FICHA DESCRIPTIVA DE MATERIA

INFORMACIÓN GENERAL			
Denominación de la materia:	*(En castellano)* Ciberseguridad de Sistemas y Aplicaciones		
	(En Inglés) Cibersecurity in Systesms and Applications		
Número de créditos ECTS:	*10,5*	**Ubicación temporal:**	1º y 2º
Idioma de impartición:	Español, inglés		
Carácter:	Obligatoria		
Módulo en el que se integra:	Tecnologías Informáticas		

SISTEMA DE EVALUACIÓN

Descripción de los Sistemas de Evaluación	*Ponderación Mínima (%)*	*Ponderación Máxima (%)*
Presentación de trabajos	0	100
Entrega de prácticas	0	100
Examen Escrito	0	100

ACTIVIDADES FORMATIVAS

Horas totales Trabajo del Alumno (25 h. x número de créditos): *262,5* **horas.**
Horas Presencialidad Máxima (30 % de las horas, salvo para Practicas Externas y TFM): *79* **horas.**

Descripción de la Actividad Formativa	*Horas Activ.*	*Presencialidad (%)*
Actividades presenciales	71	100
Actividades evaluación	8	100
Actividades no presenciales	183,5	0

METODOLOGÍAS DOCENTES

Clases Magistrales.
Aprendizaje basado en proyectos.
Trabajo en Grupo

RESULTADOS DE APRENDIZAJE
- Ser capaz de reconocer los distintos tipos de amenazas a protocolos de comunicaciones, y de decidir qué soluciones desplegar en cada caso, considerando los aspectos de configuración de los distintos mecanismos y dispositivos a emplear. - Aprender a analizar los requisitos de seguridad de diferentes entornos de aplicación con el objetivo de decidir qué conjunto de servicios aplicar en función del entorno, así como qué soluciones se pueden implementar teniendo en cuenta los distintos niveles de implicación de los usuarios y los efectos que esas soluciones tienen sobre la privacidad de los mismos.

Breve descripción de los CONTENIDOS
Esta es una materia obligatoria que ofrece al alumno una visión transversal de la problemática de seguridad, y soluciones correspondientes, desde el nivel de redes y sistemas hasta el nivel de aplicaciones. De esta manera, se introducirá al alumno en el aprendizaje de las principales amenazas en protocolos de comunicaciones tradicionales, para seguidamente entender qué mecanismos y dispositivos de seguridad para red están disponibles en el mercado y que ayudan al despliegue de un sistema seguro, además de los problemas de configuración y administración que comportan su uso. En base a esto, el alumno aprenderá los criterios principales a utilizar durante la fase de diseño de una arquitectura de seguridad. En la segunda parte de la materia, y una vez garantizada la seguridad del sistema y de la red, el alumno afrontará la problemática de seguridad en diferentes entornos de aplicación. Concretamente, y dada su trascendencia actual, se hará especial hincapié en las aplicaciones Web y aplicaciones móviles. Adicionalmente, y como complemento a los bloques de materias también obligatorias presentadas en esta Memoria, se introducirá al alumno en la problemática específica de seguridad de entornos de aplicación de sistemas Cloud e IoT, mostrando las soluciones propuestas hasta el momento por organismos de estandarización así como las desarrolladas a través de algunas iniciativas comerciales. Adicionalmente, y dada la participación activa de los usuarios en la mayoría de los entornos de aplicación, así como las implicaciones que esto tiene sobre los riesgos de privacidad de los mismos, esta parte de la materia también incluirá el aprendizaje por parte del alumno de técnicas y procedimientos que se pueden integrar en las aplicaciones con el objeto de preservar unos mínimos niveles de privacidad de los usuarios en su interacción con las aplicaciones. En resumen, el foco principal de esta materia se pondrá en los siguientes temas, que irán actualizándose a medida que vayan evolucionando, principalmente, los ámbitos de aplicación de la misma: - Amenazas en protocolos de comunicaciones - Mecanismos de seguridad en redes - Diseño de arquitecturas de seguridad - Ejecución segura de servicios y aplicaciones - Seguridad en aplicaciones Web y aplicaciones móviles - Seguridad en entornos Cloud e IoT - Privacidad del usuario

COMPETENCIAS	
Competencias básicas	CB1, CB2, CB3, CB4, CB5

Competencias generales:	CG1, CG2, CG8, CG10
Competencias Transversales:	CT1, CT2
Competencias específicas:	ETI1, ETI2, ETI3, ETI4, ETI5, ETI8