

Seguridad en 5G	
CRÉDITOS ECTS Y CARÁCTER	6 Creditos ECTS obligatorios
Ubicación temporal	Segundo curso, Modulo 2
COMPETENCIAS Y RESULTADOS DE APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON ESTE MÓDULO	
Al finalizar este módulo, el alumno tendrá las siguientes competencias:	
<ul style="list-style-type: none"> • Podrá entender y utilizar las técnicas de seguridad asociadas a redes 5G en particular aquellas vinculadas a entornos NFV y SDN. • Podrá extrapolar los conocimientos aprendidos y utilizarlos en entornos más amplios, relacionados con redes 5G. • Podrá entender y adaptarse a las nuevas tecnologías de seguridad que vayan surgiendo en redes 5G a partir de la base obtenida en este curso. 	
Tras realizar este módulo, el alumno será capaz de:	
<ul style="list-style-type: none"> • Comprender el funcionamiento básico de un criptosistema de seguridad y las técnicas criptográficas básicas. • Comprender las bases de la seguridad actual en redes 5G, incluyendo las técnicas de criptografía ligera, seguridad en sistemas operativos y protocolos de seguridad en red. • Comprender la utilización y de las diferentes técnicas y protocolos de seguridad y aplicarlos a entornos de virtualización y entornos NFV y SDV según sea necesario. 	
OBJETIVOS	
<p>El objetivo principal de este módulo es el de dar una idea general de los diferentes aspectos de seguridad asociados a las redes 5G. El módulo incluye unas sesiones iniciales de nivelación para aquellos alumnos que no dispongan de formación previa en temas de seguridad y posteriormente se centra en temas específicos vinculados a tecnologías 5G.</p>	
Al final del curso, el alumno:	
<ul style="list-style-type: none"> • Dispondrá de los conocimientos necesarios para poder entender con criterio las diferentes soluciones de seguridad disponibles en las redes 5G. • Tendrá los conocimientos necesarios para aplicar las soluciones de seguridad vinculadas a tecnologías NFV y SDN, así como a diferentes entornos de virtualización. 	
ACTIVIDADES FORMATIVAS	
<ul style="list-style-type: none"> • Teoría. Clases con material de apoyo disponible en la Web, utilizando plataforma tipo Moodle <ul style="list-style-type: none"> ○ Clases magistrales • Prácticas <ul style="list-style-type: none"> ○ Prácticas en grupos en aulas informáticas ○ Resolución de problemas, tanto individualmente como en equipo 	
SISTEMA DE EVALUACIÓN DE LA ADQUISICIÓN DE COMPETENCIAS Y SISTEMA DE CALIFICACIONES	
<ul style="list-style-type: none"> • Evaluación de las diferentes actividades realizadas por el alumno individual o colectivamente • Examen final individual de la asignatura para comprobar que el alumno ha adquirido todas las competencias previstas 	
BREVE RESUMEN DE CONTENIDOS	
Unidad 1: Fundamentos de seguridad en red	
<ul style="list-style-type: none"> • Introducción a la seguridad • Criptografía ligera • Seguridad en red • Seguridad en sistemas operativos 	
Unidad 2: Seguridad en 5G	
<ul style="list-style-type: none"> • Seguridad en comunicaciones móviles 	

- Seguridad en virtualización
- Seguridad en NFV
- Seguridad en SDN

Bibliografía

- Handbook of applied cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. <http://cacr.uwaterloo.ca/hac/>
- Cryptography and network security. Principles and Practice. William Stallings. 7th edition. 2017 Pearson.