

[MRD003] NORMATIVAS DE CIBERSEGURIDAD

DATOS GENERALES

Titulación	Máster Universitario en ROBÓTICA Y SISTEMAS DE CONTROL	Materia	SISTEMAS DE CONTROL E INTEROPERABILIDAD
Semestre	2	Curso	1
Carácter	OPTATIVA	Mención / Especialidad	
Plan	2019	Modalidad	Presencial
Créditos	3	H./sem.	0
		Idioma	CASTELLANO
		Horas totales	32 h. lectivas + 43 h. no lectivas = 75 h. totales

PROFESORES

LIZARRAGA DURANDEGUI, JESUS MARIA

CONOCIMIENTOS PREVIOS REQUERIDOS

Asignaturas	Conocimientos
(No se requiere haber cursado asignaturas previas específicas)	(No se requieren conocimientos previos)

COMPETENCIAS

COMPETENCIAS VERIFICA

ESPECÍFICA

MRCE18 - Comprender la legislación y normativa existente en materia de ciberseguridad y verificar la conformidad del sistema respecto a ellas

TRANSVERSAL

MRCTR2 - Capacidad para ejercer su profesión con actitud cooperativa y participativa, y con responsabilidad social

BÁSICA

M_CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

RESULTADOS DE APRENDIZAJE

RA181 Identifica, diferencia y utiliza los estándares principales en materia de seguridad, así como la legislación existente colaborando de manera activa para evaluar y asumir la responsabilidad social implícita en la propuesta

ACTIVIDADES FORMATIVAS

	HL	HNL	HT
Desarrollo, redacción y presentación de memorias, informes, material audiovisual, etc. relativas a proyectos/POPBLs, realizados individualmente o en equipos	9 h.	23 h.	32 h.
Estudio y trabajo individual, pruebas, exámenes y/o puntos de control	2 h.	8 h.	10 h.
Presentación en el aula en clases participativas, de conceptos y procedimientos asociados a las materias	15 h.		15 h.
Resolución y realización de ejercicios, problemas y prácticas individualmente y en equipo	6 h.	12 h.	18 h.

SISTEMAS DE EVALUACIÓN

	P
Pruebas escritas y orales individuales para la evaluación de competencias técnicas de la materia	50%
Informes de realización de ejercicios, estudio de casos, prácticas de ordenador, prácticas de simulación y prácticas de laboratorio	30%
Capacidad técnica, implicación en el proyecto/PBL, trabajo realizado, resultados obtenidos, documentación entregada, presentación y defensa técnica	20%

MECANISMOS DE RECUPERACIÓN

Pruebas escritas y orales individuales para la evaluación de competencias técnicas de la materia
 Informes de realización de ejercicios, estudio de casos, prácticas de ordenador, prácticas de simulación y prácticas de laboratorio

HL - Horas lectivas: 32 h.
HNL - Horas no lectivas: 43 h.
HT - Total horas: 75 h.

CONTENIDOS

- * Estándares aplicables a ciberseguridad (ISO 27k, IEC...)
- * Legislación aplicable a la ciberseguridad
- * Planes de seguridad (continuidad de negocio, formación etc.)
- * Centros de operaciones de seguridad y gestión de incidentes

RECURSOS DIDÁCTICOS Y BIBLIOGRAFÍA

Recursos didácticos	Bibliografía
Apuntes de la asignatura	AENOR: Norma UNE-EN ISO/IEC 27001:2017
Plataforma Moodle	AENOR: Norma UNE-EN ISO/IEC 27002:2017
Presentaciones en clase	AENOR: Norma UNE-EN ISO 22301:2015
	Luis Gómez y Pedro P. Fernández, 2018. "Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad". Editorial: AENOR. Rústica. ISBN:978-84-8143-963-2
	Punit Bhatia, 2018. "Intro to GDPR". Advisera ExpertSolutions Ltd. ISBN: 978-953-8155-18-51