

[MNB001] INFRASTRUCTURE AND NETWORK SECURITY

GENERAL INFORMATION

Studies	MASTER DEGREE IN DATA ANALYSIS, CYBERSECURITY AND CLOUD COMPUTING		Subject	Cybersecurity
Semester	1	Course	1	Mention / Field of specialisation
Character	COMPULSORY		Language	ENGLISH
Plan	2019	Modality	Adapted Face-to-face	
Credits	6	Hours/week	0	Total hours 64 class hours + 86 non-class hours = 150 total hours

PROFESSORS

GARITANO GARITANO, IÑAKI

ITURBE URRETXA, MIKEL

REQUIRED PREVIOUS KNOWLEDGE

Subjects	Knowledge
(No specific previous subjects required)	<p>Able to install and manage both physical and virtual servers in a network infrastructure.</p> <p>Able to install and manage the GNU/Linux operating system and services on this operating system.</p> <p>Able to install and manage a network of both physical and virtual computers.</p>

SKILLS

VERIFICA SKILLS

SPECIFIC

MNCE06 - Recognising the main computer threats and vulnerabilities and designing, developing and implementing existing security countermeasures at the level of infrastructures and networks to address them.

CROSS

MNCTR1 - Ability to work in multidisciplinary teams and in a multilingual environment (Basque/Spanish/English) and to communicate, both orally and in writing, knowledge, procedures, results and ideas related to the life cycle of the data, cybersecurity, and development and operations.

BASIC

M_CB7 - To know how to apply the acquired knowledge and competencies and the ability to solve problems in new or unfamiliar contexts within wider (or multidisciplinary) environments related to their field of study

M_CB9 - To share knowledge, conclusions and their rationale with specialised and lay audiences in a clear, unambiguous manner

LEARNING RESULTS

RA211 The student is capable of analyzing, evaluating and selecting appropriate security measures to ensure the confidentiality, integrity and availability of information in different environments

LEARNING ACTIVITIES

	CH	NCH	TH
Development and writing of records, reports, presentations, audiovisual material, etc. on projects/work experience/challenges/case studies/experimental investigations carried out individually and/or in teams		15 h.	15 h.
Conducting tests, giving presentations, presenting defences, taking examinations and/or doing checkpoints	2 h.	12 h.	14 h.
Presentation by the teacher in the classroom, in participatory classes, of concepts and procedures associated with the subjects	12 h.		12 h.
Carrying out exercises and solving problems individually and/or in teams	7 h.	12 h.	19 h.

EVALUATION SYSTEM

	W
Reports on the completion of exercises, case studies, computer exercises, simulation exercises, laboratory exercises, term projects, challenges and problems	40%
Individual written and/or oral tests or individual coding/programming tests	60%

MAKE-UP MECHANISMS

Individual written and/or oral tests or individual coding/programming tests

CH - Class hours: 21 h.

NCH - Non-class hours: 39 h.

TH - Total hours: 60 h.

RA212 The student obtains a thorough understanding of existing security threats, as well as their impact on operations

LEARNING ACTIVITIES	CH	NCH	TH
Development and writing of records, reports, presentations, audiovisual material, etc. on projects/work experience/challenges/case studies/experimental investigations carried out individually and/or in teams		7 h.	7 h.
Conducting tests, giving presentations, presenting defences, taking examinations and/or doing checkpoints	2 h.	3 h.	5 h.
Presentation by the teacher in the classroom, in participatory classes, of concepts and procedures associated with the subjects	5 h.		5 h.
Carrying out exercises and solving problems individually and/or in teams		8 h.	8 h.
EVALUATION SYSTEM	W	MAKE-UP MECHANISMS	
Individual written and/or oral tests or individual coding/programming tests	100%	Individual written and/or oral tests or individual coding/programming tests	

CH - Class hours: 7 h.
NCH - Non-class hours: 18 h.
TH - Total hours: 25 h.

RA213 The student is able to identify, design and implement security mechanisms, individually and in groups

LEARNING ACTIVITIES	CH	NCH	TH
Development and writing of records, reports, presentations, audiovisual material, etc. on projects/work experience/challenges/case studies/experimental investigations carried out individually and/or in teams	16 h.	15 h.	31 h.
Presentation by the teacher in the classroom, in participatory classes, of concepts and procedures associated with the subjects	13 h.		13 h.
Carrying out exercises and solving problems individually and/or in teams	7 h.	14 h.	21 h.
EVALUATION SYSTEM	W	MAKE-UP MECHANISMS	
Reports on the completion of exercises, case studies, computer exercises, simulation exercises, laboratory exercises, term projects, challenges and problems	40%	Reports on the completion of exercises, case studies, computer exercises, simulation exercises, laboratory exercises, term projects, challenges and problems	
Presentation and defence of exercises, case studies, computer practical work, simulation practical work, laboratory practical work, term projects, end of degree project, master's thesis, challenges and problems	60%		

CH - Class hours: 36 h.
NCH - Non-class hours: 29 h.
TH - Total hours: 65 h.

CONTENTS

1. Introduction
2. Cryptography
3. Node Security
4. Network Security
 1. Network Protocol Security
 2. Firewalls
 3. VPNs
 4. User identification
5. Attack detection
 1. Signature-based detection
 2. Anomaly detection systems
 3. Attack response

-
4. Intrusion/Anomaly detection in industrial environments
 5. SIEM and log analysis

LEARNING RESOURCES AND BIBLIOGRAPHY

Learning resources

Subject notes
Moodle Platform

Bibliography

http://katalogoa.mondragon.edu/janium-bin/janium_login_opac_re_Ink.pl?grupo=MASTERDATUANALISIA11&ejecuta=20&