[MRD003] CYBERSECURITY REGULATIONS

GENERAL INFORMATION

Studies	Master's Degree in ROBOTICS AND CONTROL SYSTEMS			**Subject**	Interoperability Control Systems
Semester	2	**Course**	1	**Mention / Field of specialisation**	
Character	OPTIONAL				
Plan	2019	**Modality**	Adapted Face-to-face	**Language**	CASTELLANO
Credits	3	**Hours/week**	0	**Total hours**	32 class hours + 43 non-class hours = **75 total hours**

PROFESSORS

LIZARRAGA DURANDEGUI, JESUS MARIA

REQUIRED PREVIOUS KNOWLEDGE

Subjects	Knowledge
(No specific previous subjects required)	*(No previous knowledge required)*

SKILLS

VERIFICA SKILLS

SPECIFIC

MRCE18 - Understanding existing legislation and regulations on cybersecurity and verifying the compliance of the system with respect to them.

CROSS

MRCTR2 - Ability to do their job with a cooperative and participatory attitude, while being socially responsible

BASIC

M_CB8 - To be able to integrate different types of knowledge and make complex judgements based on information that, in spite of being partial or limited, includes ideas on the social and ethical responsibilities associated with the application of knowledge

LEARNING RESULTS

RA181 Identifies, differentiates and uses the main security standards, as well as existing legislation, collaborating actively to assess and assume the social responsibility implicit in the proposal.

LEARNING ACTIVITIES	CH	NCH	TH
Development, writing and presentation of memorandums, reports, audiovisual material, etc. Relating to projects/POPBLs carried out individually or in teams	9 h.	23 h.	32 h.
Individual study and work, tests and evaluations and check points	2 h.	8 h.	10 h.
Classroom presentations of relevant concepts and procedures in participatory environments	15 h.		15 h.
Individual and team solving of exercises, problems, and practices	6 h.	12 h.	18 h.

EVALUATION SYSTEM	W
Individual written and oral tests to assess technical skills of the subject	50%
Reports of solving exercises, case studies, computer practices, simulation practices and laboratory practices	30%
Technical skills, involvement in the project, finished work, obtained results, handed documentation, presentation and technical defence	20%

MAKE-UP MECHANISMS

Individual written and oral tests to assess technical skills of the subject

Reports of solving exercises, case studies, computer practices, simulation practices and laboratory practices

Comments: All assessment activities (control points, individual and group assignments, etc...) must have a minimum grade of 5 and there will be an extra opportunity for those who do not pass in the first try (except for the PBL project). In all activities with a grade less than 5 resits are mandatory and the final grade will be the resit grade. In the assessment activities, it is necessary to obtain a minimum grade of 4 to calculate the average grade of the learning outcome. Otherwise, the learning outcome grade will be the grade of the failed activity.

CH - Class hours: 32 h.
NCH - Non-class hours: 43 h.
TH - Total hours: 75 h.

CONTENTS

* Standards applicable to cybersecurity (ISO 27k, IEC ...)

* Legislation applicable to cybersecurity

* Security plans (business continuity, training etc.)

* Security operations centers and incident management

LEARNING RESOURCES AND BIBLIOGRAPHY

Learning resources
Subject notes
Moodle Platform
Class presentations

Bibliography

AENOR: Norma UNE-EN ISO/IEC 27001:2017

AENOR: Norma UNE-EN ISO/IEC 27002:2017

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 suaplicación 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