGT) 11/98, 32/2003 y 9/2014.
- Normativa técnica de infraestructuras y servicios de telecomunicaciones.

#### 3 INTRODUCCION A LA SEGURIDAD

- Introducción y Conceptos Básicos
- Análisis de riesgos.

#### 4 CRIPTOGRAFÍA

- Criptografía simétrica y clave pública
- Cifrado irreversible, Funciones de resumen y Aleatoriedad
- Algoritmos de firma digital

#### 5 ARQUITECTURA SEGURA DE REDES

- Segregación de Tráfico. Redes Privadas Virtuales.
- Túneles y Cortafuegos.
- Protocolos Seguros.
- Acceso Remoto
- Infraestructuras de Clave Pública (PKI)
- Virus y Sistemas Antivirus.

#### 6 GESTION DE LA SEGURIDAD

- Monitorización, Sistemas IDS, IPS Y Detección de Anomalías.
- Estándares de Gestión de la Seguridad.
- Cuadro de Mando de La Seguridad, Métricas.

## **7 NORMATIVA DE SEGURIDAD.**

- Regulación, SOX, LOPD, LSSI.

## **8 CUMPLIMIENTO (SECURITY COMPLIANCE)**

- Sistemas de certificación
- Auditoría y Control

## **PRACTICAS**

### **Lab 1-** Requisitos mínimos de seguridad

- Strong passwords, 2FA, cifrado de discos
- Técnicas de backup/restore.

### **Lab 2-** Seguridad de las contraseñas

- Descifrar passwords. Encontrar passwords comprometidas.
- Password recovery tools for browsers

### **Lab 3-** Técnicas de cifrado

- Cifrado simétrico
- cifrado asimétrico
- Firma electrónica
- Ataques básicos

### **Lab 4-** Comunicaciones seguras 1

- HTTPS, certificados, man-in-the-middle MITM

### **Lab 5-** Comunicaciones seguras 2

- Ataque https con sslstrip
- Ataques en redes WiFi.

### **Lab 6-** Análisis de tráfico web

- Burp, Fiddler. Formularios post y get
- Web Scraping
- Modificación de valores en una query

### **Lab 7-** SQL injection.

- sqlmap
- Ataque a base de datos

## **METODOLOGÍA DOCENTE**



## 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 llevadas a cabo por los alumnos de los temas o contenidos propuestos por el profesor. También se realizarán debates grupales y pruebas para facilitar la comprensión de los mismos. Además, se resolverán los pequeños ejercicios propuestos por el profesor.
- **Prácticas de laboratorio:** La asignatura comprende la realización de sesiones 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 en grupo e individualmente para resolver las dudas planteadas a los alumnos después de trabajar sobre los distintos temas. También se utilizarán para orientar al alumno en su proceso de aprendizaje

## Metodología No presencial: Actividades

- Estudio teórico:
  - Estudio y preparación de los temas o conceptos que vayan a ser expuestos por el profesor.
  - Estudio individual y personal por parte del alumno de los conceptos ya expuestos en las lecciones expositivas.
- Casos prácticos: Resolución de casos propuestos por el profesor
- Preparación de las prácticas del laboratorio de comunicaciones. Elaboración del documento de prácticas del laboratorio de comunicaciones, que incluyen los procedimientos, informes, resultados comentarios de cada una de las prácticas realizadas.

## RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES		
Clase magistral y presentaciones generales	Resolución de problemas de carácter práctico o aplicado	Prácticas de laboratorio
45.00	10.00	20.00
HORAS NO PRESENCIALES		
Prácticas de laboratorio	Estudio de conceptos teóricos fuera del horario de clase por parte del alumno	
10.00	140.00	
<b>CRÉDITOS ECTS: 7,5 (225,00 horas)</b>		

## EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	Peso
Examen Final de Seguridad (50%) y Normativa (5%)	<ul style="list-style-type: none"> <li>• Comprensión de conceptos.</li> <li>• Aplicación de conceptos para la resolución de problemas reales.</li> </ul>	55
<b>Evaluación del trabajo experimental:</b>	Documento de prácticas del Laboratorio <ul style="list-style-type: none"> <li>• El informe de cada práctica se entrega en el plazo de una semana después de terminar la</li> </ul>	



<ul style="list-style-type: none"> <li>Prácticas de Laboratorio (10%)</li> <li>Preguntas sobre las prácticas el día del examen final (5%)</li> </ul>	<p>sesión de laboratorio.</p> <ul style="list-style-type: none"> <li>Comprensión de conceptos.</li> <li>Aplicación de conceptos para la resolución de problemas.</li> <li>Carácter técnico y exactitud de la documentación entregada</li> </ul>	15
<p><b>Evaluación continua del rendimiento:</b></p> <ul style="list-style-type: none"> <li>Tareas relativas a Normativa de telecomunicación (25%)</li> <li>Realización de pruebas intermedias de seguimiento y ejercicios (5%)</li> </ul>	<p>Tareas relativas a normativa de telecomunicación</p> <ul style="list-style-type: none"> <li>Comprensión de conceptos.</li> </ul> <p>Realización de pruebas intermedias de seguimiento y ejercicios</p> <ul style="list-style-type: none"> <li>Comprensión de conceptos.</li> <li>Aplicación de conceptos para la resolución de problemas.</li> <li>Análisis e interpretación de los resultados obtenidos en la resolución de problemas</li> </ul>	30

### Calificaciones

70% de la calificación final en la asignatura corresponde a la parte de Seguridad.

30% de la calificación corresponde a la parte de Normativa.

Para aprobar la asignatura los alumnos deben alcanzar al menos 4 puntos sobre 10 tanto en la parte de Seguridad como en la parte de Normativa.

Los criterios de calificación son los mismos en convocatoria ordinaria y extraordinaria.

### PLAN DE TRABAJO Y CRONOGRAMA

Actividades	Fecha de realización	Fecha de entrega
Lectura y estudio de los contenidos teóricos en los apuntes de la asignatura	Después de cada clase	
Ejercicios	Después de la clase en la que son propuestos	Siguiendo día de clase
Tareas relativas a normativa de telecomunicación	Después de la clase final a cuyo tema se refieren	Semana siguiente a la clase final a cuyo tema se refieren
Preparación de las practicas de laboratorio	Uno o dos días antes de cada practica	
Entregas parciales del documento de practicas	Después de cada práctica	Semana posterior a la realización de la practica
Preparación de Examen Final	Diciembre	



## BIBLIOGRAFÍA Y RECURSOS

### Bibliografía Básica

Normativa:

- Material específico desarrollado por el profesor accesible a través del portal de recursos de la asignatura.

Seguridad:

- Fundamentos de seguridad en redes: aplicaciones y estándares. William Stallings. Pearson Prentice Hall. ISBN: 8422052400221

### Bibliografía Complementaria

Normativa:

- Comentarios a la Ley General de Telecomunicaciones Javier Cremades y Jaime Rodríguez-Arana. Editorial La Ley.
- Liberalización, competencia y regulación de las telecomunicaciones en España. Jaime García – Legaz Ponce. Revista Economía Industrial Nº 337.
- Comunicaciones electrónicas de la Unión Europea. Alabau y Guijarro.

Seguridad:

- Criptored. [www.criptored.upm.es](http://www.criptored.upm.es)
- Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. CRC Press. ISBN: 0284932852327
- Criptografía y Seguridad en Computadores. J. Manuel Lucena.

En cumplimiento de la normativa vigente en materia de **protección de datos de carácter personal**, le informamos y recordamos que puede consultar los aspectos relativos a privacidad y protección de datos [que ha aceptado en su matrícula](#) entrando en esta web y pulsando "descargar"

<https://servicios.upcomillas.es/sedelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>