ΔΙΠΑΕ CYQAA

ΦΟΡΕΑΣ ΔΙΑΣΦΑΛΙΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΗΣ ΑΝΩΤΕΡΗΣ ΕΚΠΑΙΔΕΥΣΗΣ

CYPRUS AGENCY OF QUALITY ASSURANCE AND ACCREDITATION IN HIGHER EDUCATION

eqar//// enqa.

Doc. 300.1.2

Higher Education Institution's Response

(Joint – MUNDUS, conventional programme of study)

Date: 24.01.2024

Institution:

European University Cyprus (EUC), Cyprus

District: Nicosia, Cyprus

Title of the programme of study in Greek:

Κοινό Μεταπτυχιακό στην Προηγμένη Κυβερνοασφάλεια (2 Έτη/120 ECTS, Μεταπτυχιακό)

Title of the programme of study in English:
Joint Master's in Advanced Cybersecurity (2 Years/120 ECTS, Master of Science)

Faculty (for universities):
School of Sciences

Department (for universities):
Department of Computer Science and Engineering

Sector (for non-universities):
Private University

Language(s) of instruction: English

Name the concentrations (if any):
In the Greek language: Concentrations
In the English language: Concentrations

Programme status (*check the box where applicable and complete accordingly*):

1. New programme of study: ☒
   1.1. Expected to operate in the Winter/Spring semester of the academic year 2025-2026
2. Currently operating programme of study: ☐
   2.1. Programme title on the last accreditation:
   Click or tap here to enter programme title
   2.2. Reference number: Click or tap here to enter Reference Number
   2.3. Expiry date of the last accreditation: Click or tap to enter date of accreditation
3. Evaluated by CYQAA and did not get accreditation the academic year YYYY
   3.1. Programme title as it was submitted:
   Click or tap here to enter the programme title as it was submitted
   3.2. Reference number: Click or tap here to enter number

Programme category (*check the box where applicable*):

1. Conventional ☒
2. E - Learning ☐
3. Joint (for universities) ☒
   (Name of collaborating university/ies)
   Click or tap here to enter collaborating university/ies

The present document has been prepared within the framework of the authority and competencies of the Cyprus Agency of Quality Assurance and Accreditation in Higher Education, according to the provisions of the "Quality Assurance and Accreditation of Higher Education and the Establishment and Operation of an Agency on Related Matters Laws" of 2015 to 2021 [L.136(I)/2015 – L.132(I)/2021].

A. Guidelines on content and structure of the report

- *The Higher Education Institution (HEI) based on the External Evaluation Committee's (EEC's) evaluation report (Doc.300.1.1 or 300.1.1/1 or 300.1.1/2 or 300.1.1/3 or 300.1.1/4) must justify whether actions have been taken in improving the quality of the programme of study in each assessment area. The answers' documentation should be brief and accurate and supported by the relevant documentation. Referral to annexes should be made only when necessary.*

- *In particular, under each assessment area and by using the 2nd column of each table, the HEI must respond on the following:*

  - *the areas of improvement and recommendations of the EEC*
  - *the conclusions and final remarks noted by the EEC*

- *The institution should respond to the EEC comments, in the designated area next each comment. The comments of the EEC should be copied from the EEC report **without any interference** in the content.*

- *In case of annexes, those should be attached and sent on separate document(s). Each document should be in *.pdf format and named as annex1, annex2, etc.*

1. Study programme and study programme's design and development

(ESG 1.1, 1.2, 1.7, 1.8, 1.9)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. The EEC strongly recommends keeping students fully informed about the number of lectures, readings and learning activities, along with the expected study time, to help them plan their studies. This information should be included in both the study guides and the student handbook for easy access.	We thank the EEC for their valuable feedback and recommendations regarding our Joint Master in Advanced Cybersecurity programme of study during the recent accreditation team visit. We appreciate the insights provided by the EEC and acknowledge the importance of keeping students fully informed about the program's components and expectations. According to the European Education and Culture Executive Agency (EACEA) this information needs to be finalized and issued during the preparatory period provided after a successful EMJM project (max. 1 year – dedicated to preparatory activities as provisioned here slide 13). Please also see below our latest communication with EACEA, where it is pointed out that during this preparatory period partners based on the recommendations of the funding body will need to "prepare the first call for applications of students via your project website: Student selection must be organised transparently, impartially and equitably. The results of the selection will need to be communicated through the project specific EACEA mobility tool at latest end of April 2025 to the Agency".	Choose level of compliance:

	In more specific to this EEC insightful recommendation to enhance communication with students regarding the number of lectures, readings, and learning activities, along with the expected study time, we are committed to implementing the following actions during the timeframe above: – **Revision of Study Guides and Student Handbook:** thoroughly review and update our course outlines and develop a Student Handbook per study Track, to incorporate detailed information about the number of lectures, required readings, and various learning activities associated with each course within the programme of study. This information will be presented in a clear and accessible format to facilitate easy reference for our students. – **Transparency in Curriculum Documentation:** To ensure transparency, to provide a breakdown of the expected study time for each component, taking into consideration lectures, individual study, group work, and any additional activities. This breakdown will offer students a comprehensive understanding of the time commitment required for successful completion of the program. – **Regular Communication Channels:** As mentioned	

	during the EEC site visit, we will establish and maintain regular communication channels, such as a centralized maintained website, and a dedicated space on the LMS, to keep students informed of any updates or events, ensuring they have the latest information about the programme of study. The LMS will also act as a point for students to socialize and exchange ideas and experiences. – **Orientation Sessions for New Students:** During the orientation sessions for new students, emphasis will be placed on the importance of understanding the Study Guides and Student Handbook, providing guidance on how to effectively plan their studies based on the information provided.	
2. There is considerable variation in workload across different courses, with ECTS ranging from 1 to 10. Consequently, tracks of 120 ECTS comprise a varying number of courses, from 12 to 18, plus the master's thesis. This variation arises from the differing standards employed by HEIs in breaking down learning outcomes into efforts required for individual courses. Students will need to be guided to make sure they allocate an appropriate amount of time to courses with differing ETCS values. We note that some work may be required to validate the relationship between ETCS and	We appreciate the EEC's attention to detailing and understanding the challenges associated with varying ECTS values. In response to the EEC's comments, we would like to assure the Committee that we recognize the importance of **providing clear guidance to students** on managing their time effectively, considering the differences in ECTS values for individual courses. To address this concern, and recognizing the varying ECTS values, in the timeframe expected by the	Choose level of compliance:

actual/perceived student workload across the consortium.	EACEA, we will develop comprehensive guidance materials (please also see response on item 1 above) to assist students in understanding and allocating an appropriate amount of time to courses with differing ECTS values. This guidance will be incorporated into the Study Handbook and orientation materials to enhance students' awareness and planning. As noted by the EEC, a thorough **review and validation** of the relationship between ECTS and actual/perceived student workload will be conducted across the consortium. This process will involve collecting feedback from students, faculty, and relevant stakeholders to ensure that the ECTS values accurately reflect the time commitment required for each course. This will only be possible after we run the Joint Master programme of study for the first full cycle so that we can have a clear picture of the feedback from both first year and second year students from each Track. We are also committed to implementing a **continuous monitoring** and an **iterative improvement process** to address any discrepancies identified by students’ feedback. This iterative approach will involve regular reviews and adjustments to maintain alignment with best practices.	
3. There are areas in which the course might develop new	The EEC’s observation regarding potential areas for	Choose level of compliance:

opportunities for added value beyond those already addressed during the site visit. For instance, there was little discussion about how stakeholders both from industry and government in different countries might inform and support the work in other partner countries – providing international experience of new and emerging cyber threats or mitigations.	further development, particularly in engaging stakeholders from industry and government across different partner countries, is well-received. In response to the EEC's recommendation, we are committed to exploring and implementing initiatives that enhance international collaboration and provide valuable experiences related to emerging cyber threats and mitigations. Thus, we will actively pursue collaborations with industry and government stakeholders from different countries to foster a robust network of expertise. This will involve **engaging these stakeholders in advisory roles** (through the Industrial Advisory Board), allowing them to contribute their insights and experiences to inform and support the work across partner countries. To enrich the educational experience of students, we will **incorporate international perspectives** on cyber threats and mitigations into our curriculum. This will include guest lectures, case studies, and real-world scenarios shared by stakeholders from various regions, providing students with a broader understanding of global cybersecurity challenges. This was also discussed during EEC's site visit.	
4. We note that some of the public information necessary to promote the course has still to be	We confirm the EEC's comment, and indeed all public material which will be developed, will be published through a worked	Choose level of compliance:

developed once Lot 1 funding has been secured.	website under the EMDM funding received. We commit to augmenting the website with public information to enhance visibility, transparency, and accessibility. Specifically, the website will feature Study Guides for each study track, community channels, orientation details, templates for student agreements, information on common services provided to students, administrative details from each partner HEI, and other event publications, as detailed in point 1.1 above.	

2. Student – centred learning, teaching and assessment

(ESG 1.3)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. Given the heterogeneity of learning activities and assessment structures across tracks and courses, which arise from different standards set by national accreditation agencies and the HEIs, the EEC suggests including clear, detailed assessment information in the student handbook to prevent confusion. Optional non-graded formative self-assessment tasks with indicative answers could be provided in the study guides, assisting students in self-assessing their understanding and competencies.	The EEC's suggestion to enhance clarity through detailed assessment information in the student handbook and the inclusion of optional non-graded formative self-assessment tasks is duly noted. As stated in item 1.1 above, a **comprehensive Student Handbook** will be compiled to include clear and detailed assessment information for each track and course within the programme of study. This will provide students with a comprehensive understanding of the assessment structures, criteria, and expectations, helping to prevent confusion and ensuring consistency. We have also agreed to establish **consistent communication channels** to inform students about assessment standards and practices. This will include orientation sessions, regular updates, and dedicated VLE channels where students can seek clarification on assessment-related matters.	Choose level of compliance:
2. The introduction to the programme states there is a need to support "lifelong learning" in cybersecurity across Europe. The present proposals are naturally focussed on Masters provision for students exiting a recent Undergraduate degree. The Joint-Mundus programme is	In response to these recommendations of the EEC, we recognize the importance of expanding our transnational program to cater to a broader audience, including those seeking part-time learning opportunities and individuals with existing job and family commitments and this	Choose level of compliance:

not structured to support part-time learning nor the distance education that might help those looking to reskill, or to support students with existing jobs/families to support. In the future, the EEC encourages the team to consider these areas for further development.	aligns with the lifelong learning mode. As stated during the site visit, while discussing this topic, it is not possible at this stage to allow part-time studies nor distance education because according to the Erasmus Mundus regulations (website here), during the study period, the scholarship can only be awarded in full, and to full-time students. The scholarship is awarded for full-time enrolment and will cover the entire duration of the Master programme. However, as soon as the Erasmus Mundus Joint master project is over, and there will be no scholarships awarded by the EACEA, we will explore and develop structures within the Joint Mundus program that **accommodate part-time learning** for self-funded students, for the sustainability of the programme as well. This may involve designing flexible schedules for students taking lower burden of ECTS per semester, evening classes, or weekend sessions to cater to individuals who wish to pursue the program while balancing other commitments. Recognizing the significance of E-Learning/Distance Education, we will investigate the feasibility of **incorporating E-Learning components** into the program in the degree that the Erasmus Mundus Joint master will allow the consortium. This could involve the use of online platforms, virtual classrooms, and asynchronous	

	learning opportunities to provide accessibility to a wider audience.	
3. There are considerable opportunities to involve students in wider research programmes – although this was addressed in passing during the visit, the EEC would welcome further consideration of research-led teaching as the course develops.	We will actively provide opportunities for **students to engage in wider research programs** as the programme evolves. This may involve collaborations with research centers (all partners have very well structured and reputable research centers in place), industry partners, and relevant institutions to provide students with hands-on experience in cutting-edge cybersecurity research. We will therefore systematically review and enhance the courses to **include dedicated research components**, ensuring that students have the opportunity to apply theoretical knowledge to real-world challenges. This may involve the inclusion of research-focused projects, case studies, and opportunities for collaboration with faculty members on ongoing research initiatives. In addition, we will actively encourage and support students to participate in **research conferences and contribute to publications** in the field. This exposure will not only enhance their research skills but also contribute to the broader academic community, and will prepare them for the Master Thesis compulsory component in each study track.	Choose level of compliance:
4. Student assessment is noted as partially compliant based on the need to provide assurances of appropriate	In response to the EEC's comment, it's important to note that all consortium partners adhere to the educational	Choose level of compliance:

formative assessment at partners where a final exam forms the predominant mode of assessment.	standards of their respective countries. For instance, in the Italian system followed by POLIMI in Italy, courses typically undergo evaluation through a single final exam. This exam is made available multiple times throughout the year, providing students with the flexibility to choose the most suitable examination period. After completing the exam, students have the opportunity to engage in a feedback session with the instructor. This post-exam discussion allows students to gain insights into their performance, seek clarification on challenging topics, and understand any mistakes made during the assessment. Furthermore, the iterative nature of the exam process enables students to improve their scores by retaking the exam if they wish to enhance their understanding of the material or aim for a higher grade. This approach aligns with the educational practices within the Italian system, emphasizing continuous learning and improvement.	

3. Teaching staff

(ESG 1.5)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. The EEC suggests creating a handbook for faculty staff with clear guidelines to ensure a homogeneous, common view of teaching practices across the different courses. The EEC welcomes the proposals for student handbooks and for handbooks on administrative practice across the partner sites.	We appreciate the EEC's constructive feedback regarding the need for a Faculty Handbook. The suggestion aligns with our commitment to excellence and consistency in teaching and learning practices. We will therefore initiate in the timeframe of the year provided for preparatory activities, the development of a **comprehensive Faculty Handbook** that outlines clear guidelines for teaching practices. This handbook will serve as a reference for faculty members across partner institutions, promoting a common understanding of teaching methodologies, assessment practices, and pedagogical approaches. Recognizing the importance of **collaborative input**, the faculty members from different partner sites will be involved in the creation of the handbook. This collaborative effort will ensure that the handbook reflects the diverse expertise and experiences within our academic community and echoes the different pedagogical models used in the partner HEIs.	Choose level of compliance:
2. As the course develops, the EEC recommends one central resource for administrative information across the network. We note that the partners use very different platforms for content delivery and management (Blackboard, Sakai, Canvas, Moodle, etc).	In response to the EEC recommendation, a **central resource for administrative information** accessible to students across all partner HEIs will be available. This resource will serve as a unified point of reference, providing consistent and up-to-date	Choose level of compliance:

This is entirely appropriate. There is little prospect of getting all partner HEIs to agree on a common platform. However, students across each HEI will need a single point of reference for some administrative information and if each node duplicates these details, then there is a possibility for confusions and inconsistency. A simple approach might be to link from each on-line environment to a single pdf handbook. This would still enable each site to maintain course specific information.	information on administrative matters. To streamline access and avoid duplication, a **single PDF handbook of administrative details** will be created. This handbook will be linked to each partner's online environment, ensuring that students have easy access to essential administrative details while allowing each site to maintain course-specific information. We commit to regular updates and maintenance of the central resource and the linked PDF handbook to ensure that students receive the most accurate and current administrative information. This approach will help minimize confusion and maintain consistency across the network. The Administrative Handbooks (per study track) will be uploaded on the project website and students will have continuous access to them. Further, each partner HEI will facilitate the integration of the central resource and the linked PDF handbook into their respective online environments. This collaborative effort will ensure a seamless user experience for students.	
3. There are opportunities to link material on similar topics taught be different HEIs – so that students can see more than one perspective. It is unclear how this might be supported across the different learning environments. However, short podcasts or videos might be produced by different staff working on common topics to stimulate debate and motivate students	In the timeframe of the year provided for preparatory activities, , we will produce some short podcasts or videos, or even live debates organized between HEIs teaching the same or similar topics. Then the material will be posted in the VLEs of the HEIs involved. This approach will expose students to various viewpoints, fostering a deeper understanding of the subject matter and stimulating debate.	Choose level of compliance:

beyond what is possible from any single HEI.		
4. The EEC would welcome target information about Staff-Student-Ratios across the partners especially where the proposed courses are shared with other programmes not considered in this evaluation.	As soon as the programme initiates and we have the first two years completed, we will compile and provide target Staff-Student Ratios for each partner institution, especially in instances where the proposed courses are shared with other programs.	Choose level of compliance:
5. As noted in the previous sections, the EEC were provided with outline details about the way research will inform teaching, but further details would be welcome for instance to demonstrate that the research strengths of each partner are well aligned to the material they will be delivering to the students on each track.	A **detailed mapping of the research strengths** of each partner institution to the material delivered in the study tracks has been developed. This mapping highlights the direct connections between the expertise of faculty members and the content covered in the courses, ensuring a clear alignment. Please refer to ANNEX III for the detailed mapping of research strengths per partner.	Choose level of compliance:

4. Student admission, progression, recognition and certification *(ESG 1.4)*

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. The EEC suggests that the student handbook should include common regulations on plagiarism and other forms of academic fraud, ensuring clear rules as students transition between different HEIs.	We acknowledge the importance of ensuring clear and consistent rules for students as they transition between different HEIs within our Joint Master in Advanced Cybersecurity programme of study. All partner HEIs of the consortium will collaborate in the timeframe of the year provided for preparatory activities, to develop **common regulations on plagiarism and academic fraud**. These regulations will be designed to provide students with a standardized understanding of academic integrity, regardless of the institution they are attending. The common regulations on plagiarism and academic fraud will be incorporated into the Student handbook. The Student Handbook will clearly outline the consequences of plagiarism and academic fraud. This includes details on disciplinary actions that may be taken in case of violations. Providing this information upfront will emphasize the significance of academic integrity. During orientation sessions for new students, the importance of academic integrity will be emphasized and students will be provided detailed explanations of the common regulations on plagiarism and academic fraud. This proactive approach will help students understand and adhere to the established guidelines from the outset.	Choose level of compliance:
2. Plans to gather evidence of effectiveness of student monitoring and feedback were not demonstrated during the evaluation. Measures must assess the value of specific improvement	Indeed, a **feedback mechanism** will be implemented that allows students to express their thoughts on the clarity and usefulness of the provided information. This will help us continuously improve our communication strategies.	Choose level of compliance:

measures and action plans taken by the HEIs This particularly applies across the different tracks, contributing to a unified approach for the continuous improvement cycle of the joint program. is important not simply to identify problems in progression but also for continuing to assess the effectiveness of any interventions or changes that might then be put in place to support the students going forward.	In addition, the consortium will develop and implement specific strategies for gathering evidence on the effectiveness of student monitoring and feedback. This may include regular surveys, focus group discussions, and feedback sessions to collect quantitative and qualitative data on students' experiences and perceptions. Our approach will include a comprehensive assessment of specific improvement measures and action plans implemented by HEIs across different tracks. This assessment aims to gauge the impact of interventions and changes on student progression and overall satisfaction. Recognizing the importance of a unified approach, the consortium will establish mechanisms for sharing best practices and lessons learned across partner HEIs. This collaborative effort will contribute to a continuous improvement cycle, ensuring that successful strategies are implemented consistently. The evaluation will extend beyond identifying problems in student progression. The focus will be on assessing the effectiveness of interventions and changes, with a particular emphasis on understanding how these measures support students in their academic journey. The consortium is committed to adopting a data-driven decision-making process. The evidence gathered will inform strategic decisions related to student support, allowing for targeted interventions and adjustments based on the identified needs and challenges. The consortium will maintain transparent communication with stakeholders, including faculty, and students sharing findings from the assessment of student monitoring and feedback effectiveness. This open dialogue ensures ongoing collaboration and informed decision-making.	

3. The EEC notes that the HEIs should agree on a common approach to supporting students socially, especially online. The students must adapt to a variety of online platforms. This reduces their opportunities for connections with others. A common online platform could be easily set up for all students in this Joint-Mundus program, providing basic support for communication and experience sharing. We also note that the development of a common social on-line community will promote self-help between students – where those in year 2 on a track can provide advice and support to the new year 1 cohort.	As mentioned during the EEC site visit, the consortium will establish and maintain **regular communication channels**, such as: 1) a centralized maintained website, 2) a common social online community, and 3) a common informative online platform for all students in the Joint Erasmus Mundus program, to keep students informed of any updates or events, ensuring they have the latest information about the programme of study. The LMS will also act as a point for students to socialize and exchange ideas and experiences. The **common online platform** will provide basic support for communication, ensuring that students have easy access to essential information, announcements, and opportunities for interaction. In the consortium we will actively promote social interaction within the **common social online community**, facilitating opportunities for students to connect, engage, and share experiences. This approach aims to enhance the sense of community and support the social well-being of our students. It will also encourage peer support and mentorship and students in advanced stages of the program may provide valuable advice and support to new cohorts, fostering a culture of self-help and collaborative learning. During orientation sessions, students will be introduced to the common online administrative platform, the social online community emphasizing its features and benefits for social connection. This will ensure that students are familiar with the various online platforms from the beginning of their academic journey.	Choose level of compliance:
4. The EEC note that many of the activities and innovations are staff led. Once the course goes 'live' the EEC would encourage the	In response to the EEC's comment, we would like to highlight the existing framework within our programme of study that contains: • **Dedicated Cybersecurity Labs:**	Choose level of compliance:

development of student-led support initiatives. The partners described a range of existing activities within each site but there would also be more creative possibilities for student-led projects a cross borders – for instance, “capture the flag” exercises in which students from one partner attempts to compromise the defences created by another. ENISA and NATO both have examples of these exercises as a means of developing cyber skills.	Our Joint Master program incorporates dedicated cybersecurity labs, such as the Cybersecurity Lab (EMC225, EMC325, EMC425) at UMU and an additional CyberSecurity Lab II element (EMC331) at ELTE within their study track. These labs serve as spaces for the development of student-led initiatives, including projects oriented around activities like "Capture the Flag," pen testing exercises, and Cybersecurity Hackathons. "Capture the flag" virtual / hybrid games can be implemented within the "Brno University of Technology Cyber Arena", which is a platforme developed by BUT (https://www.utko.fekt.vut.cz/en/butca-cyber-arena). This platform is also included and used in all BUT cyber security courses. • **Integrated Exercises and Academic Coordination:** The academic design of our program emphasizes coordination between courses to enhance the integration of exercises. This ensures that the practical outcomes of certain courses can seamlessly continue into subsequent ones, providing students with a holistic and interconnected learning experience. • **Summer Schools and External Activities:** To further enrich student activities, we actively encourage participation in external events and programs. For instance, our students have the opportunity to engage in summer schools and events like Cybercamp (https://www.incibe.es/eventos/cybercamp). Notably, UMU takes charge of coordinating activities for the region of Murcia in such events. • **Collaboration with ENISA and NATO Initiatives:** In the spirit of fostering creativity and practical skill development, we are exploring opportunities to collaborate with	

	initiatives led by ENISA and NATO. "Capture the Flag" exercises, inspired by successful examples from these organizations, are envisioned as part of our student-led projects. We are committed to continually enhancing the student experience through innovative, collaborative, and hands-on activities.	
5. The EEC would welcome some discussion as to whether the relationship with ENISA profiles will be sufficient to gain certification in each of the member states involved in this proposal; given that security is a national prerogative across Europe.	ENISA's profiles serve as guidelines for potential profiles. These guidelines were thoroughly considered when structuring the syllabi for our Joint Master's programme of study. However, it's important to note that they do not exert any influence over national accreditation systems; rather, they function as useful guidelines. The consortium's primary goal in incorporating ENISA profiles is to showcase that students will acquire skills, knowledge and capabilities aligned with the profiles outlined by ENISA, as well as with the European job market needs, as identified by ENISA while preparing the European Cybersecurity Skills Framework (ECSF). .	Choose level of compliance:

5. Learning resources and student support
(ESG 1.6)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. Despite the availability of resources, a significant continuity problem exists when students transition between HEIs. They lose access to the previous HEI's facilities, including software licenses, data, assignments, and course content, creating inconvenience and potential disruption in their learning process. Ensuring this data portability and access across HEIs would be a significant enhancement to this joint experience. There is a need to consider the continuing "digital identity" of the student both while they are studying and after graduation – providing continued access to material for alumni will enhance opportunities for student-led and self-help initiatives.	The partner HEIs will work collaboratively to develop and implement data portability policies. These policies will focus on ensuring seamless access to essential resources, including software licenses, data, assignments, and course content, as students transition between institutions. During the site visit we have discussed with the EEC the option of establishing a unified access platform that enables students to retain access to the necessary facilities and materials irrespective of the HEI they are currently enrolled in. While this option would facilitate a smooth transition and minimize disruption in the learning process, it was said that it is not possible, mainly because each HEI uses its own student platforms which are interoperable with the rest of the software used in each HEIs (e.g. registration system, admissions, customer resource management, etc.). Yet, recognizing the importance of a student's digital identity, the consortium will develop strategies to preserve and maintain their access to the first year HEI (even if they have moved to second year) and to relevant materials even after graduation. This initiative aims to empower alumni with ongoing opportunities for self-help initiatives and continuous learning.	Choose level of compliance:

	All information and policies regarding the data portability and access procedures will be incorporated into orientation sessions and will be readily available in Student Handbooks (posted both on the website and the common online administrative platform) to ensure awareness and understanding.	
2. The EEC notes that some required readings consist of entire volumes, which may not be practical for students needing to study efficiently. Some of the HEIs use a curriculum builder that helps staff form reading lists in a more flexible manner. This is to be commended.	The consortium will explore the option of using a curriculum builder like Leganto that seamlessly integrates with popular Learning Management Systems, such as Blackboard, Canvas, and Moodle. This integration allows for a smooth flow of information between the curriculum builder tool and the LMS used by the institution. The consortium has also conducted some changes in the course syllabi as indicated in Annex Iand Annex II, in an effort to indicate which particular chapters from each required textbook should be studied.	Choose level of compliance:
3. Where course reading is set as an entire book, the EEC recommend that staff provide clear guidance to students on the relevant sections of these volumes, along with the recommended study time. This will direct students and help them plan their study effectively.	The consortium has now conducted a comprehensive review of required readings to ensure that the selected materials are essential, relevant, and conducive to efficient study. This review process involved collaboration among faculty members to curate reading lists that balance depth of content with practicality. All changes are highlighted in Annex II.	Choose level of compliance:
4. This course will develop a cohort of students with advanced cybersecurity skills and there is, therefore, a need for all HEIs to regularly review the security of their systems.	In the timeframe of the year provided for preparatory activities, all partner HEIs will work collaboratively to develop a comprehensive **'code of conduct'** that addresses ethical hacking and	Choose level of compliance:

We encourage all HEIs to agree a 'code of conduct' that addresses topics such as 'ethical hacking' of the HEI systems. Plans should be put in place to address any compromise of the systems and networks used by this cohort of students. These plans should be exercised through drills that may also involve the students.	outlines guidelines for responsible behavior when interacting with HEI systems. This code will serve as a foundation for ensuring a secure and ethical cybersecurity learning environment. Recognizing the dynamic nature of cybersecurity threats, the consortium commits to conducting **regular security reviews of systems and networks** used by our cohort of students. The consortium will also ensure that it provides an isolated network for them to experiment with. These reviews will be carried out collaboratively among partner HEIs to share best practices and ensure a consistently high level of security across the consortium. Comprehensive **incident response plans** will be developed to address any compromise of systems and networks. These plans will outline the steps to be taken in the event of a security incident, including communication protocols, mitigation strategies, and responsibilities of relevant stakeholders. We endorse the suggestion to involve students in **cybersecurity drills**. These exercises will not only test the effectiveness of incident response plans but will also provide students with hands-on experience in dealing with real-world cybersecurity scenarios. This practical exposure is invaluable for their skill development. Security drills will be conducted regularly, involving both faculty and students. These drills will simulate various cybersecurity incidents,	

	allowing participants to practice response procedures and identify areas for improvement. The outcomes of these drills will inform ongoing enhancements to our security protocols. Further to the above, **ongoing training and educational programs** will be implemented to keep both faculty and students abreast of the latest cybersecurity threats and best practices. This proactive approach ensures a well-informed community capable of responding effectively to emerging challenges.	
5. Just as the EEC would welcome clarity over the teaching staff-student ratios, the February proposal for Lot 1 funding might also benefit from details about the administrative and support staff-student ratios in each node	Upon implementation of the program, the consortium will compile detailed data on administrative and support staff-student ratios at each node within our program. This information will be gathered in collaboration with partner HEIs to ensure accuracy and consistency.	Choose level of compliance:

6. Additional for doctoral programmes

(ALL ESG)

N/A

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
Click or tap here to enter text.	Click or tap here to enter text.	Choose level of compliance:
Click or tap here to enter text.	Click or tap here to enter text.	Choose level of compliance:
Click or tap here to enter text.	Click or tap here to enter text.	Choose level of compliance:
Click or tap here to enter text.	Click or tap here to enter text.	Choose level of compliance:
Click or tap here to enter text.	Click or tap here to enter text.	Choose level of compliance:

7. Eligibility (Joint programme)
(ALL ESG)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. The existing courses run across the HEIs are not in cyber security – nor does it seem many are in software or computer networks. Hence, there may be a need to consider in more detail the provision of electronic resources and "digital identity" that represent new opportunities for value added across the HEIs.	ELTE as a partner institution will provide a mix of applied data science and cybersecurity courses which were selected as most applicable towards obtaining the skills needed by professionals in the broad "Security Analyst" job profile. The applied data science courses are not specifically security-oriented, but needed to perform the day-to-day tasks of most security analysts. Also in regards to the BUT course "Parallel Data Processing", while the Parallel Data Processing course primarily focuses on data analysis and parallel computing, the skills and knowledge gained are fundamental in cybersecurity contexts. • Data Security: Apache Spark and other parallel technologies are widely used in big data analytics, specifically in security analytics, threat detection, and anomaly detection, which are integral components of cybersecurity. • Data Privacy: Data operations such as aggregation, classification, regression, and clustering are components of data privacy, i.e., Statistical Disclosure Control techniques such as microaggregation and general recording methods. • Applied Cryptography: Parallelization is used as an optimization technique that needs to be well-known to avoid encountering security bugs. This understanding is crucial	Choose level of compliance:

	when implementing cryptographic algorithms in a parallelized environment, ensuring their efficiency and security.	
2. It is also crucial to align the programme's curriculum with industry demands and promote the development of cybersecurity skills that are in high demand.	We agree with the EEC's recommendation and we have already provisioned to establish and maintain strong connections with industry partners to stay abreast of the latest developments, emerging trends, and evolving skill requirements in the cybersecurity field. Forming and running the Industrial Advisory Board comprising of industry experts and professionals who can provide valuable insights into current industry demands. Their input has guided curriculum development to ensure its relevance and alignment with real-world needs, and will still continue to do so, since implementing a continuous review process for the program's curriculum is vital, in order to incorporate timely updates based on industry feedback, technological advancements, and changes in the cybersecurity landscape. Enhancing the program's focus on practical, hands-on skills directly translate to the demands of the cybersecurity industry. This will include incorporating practical exercises, labs, and real-world case studies into the curriculum. In the event that Erasmus Mundus Joint Master (EMJM) Lot 1 proposal is successful, we will facilitate internship and industry placement opportunities for students to gain practical experience, network with	Choose level of compliance:

	professionals, and apply their skills in real-world settings. Encouraging collaboration with cybersecurity professionals through guest lectures, workshops, and joint projects, has been provisioned. This exposure will provide students with insights into industry best practices and challenges. Lastly, we will establish a feedback mechanism that solicits input from industry partners, alumni, and employers to assess the effectiveness of the program in meeting industry demands. This feedback will drive continuous improvement efforts.	

B. Conclusions and final remarks

Conclusions and final remarks **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1. Overall, we find: - that they have an open international mind-set (e.g. Erasmus exchange focused on cybersecurity); - high quality and capable of satisfying demand for professionals with appropriate qualification in accordance with the development needs of modern western economies and the trends of the global education market; - contributions to the individual student's personality growth and social development; - a contemporary education approach that meets the demands of the cybersecurity market and promotes the transformation of the (national) economy by focusing on the development of cybersecurity competencies, skills and creativity needed. - Reviewing, assessing and appraising the course, we find they are in overall compliance and are to be recognized in the delivery of programmes demonstrating an efficient and effective approach to the core business and the continuous improvement thereof.	We express our sincere gratitude to the EEC for the comprehensive review of our Joint Master in Advanced Cybersecurity programme of study. The EEC's valuable insights and positive observations affirm our commitment to delivering a programme that meets the evolving demands of the cybersecurity landscape and contributes to the professional growth of our students. We appreciate the recognition of the following key strengths in our programme and in particular the EEC's acknowledgment of our programme's open international mindset, exemplified by initiatives, such as the Erasmus exchange focused on cybersecurity, validates our commitment to providing a global perspective in cybersecurity education. The recognition of our programme as high quality and capable of satisfying the demand for cybersecurity professionals aligns with the consortium's dedication to delivering a curriculum that meets the needs of current EU economies and the global education market.	Choose level of compliance:

	The acknowledgment of our programme's contributions to individual student personality growth and social development reflects our holistic approach to education, ensuring that students not only acquire technical and practical skills but also develop personally and socially. The EEC's positive assessment of our contemporary education approach that meets the demands of the cybersecurity market and promotes the transformation of the EU economy is a testament to our commitment to staying current with industry trends and fostering creativity and innovation. All partner HEIs taking part in this Joint Master programme of study, are grateful for the recognition of our programme's overall compliance and efficiency in delivering programmes of study.	

C. Higher Education Institution academic representatives

Name	***Position***	***Signature***
Dr. Yianna Danidou	Program Coordinator	Yianna Danidou
Dr. Ioannis Michos	Chairperson, Department of Computer Science and Engineering	Ioannis Michos Ioannis Michos (Jan 25, 2024 16:01 GMT+2)
Prof. Panagiotis Papageorgis	Dean, School of Sciences	Panagiotis Papageorgis Panagiotis Papageorgis (Jan 25, 2024 15:55 GMT+2)

Date: 24/1/2024

European University Cyprus

ANNEXES 1 & 2

ANNEX 2

<table>
<tr><td>Course Title</td><td colspan="5">Introduction to Cybersecurity</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC111</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 1st Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Yianna Danidou</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces the fundamental concepts and terminology of cybersecurity as a whole, and functions as a short introduction to the large number of cybersecurity topics that are covered within this MSc programme.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon succesful completion of this course students should be able to:
• Describe the meaning and position of fundamental cybersecurity concepts and terminology
• Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model
• Classify and describe different cybersecurity components and how they contribute to effective defence
• Classify and describe different potential routes for cyber attacks.
• Recognise the importance and application of IT law and cybersecurity certification</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>None</td></tr>
</table>

Course Content	Introduction: Refresh on fundamental networking principles and devices and distributed systems, the context within which cybersecurity (or lack thereof) can be present. Network structure and ways of communication. History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.) Current importance of cybersecurity, given the connectedness of most of our daily lives. Analysis of critical infrastructures and the position of critical information infrastructures within these – importance of the protection of such systems for the smooth operation of essential services in all areas of life. The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Asset protection (including data) as a valuable business operation and its contribution to business survivability. Main principles of cybersecurity – confidentiality, integrity, availability and combinations thereof, resulting in other important cybersecurity concepts and services – accountability, non-repudiation, authenticity, resilience, business continuity and disaster recovery, audit, cybercrime, data / system / network forensics, cyberdefence. Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover. Applicable cybersecurity and IT law Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust. Introduction to ISO/IEC 27001 Information security management. Introduction to other courses in this MSc (to aid selection of the elective courses). Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*“Introduction to Computer Networks and Cybersecurity”,* by Chwan-Hwa (John) Wu and J. David Irwin *“Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover”*, by Lee Mark Zeichner

	“Management of Information Security” by Michael E. Whitman, Herbert J. Mattord “CISSP Guide to Security Essentials” By Peter Gregory “Principles of Information Security” by Michael E. Whitman, Herbert J. Mattord *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines* (ISC)^2, ISACA, and other cybersecurity websites
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Communications and Network Security</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC112</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 1st Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Konstantinos Vavousis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces fundamental concepts of communications and network security, particularly in the context of internal and external threats to the operation of the network and to the devices that are attached to it.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, and separation of duties.
• Explain the basic types of networking device, both logical and physical.
• Differentiate between the various properties of security as they relate to the design of authentication protocols and the use of asymmetric and symmetric cryptography
• Classify and describe the different types of malware, network vulnerabilities and attacks.
• Classify and describe different types of wireless network attacks including sensor networks and Internet of Things (IoT)
• Describe and evaluate methods and devices used to protect networks.
• Compare security mechanisms of Cloud Computing
• Describe the key issues when managing emergencies</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>EMC111</td></tr>
<tr><td>Course Content</td><td colspan="5">Introduction: Refresh on fundamental networking principles and devices, OSI and TCP/IP models. Different types of networking areas – WAN, LAN, MAN, PAN, wireless and mobile systems.

Security Principles: Security Properties, the network as a route for cyberattacks, types of attacks, security mechanisms and services.</td></tr>
</table>

	Threats and Attacks: Threats and vulnerabilities, hardware vs. software vulnerabilities, social engineering, malware types, Network attacks: scanning, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-middle, session takeover, ARP poisoning, ICMP attacks, DNS poisoning, phishing, spam, Security protocols at the various OSI layers: TLS, SSL, IPsec, authentication protocol design based on Asymmetric and Symmetric encryption, Security properties of symmetric and asymmetric encryption, digital signature properties Wireless Network Security: Encryption and key management vulnerabilities, wireless sniffing, war-driving, mobile/cellular cell spoofing, eavesdropping, wireless sensors security, routing attacks, IoT security General protection, prevention and detection: Firewalls and packet filtering, demilitarized zones (DMZ), intrusion detection and prevention systems, IPsec, VLANs and network zoning, authentication, system hardening, encryption, authentication, , honeypots , Cloud computing Disaster and Risk Management: Managing emergencies, factors for quick disaster response Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*“ Computer Networking: A Top-Down Approach (7th Edition), by Jim Kurose and Keith Ross.* *“Guide to Computer Network Security, 4th Edition”, by Joseph Migga Kizza* *“Network Security Essentials: Applications and Standards”, Sixth Edition, by William Stallings* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	EMC113				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Yianna Danidou				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course provides an overview of the broad and constantly emerging field of cybersecurity policy, governance, law and compliance. The importance of the role of security policy is discussed.				
Learning Outcomes	Upon succesful completion of this course, students should be able to: • State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security. • State and interpret the different components of a comprehensive organizational cybersecurity policy. • State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment. • Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function. • Recognize and explain major applicable legislation and regulatory framework (local, European, international). • Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.				
Prerequisites	None	Co-requisites	EMC111		

Course Content	Introduction: Concepts of cybersecurity, its relationship with network and information security, cybercrime, cyberdefence, and related definitions. Concepts of policy, governance, related law and compliance, and the relationships between them. Principles: Information security components and concepts, confidentiality, integrity, availability. Policy: definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures. Governance: Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation. Law: Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations. IT and Law: Introduction, Terminology, and the Nature of Cyberspace and Threats. Cyber-regulation and cyber-regulatory theory. Cyberproperty and Intellectual Property. Cyber-rights, Speech Harm, Crime and Control. Roles of International Law, the State, and the Private Sector in Cyberspace. Authentication and Identity Management. Speech, Privacy and Anonymity in Cyberspace. Trust. Compliance: Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.
Teaching Methodology	Face – to – face
Bibliography	*“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *“Information Security Governance: A Practical Development and Implementation Approach”*, by Krag Brotby

	“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”, by Scott E. Donaldson *“Cyber Security and IT Infrastructure Protection”*, by John R. Vacca *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Cybersecurity Architecture and Operations				
Course Code	EMC121				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Nikos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify the various components of a comprehensive cybersecurity architecture within an organization. • Describe and classify controls that meet specific control objectives and to treat identified risks. • Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc. • Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover. • Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others. • Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control. • Evaluate and select appropriate architectural and operational options according to the organizational risk environment.				
Prerequisites	None	Co-requisites	EMC111		

Course Content	Introduction: Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication. Processes: User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others. Phases: Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover. Identify: Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process. Protect: Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening. Detect: Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicatiors of compromise (IOC). Respond: Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls. Recover: Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes. Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.
Teaching Methodology	Face – to – face
Bibliography	*Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.* *Santos, O., Developing Cybersecurity Programs and Policies. Pearson.*

	“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor) *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker* *ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management* *ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements* *Contreras, J., 2013. Developing a Framework to Improve Critical Infrastructure Cybersecurity (Response to NIST Request for Information Docket No. 130208119-3119-01). SSRN Electronic Journal.* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

<table>
<tr><td>Course Title</td><td colspan="6">Ethical Hacking and Penetration Testing</td></tr>
<tr><td>Course Code</td><td colspan="6">EMC122</td></tr>
<tr><td>Course Type</td><td colspan="6">Compulsory</td></tr>
<tr><td>Level</td><td colspan="6">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="6">1st Year / 2nd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="6">Konstantinos Vavousis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td colspan="2">3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="6">The objective of this course is to provide a detailed introduction into the world of ethical hacking and to understand its usefulness to organizations in practical terms. Hacking concepts, tools and techniques, and countermeasures are covered, along with how penetration testing fits into a comprehensive cybersecurity regime. Beyond the confines of ethical hacking, this course covers aggressive hacking techniques that are essential knowledge for professionals who need to be able to defend against such advanced attacks.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="6">Upon succesful completion of this course students should be able to:
• Define the different types of hacking and its legal and illegal uses in the cybersecurity world
• Identify and evaluate the different type of hacking attacks and how these attacks proceed
• Explain the principles of vulnerability research
• Describe the different phases of ethical hacking and select appropriate techniques depending on the assignment.
• Define, describe and perform the different kinds of penetration testing – black box, grey box, white box.
• Make effective use of penetration testing related tools
• Define which tool is more effective at each step of a penetration testing project</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td colspan="2">EMC111</td></tr>
</table>

Course Content	Introduction: Definition of ethical hacking and penetration testing, position within a comprehensive cybersecurity posture, applicable national and international laws, difference between ethical (white hat), non-ethical (black hat) and grey hat hackers, vulnerability research and zero-day vulnerabilities. Hacking phases: The five phases of hacking – reconnaissance, scanning, gaining access, maintaining access, covering tracks. Reconaissance: Discovery of target information, footprinting, competitive intelligence, social engineering, Google hacking, website footprinting, email tracking Scanning: TCP flags, ping sweeps, connect scans, TCP flag manipulation, SYN scans, IDLE scans, scanning tools, banner grabbing, vulnerability scanning, ip spoofing, enumeration techniques and tools Gaining and maintaining access: password cracking, dictionary attacks, brute force attacks, hashing attacks, privilege escalation, executing applications, malware (viruses, worms, trojans, rootkits, spyware, botnets), lalware detection and anti-malware software, DoS/DDoS, network sniffing, MAC, ARP and DNS attacks, session hijacking, web application attacks, SQL injection, wireless network and mobile device attacks, cryptanalysis and related attacks. Covering tracks: Rootkits, disabling auditing, clearing logs, anonymisers, proxies, hiding files, track covering tools Practical penetration testing: Penetration testing methodology, ethical considerations, assignments and contracts, reporting, relationship to audits and audit techniques. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities and challenges of penetration testing.
Teaching Methodology	Face – to – face
Bibliography	*Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing.* *Harper, A., Regalado, D., Linn, R., Sims, S., Spasojevic, B., Martinez, L., Baucom, M., Eagle, C., & Harris, S. (2018). Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition (5th ed.). McGraw-Hill Education.* *Gaia, J., Ramamurthy, B., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X. and Yoo, C., 2020, January. Psychological Profiling of*

	Hacking Potential. In Proceedings of the 53rd Hawaii International Conference on System Sciences. *“Hacking: The Art of Exploitation, 2nd Edition”, by Jon Erickson* *“Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Cybersecurity Risk Analysis and Management</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC123</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Nikos Tsalis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces the fundamental concepts of cybersecurity risk analysis and management, as well as its position as the foundation for cybersecurity protective mechanisms. It covers a wide range of principles and processes related to risk management and sets the scene for the development of comprehensive cybersecurity controls to protect an organizations assets according to the risk appetite of senior management.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon succesful completion of this course students should be able to:
• Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities
• Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc.
• Recognise the difference between vulnerabilities and threats.
• Classify and describe a number of different risk assessment/management methodologies.
• Classify and describe different assets and their values (including tangible and intangible assets).
• Identify and explain various threat sources and the impacts that their materialization may manifest.
• Describe the risk management process, as it pertains to the protection of assets.
• Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>EMC111</td></tr>
</table>

Course Content	Introduction: Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme. Principles: Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. Assets: Tangible and intangible assets in the cyber world (hardware / software / data, classification, criticality based on the importance and value to organization (not just monetary), dependencies, potential for critical national infrastructure. Vulnerabilities: Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information. Threats: Cyber threat categorization, sources, motivation, type, technical vs. non technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood. Risk analysis: Risk as a combination of possible impact of a threat exploiting a vulnerability and the probability of such an impact occurring, evaluation of cyber risks, categorization, qualitative and quantitative risk analysis, pre-requisites for meaningful quantitative cyber risk assessment, methodologies, risk register. Risk management: Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organisation's environment, building an organisation's cybersecurity control environment from the results of risk analysis, introduction to basic cybersecurity controls. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical uses challenges of risk analysis and management in real environments.
Teaching Methodology	Face – to – face
Bibliography	*"Effective Cybersecurity: A Guide to Using Best Practices and Standards 1st Edition, by Willian Stallings* *"Cyber-Risk Management" by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen*

	Samimi, A., 2020. Risk Management in Information Technology. Progress in Chemical and Biochemical Research, pp.130-134. *“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *Tarek, M., Mohamed, E.K., Hussain, M.M. and Basuony, M.A., 2017. The implication of information technology on the audit profession in developing country. International Journal of Accounting & Information Management.* *“How to Measure Anything in Cybersecurity Risk”*, by Douglas W. Hubbard and Richard Seiersen *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”*, by Anne Kohnke and Dan Shoemaker
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Data Privacy in the era of Data Mining and AI				
Course Code	EMC124				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Nikos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide a comprehensive overview of growing data privacy threats to future communication technologies and Internet of Things (IoT) applications such as the Smart Grid and Smart Cities, e-Health and Wireless Sensor Technologies. Recent advances in the technical ICT fields of pervasive communications, combined with the science of big data mining and machine learning, are continuously transforming the way we interact with each other, with physical devices and infrastructures. Such technologies are becoming more tightly intertwined with our daily activities and we are becoming more integrated into the cyber-physical systems that surround us. The positive (economic) impact on society of such advances is enormous; however, big data information flows exposes important privacy details of our daily lives and our behavioural patterns. Such information may potentially be abused for purposes ranging from digital identity theft to targeted marketing, or discrimination based on medical history or other digital footprints, leading to fundamental privacy concerns. On this basis, the objectives of this course further include: a) Understanding interdisciplinary aspects of data handling and cyber security solutions: ultimately, this involves modelling and defining the trade-off between privacy and utility in information sharing IoT scenarios, in a mathematically rigorous way. b) Familiarise with fundamental data mining and machine learning algorithms with a focus on their application as privacy-invasive technologies. c) Learn how to develop application-specific privacy enhancing techniques, including security layers such as intrusion detection, privacy-by-design methods, and privacy-aware sensing.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Discuss privacy-by-design principles.				

	• Get an overview of EU legislative and business regulatory aspects of data handling. • Use cyber security protocols to engineer holistic data privacy system solutions. • Apply fundamental data mining and activity recognition algorithms to run privacy-invansive security tests. • Demonstrate the principles of differential privacy by implementing privacy-preserving algorithms. • Design privacy solutions for IoT scenarios, including Smart Grid, Smart Cities and wearable sensor technologies.		
Prerequisites	None	Co-requisites	EMC111
Course Content	IoT scenarios and privacy concerns: Smart meter data collection, wearable and smartphone mobile sensing technologies, data handling and data linking potential risks and system-level analysis. Mathematical privacy metrics and privacy invasion tools: relative entropy, mutual information, cluster classification, regression analysis, residual features, activity recognition, non-intrusive appliance load monitoring, exploratory data mining, differential privacy and atypicality. Cyber-security privacy protection solutions: anonymisation with trusted third party, data aggregation, data splitting, secure multi-party communication protocols, homomorphic encryption, zero-proof cryptosystem, data obfuscation, physical behaviour optimisation. Anonymity networks (e.g. Tor and I2P), ethics Information-theoretic privacy preserving techniques: privacy-utility trade-off optimisation, privacy-aware data sensing, lossy data compression, rate-distortion function, differentially private billing. General Data Protection Regulation (GDPR) Standardisation, regulatory and business aspects: consent-based approaches, ethical aspects of data collection, access control restrictions, business requirements and risks. ISO/IEC 27001 family of standards. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical privacy scenarios and IoT considerations.		
Teaching Methodology	Face – to – Face		
Bibliography	*Keith M Martin, Everyday Cryptography: Fundamental Principles and Applications. Oxford University Press.* *Brij Bhooshian Gupta, Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices.*		

	R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," in IEEE Access, vol. 5, pp. 10562-10582. *Clarence Chio, David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms.* *Dua, S. and Du, X., Data mining and machine learning in cybersecurity. Auerbach Publications* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Incident Response and Forensic Analysis</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC125</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher's Name</td><td colspan="5">Dimitrios Baltatzis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyze and respond to. The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Incident response encompasses the entire process of identifying intrusions, develop the information necessary to fully understand them, elaborate and execute actions to contain, eradicate and recover from cyber incidents. Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon succesful completion of this course students should be able to:
• Define and describe the main phases of incident response
• Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident
• Identify different kinds of attacks methods to counter their effects
• Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up
• Explain the principles of evidence collection and the chain of custody
• Identify and evaluate key forensic analysis techniques
• Describe the application of such techniques to real situations and the connection with incident response</td></tr>
</table>

	• Gather and maintaining a Computer Incident Response Team (CSIRT) with the set of regulations and frameworks that should be followed • Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection. • Contact forensic analysis investigations using the appropriate tools and methodologies		
Prerequisites	None	Co-requisites	EMC111
Course Content	Introduction: Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles. Preparation: Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates. Identification: Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC). Containment: Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation. Eradication: Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully. Recovery: Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process. Follow-up: Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement. Contact url investigation, DNS analysis. Digital Forensics Investigation Process: Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures.		

	Technical forensics tools and techniques: Hard disks, removable media and file systems, Windows forensics, duplication/imaging ofstorage media, file carving by recovering deleted files and hidden or deleted partitions, steganography and image forensics, log analysis, password crackers, network discovery, collecting and examing memory from a live system, emailforensics, mobile forensics, investigation of attacks, common tools (Autopsy, FTK, Nmap, volatility, etc.) Business case study and lecture: Lecture by invited experts from the cybersecurity industry, including law enforcement. Discussion normally focuses on the practicalities and challenges of incident response and the ways in which forensic analysis contributes to successful cybercrime prosecutions.
Teaching Methodology	Face – to – Face
Bibliography	*“Incident Response & Computer Forensics, Third Edition”* by Jason T. Luttgens and Matthew Pepe *“Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder”*, by Don Murdoch *“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”*, by Leighton Johnson *“The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics”*, by John Sammons *“Digital Forensics with Open-Source Tools”*, by Cory Altheide and Harlan Carvey *Digital Forensics and Incident Response, Second Edition, Gerard Johansen, 2020 Packt Publishing* *Introductory Computer Forensics A Hands-on Practical Approach, Xiaodong Lin, 2019* *Practical Cyber Forensics, An Incident-Based Approach to orensic Investigations, Niranjan Reddy, 2019* *“Digital Forensics Processing and Procedures”*, by David Lilburn Watson and Andrew Jones IEEE Journals and Magazines

Assessment	Final Examination	50%
	Midterm Examination	40%
	Attendance/Participation	10%
Language	English	

Course Title	Mobile Network Communication Systems				
Course Code	EMC131				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Assoc Prof. Jiri Hosek, Ph.D., Pavel Masek, Ph.D., Radek Mozny				
ECTS	6	Lectures / week	2 Hours / 13 weeks	Laboratories / week	3 Hours / 13 weeks
Course Purpose and Objectives	The attention will be focused on the theoretical background of mobile networks i.e., architecture of mobile networks; definition of the communication technologies and mechanisms by 3GPP; the key parts of the LTE (EPS); radio access network (RAN) of the 4G+ mobile networks; protocol stack in the EPS; procedures in the LTE network; voice over LTE; next-generation mobile systems (5G NR). In parallel to the theoretical lectures, the laboratory exercises, using the Network Simulator 3 (NS-3), will take place to verify the theoretical assumptions in the simulation environment.				
Learning Outcomes	By the end of this course, students are expected to be able to: • understand the theoretical background of mobile networks i.e., architecture of mobile networks; definition of the communication technologies and mechanisms by 3GPP; the key parts of the LTE (EPS); radio access network (RAN) of the 4G+ mobile networks; protocol stack in the EPS; procedures in the LTE network; voice over LTE; and finally next-generation mobile systems (5G NR). • implement the gained theoretical background in the simulation environment (Simulator 3, NS-3) to solve different practical problems.				
Prerequisites	The subject knowledge Basic knowledge of information and communication technologies (ICT) on the Bachelor degree level is required.	Co-requisites	None		

Course Content	**Lectures** 1. Opening lecture (general information; teaching; selected platforms). 2. Overview of the legacy cellular systems (2G – GSM, GPRS, EDGE). 3. Overview of the legacy cellular systems (3G – UMTS; HDSPA/HSPA; HSPA+). 4. Introduction to the LTE/EPS systems. EPS reference model. 5. LTE (EPS) – roaming, security, billing, EPS UE, EPS tracking. 6. AS and NAS procedures. Management of radio resources in the EPS network. 7. Characteristics of the radio interface (physical layer), U/C-Plane. 8. LTE (initial) access and call procedures. Communication protocols – in detail. 9. Bearer Management in LTE. 10. Spectrum Allocation in LTE. 11. Resource Element Mapping in LTE – in detail. 12. Voice and Text Messages over LTE. 13. Next-generation Mobile Networks (5G NR). **Laboratories:** 1. Laboratory introduction, security in the lab, explanation of the course plan 2. Numerical exercise - selection and reselection in 2G (GSM). 3. Numerical exercise - selection and reselection in 2G (GPRS). 4. Numerical exercise - selection and reselection in 4G (LTE) 5. Network Simulator 3 – intro, core concepts and abstractions 6. Network Simulator 3 – debugging, tracing 7. NS-3 – tracking; bus topology 8. NS-3 – IEEE 802.11 models; WiFi topology helpers 9. NS-3 – advanced tracing; TCP window 10. NS-3 – LTE module LENA; initial scenario 11. LENA; basic scenario, EPC scenario; EPC with emulation mode 12. mmWave module (propagation models, channel models, and mobility) 13. Final test

Teaching Methodology	Face-to-Face
Bibliography	All necessary study materials are provided to the students via BUT eLearning system. [1] Sauter, M. (2017). From GSM to LTE-advanced Pro and 5G: An introduction to mobile networks and mobile broadband. John Wiley & Sons. [2] Dahlman, E., Parkvall, S., & Skold, J. (2018). 5G NR: The next generation wireless access technology. Academic Press. [3] Zaidi, A., Athley, F., Medbo, J., Gustavsson, U., Durisi, G., & Chen, X. (2018). 5G Physical Layer: Principles, Models and Technology Components. [4] Rappaport, T. S., Heath Jr, R. W., Daniels, R. C., & Murdock, J. N. (2014). Millimeter wave wireless communications. Pearson Education
Assessment	Examinations 70 % Assignments 20 % Class Participation and Attendance 10 % 100 %
Language	English

Course Title	Foundations of Cryptography				
Course Code	EMC132				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher’s Name	Dr. Sara Ricci (Guarantor) and Dr. Petr Dzurenda				
ECTS	6	Lectures / week	2 Hours / 13 weeks	Laboratories / week	3 Hours / 13 weeks
Course Purpose and Objectives	The goal of the course is to provide students with the basic knowledge of cryptography. During the course, students will study the theoretical foundations, the most common algorithms, and concepts used in modern cryptography.				
Learning Outcomes	By the end of this course students are expected to be able to: • understand theoretical foundations of cryptography and computer security • analyze and design security solutions for information and communication technologies (ICT) • understand basic principles of algebraic structures used in cryptography and basic cryptographic primitives.				
Prerequisites	Basic knowledge of cryptography and mathematics are recommended.	Co-requisites	None		
Course Content	**Lectures** 1. History and Terminology 2. Number Theory and Complexity Theory 3. Modular Arithmetic and Groups 4. Prime Numbers 5. Random Number Generation 6. Asymmetric Cryptography 7. Symmetric Cryptography 8. Elliptic Curves in Cryptography				

	9. Bilinear Pairings in Cryptography 10. Pairing-based Protocols 11. Digital Signatures and Sigma Protocols 12. Commitments 13. Practical authentication **Laboratories:** 1. Monoalphabetic and Polyalphabetic ciphers 2. GCD, Euler Function and Complexity Theory 3. Modulus, Multiplicative Groups and Generators 4. Prime Numbers 5. Random Number Generators 6. Diffie-Hellman, RSA and DSA schemes 7. Stream Ciphers and Hash Functions 8. Elliptic Curve 9. EC Cryptography 10. Pairing-based Protocols 11. Digital Signatures and Sigma Protocols 12. Commitments 13. Cryptographic Protocols in applications
Teaching Methodology	Face-to-Face
Bibliography	[1] Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson, 2016, ISBN 978-0134444284 [2] Hoffstein, J., Pipher, J., Silverman, J. H.: An introduction to mathematical cryptography. New York: Springer, 2014, ISBN 978-1493917105 [3] Oorschot, P. C. v.: Computer Security and the Internet: Tools and Jewels. [4] Washington LC., Elliptic curves: number theory and cryptography CRC press; 2008
Assessment	Examinations 60 % Assignments 15 % Class Participation and Attendance 25 % 100 %
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Modern Cryptography</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC133</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Dr. Sara Ricci (Guarantor), Dr. Petr Dzurenda, Ing. Patrik Dobiáš</td></tr>
<tr><td>ECTS</td><td>6</td><td>Lectures / week</td><td>2 Hours / 13 weeks</td><td>Laboratories / week</td><td>2 Hours / 13 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective of this course is to provide students with detailed theoretical and practical knowledge of modern cryptographic schemes and their concrete application. The course places great emphasis on practical exercises, where students can try and implement individual technologies themselves.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">By the end of this course students are expected to be able to:
• Have theoretical and practical knowledge on current modern cryptography and its concrete applications. In particular, on post-quantum cryptography, cloud computing, secure data processing, e-voting, cryptocurrencies, and data privacy.
• develop modern cryptographic systems based on the topics explained in the course.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">Basic knowledge of algebra (e.g., matrices and algebraic structure) and cryptography on bachelor level are recommended.</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5"><b>Lectures</b>
1. Post-quantum cycle: Introduction to Post-Quantum Cryptography
2. Post-quantum cycle: Lattice-based Cryptography
3. Post-quantum cycle: LWE and RLWE Problems
4. Post-quantum cycle: Kyber, Saber and Dilithium
5. Secure computation cycle: Homomorphic Encryption</td></tr>
</table>

	6. Secure computation cycle: Fully Homomorphic Encryption and Applications 7. Secure computation cycle: Secret Sharing 8. Secure computation cycle: Secure Multiparty Computation 9. Decentralized systems cycle: Blockchain 10. Decentralized systems cycle: Cryptocurrencies 11. Decentralized systems cycle: Smart Contracts 12. Data Privacy cycle: Data Anonymization 13. Data Privacy cycle: Differential Privacy, k-anonymity and Record Linkage **Laboratories:** 14. Introduction to python 15. Numpy library and Lattice 16. LWE problem and Regev scheme 17. pqcrypto library and benchmarking 18. Homomorphic Encryption 19. Fully Homomorphic Encryption and Applications 20. Secret Sharing 21. Secure Multiparty Computation 22. Blockchain 23. Cryptocurrencies, Multisignatures and PETs 24. Smart Contracts 25. Data Anonymization 26. K-anonymity
Teaching Methodology	Face-to-Face
Bibliography	All necessary study materials are provided to the students via BUT eLearning system. [1] Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography. Springer. [2] Schoenmakers, B.: Lecture Notes Cryptographic Protocols. Technical University of Eindhoven. [3] Goldreich, O.: Foundations of Cryptography Volume 2 - Basic Applications. Cambridge University Press. [4] Hundepool, A., Domingo-Ferrer, J., et al.: Statistical disclosure control. John Wiley & Sons.

Assessment	Examinations	60 %
	Assignments	18 %
	Class Participation and Attendance	22 %
		100 %
Language	English	

Course Title	Parallel Data Processing				
Course Code	EMC134				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Vojtech Myska / Assoc. prof. Radim Burget, Ph.D.				
ECTS	6	Lectures / week	2 Hours / 13 weeks	Laboratories / week	3 Hours / 13 weeks
Course Purpose and Objectives	The goal of the course is to introduce parallelization for data analysis with using common processors, graphic processors and distributed systems.				
Learning Outcomes	By the end of this course, students are expected to be able to: • design and implement various forms of parallel systems to solve big data challenge. • Know and understand various techniques for the parallelization of computations using CPU and GPU and further techniques for distributed computations. • know how to control technologies Apache Spark, Kafka, Cassandra to solve distributed data processing with using data operations: data transformations, aggregation, classification, regression, clustering, frequent patterns.				
Prerequisites	The subject knowledge Basic knowledge of information and communication technologies (ICT) on the Bachelor degree level is required.	Co-requisites	None		
Course Content	**Lectures:** 1. Introduction 2. CPU Parallel Computing 3. GPU Introduction 4. GPU Memory 5. GPU Synchronization				

	6. GPU Parallel Patterns 7. GPU Matrix Operations and Streams 8. Spark Introduction 9. Spark Advanced Operations 10. Spark Machine Learning 11. Spark Streaming 12. Other Parallel Technologies 13. Overview and Discussion 14. Final exam **Computer excercises:** 1. Introduction 2. CPU Parallel Computing 3. GPU Introduction 4. GPU Memory 5. GPU Synchronization 6. GPU Parallel Patterns 7. GPU Matrix Operations and Streams 8. Spark Introduction 9. Spark Advanced Operations 10. Spark Machine Learning 11. Spark Streaming 12. Other Parallel Technologies 13. Defence of the project
Teaching Methodology	Face-to-Face
Bibliography	All necessary study materials are provided to the students via BUT eLearning system. [1] Dasgupta, Nataraj. "Practical big data analytics: Hands-on techniques to implement enterprise analytics and machine learning using Hadoop, Spark, NoSQL and R." (2018) [2] BARLAS, Gerassimos. Multicore and gpu programming: an integrated approach. ISBN 9780124171374

Assessment	Examinations	100 %
	Assignments	0 %
	Class Participation and Attendance	0 %
		100 %
Language	English	

Course Title	Semestral Thesis				
Course Code	EMC135				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Assoc. Prof. Petr Čika, PhD				
ECTS	1	Lectures / week	1 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	The aim of the course is for students to elaborate an individual technical project whose theme is chosen from a list of themes offered by the respective Department.				
Learning Outcomes	Students solve a special problem as an individual technical project whose theme is chosen from the list of themes offered at the department. After course completion, students will be able to: - independently develop a technical project, - write a technical report for the project, - defend the project.				
Prerequisites	None	Co-requisites	None		
Course Content	None				
Teaching Methodology	Face-to-Face				
Bibliography	None				
Assessment	Examinations Assignments Class Participation and Attendance	100 % 0 % 0 % 100 %			
Language	English				

<table>
<tr><td>Course Title</td><td colspan="5">Data Structures and Algorithms</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC136</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Assoc. prof. Radim Burget, Ph.D.</td></tr>
<tr><td>ECTS</td><td>5</td><td>Lectures / week</td><td>2 Hours / 13 weeks</td><td>Laboratories / week</td><td>2 Hours / 13 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">To provide theoretical knowledge of information gathering, processing and sharing in communication systems, and of their structure, behaviour and mutual interaction.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">By the end of this course, students are expected to:
• design and implement various forms of abstract data types and its application to solve specific problems.
• To solve them students know how to use linear, tree and graph data structures,
• furthermore they know how to search in the data structures and use genetic algorithms for search in a search space and optimization.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">The subject knowledge Basic knowledge of information and communication technologies (ICT) on the Bachelor degree level is required.</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5"><b>Lectures:</b>
1. Information representation, objective oriented design.
2. Information representation, introduction to data structures.
3. Complexity, computability and automata theory.
4. Information representation, linear data structures and sorting.
5. Information representation - tree data structures.
6. Information representation - graph theory.
7. Information access - spanning tree.</td></tr>
</table>

	8. Information access - graph search. 9. Information access – machine learning 1/2. 10. Information access – machine learning 2/2. 11. Information access - genetic algorithms. 12. Information access - optimization. 13. Parallel computations. **Computer exercises:** 1. Introduction to OON. 2. Information representation I. 3. Information representation II. 4. Linear data structures. 5. Binary search trees. 6. Graphs theory. 7. Search in Graphs. 8. Midexam. 9. Search in Graphs - Dijkstra algorithm. 10. Data mining - decision trees. 11. Optimization - genetic algorithms.
Teaching Methodology	Face-to-Face
Bibliography	All necessary study materials are provided to the students via BUT eLearning system. GOODRICH, T.M., TAMASSIA, R. Data Structures and Algorithms in Java. 2000.
Assessment	Examinations 100 % Assignments 0 % Class Participation and Attendance 0 % 100 %
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Modern Network Technologies</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC137</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Prof. Jaroslav Koton, Ph.D.; Ing. Ondřej Krajsa, Ph.D.</td></tr>
<tr><td>ECTS</td><td>5</td><td>Lectures / week</td><td>2 Hours / 13 weeks</td><td>Laboratories / week</td><td>2 Hours / 13 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The aim of the course is to introduce principles and methods implemented in modern network technologies to maintain the required throughput and reliability. The course is oriented mainly to different aspects of data flow control preventing or dealing congestion of active network elements to provide Quality of Service support in packet networks.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">By the end of this course, students are expected to be able to:
• know and understand data flow-control algorithms and mechanisms implemented on relevant levels of the OSI/ISO Reference Model and quality-of-service support mechanisms used in fixed, wireless and mobile communication networks.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">The subject knowledge Basic knowledge of information and communication technologies (ICT) on the Bachelor degree level is required.</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5"><b>Lectures:</b>
1. Queuing theory - mathematical representation
2. Queuing theory – Kendall classification, Markovian system of queue control
3. Qualitative parameters of communication networks
4. Throughput control
5. Flow control and error correction on data link layer</td></tr>
</table>

	6. Flow control in TCP – introduction 7. Implementation methods of TCP 8. Retransmission time-out and congestion window control in TCP 9. Mechanisms for congestion window control in TCP 10. Quality of Service in communication networks - basic requirements 11. Quality of Service - marking, classification, metering 12. Quality of Service - packet scheduling, active queue management, ECN 13. Support of Quality of Service in wireless networks **Computer exercises:** 1. Introduction to laboratories and the used Mikrotik hardware 2. Queue theory and its application 3. Router OS, routing, bridging/switching 4. Wireless network configuration, CAPsMAN 5. Firewall – protection against attacks 6. Scripting – automation of router maintenance tasks 7. Quality of Service support 8. Quality of Service in wireless network 9. IP tunnels 10. l2TP/IPSec, IPSec IKEv2 11. MPLS/VPLS in Mikrotik 12. Compensatory exercise 13. Credit test
Teaching Methodology	Face-to-Face

Bibliography	All necessary study materials are provided to the students via BUT eLearning system. [1] LARSSON, C. Design of Modern Communication Networks. Methods and Applications, 1st edition, Academic Press - Elsevier, ISBN: 978-0-12-407238-1, 2014 [2] BHAT, U. NARAYAN, An Introduction to Queueing Theory, Modeling and Analysis in Applications, Springer, ISBN: 978-0-8176-8420-4, 2015. [3] KOTON, J. Modern Communication Networks, lecture notes, 2018. [4] WEHRLE, K., GUNES, M., GROSS, J. Modeling and Tools for Network Simulation, Springer-Verlag Berlin Heidelberg, ISBN: 978-3-642-12330-6, 2010 [5] FARREL, A. et al. Network Quality of Service: Know It All, 1st edition, Morgan Kaufmann, ISBN: 978-0-12-374597-2, 2008. [6] STALLINGS, W. Data and Computer Communications, 10th edition, Pearson Education Limited, ISBN: 978-12-9-201738-8, 2013.
Assessment	Examinations 80 % Assignments 0 % Class Participation and Attendance 20 % 100 %
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Optical Networks</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC138</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Assoc. prof. Petr Münster, Ph.D.</td></tr>
<tr><td>ECTS</td><td>5</td><td>Lectures / week</td><td>2 Hours / 13 weeks</td><td>Laboratories / week</td><td>2 Hours / 6 weeks
Seminar
2 Hours / 7 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The goal is to gain knowledge about optical fibers, current optical networks, basic components of transmission systems, but also optical network measurement techniques.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">By the end of this course, students are expected to be able to:
• discuss the advantages and disadvantages of different types of optical fibers for information transmission,
• splice optical fibers,
• become acquainted with the deployment of different technologies in networks,
• design an optical networks,
• acquire knowledge of FTTx (fiber to the building, home, etc.) networks,
• acquire knowledge of the multiplexing techniques WDM (Wavelength division multiplexing),
• acquire knowledge of components used in fiber optic networks,
• acquire knowledge from measurement of optical fibers and networks,
• get the orientation of the problems of dispersion (CD - Chromatic dispersion, PMD - Polarization mode dispersion),</td></tr>
<tr><td>Prerequisites</td><td colspan="2">Profficiency is required on the Bachelor's degree level. Students should have the knowledge of and optical signal transmission. Some basic knowledge in the area of transmission of</td><td colspan="2">Co-requisites</td><td>None</td></tr>
</table>

	binary signals and be able to tackle distortions in the transmission. It is recommended the completion of the course Transmission media, taught in the second year of the bachelor program.		
Course Content	**Lectures:** 1. Optical sources 2. Optical detectors 3. Optical fibers and cables 4. Linear and nonlinear phenomena in an optical fiber 5. Optical amplifiers 6. Optical modulators and switches 7. Passive optical components 8. Optical networks 9. Additional telecommunications network services 10. Sensing systems and their application 11. Fibre optic sensors I. 12. Fibre optic sensors II. 13. Summary **Numerical exercises:** 1. Calculation of basic fiber parameters I. 2. Calculation of basic fiber parameters II. 3. Calculation of network parameters I. 4. Calculation of network parameters II. 5. Calculation of network parameters II. 6. Optical amplification		
Teaching Methodology	Face-to-Face		

Bibliography	All necessary study materials are provided to the students via BUT eLearning system. [1] Filka, M: Optical Networks for joint teaching programme of BUT and VSB-TUO
Assessment	Examinations 70 % Assignments 0 % Class Participation and Attendance 30 % 100 %
Language	English

Course Title	Diploma Thesis				
Course Code	EMC141				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year / 4th Semester				
Teacher's Name	Assoc. Prof. Petr Čika, PhD				
ECTS	30	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	The aim is for the student to elaborate independently a diploma project to conclude the MSc studies. The student chooses the theme of the diploma project from a list of themes offered by the respective Department.				
Learning Outcomes	On completion of the course, students are expected to be able to: • independently develop a technical project, • write a technical report for the project, • defend the project.				
Prerequisites	A successful defence of the Semestral project (MPC-SPI).	Co-requisites	None		
Course Content	None				
Teaching Methodology	Face-to-Face				
Bibliography	None				
Assessment	Examinations Assignments Class Participation and Attendance	100 % 0 % 0 % 100 %			
Language	English				

TRACK 2

Course Title	Cyberattack Techniques and Ethical Hacking				
Course Code	EMC211				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	Antonio Ruiz Martínez, Félix Gómez Mármol				
ECTS	6 ECTS	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks
Course Purpose and Objectives	The goal of the course is to introduce students in attacking computer systems through an ethical hacking process. Students will know the different kind of security assessments that could be made and they will learn the different steps of a ethical hacking process through some laboratories where they will attack an scenario.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. • Collaborate when solving a problem in the field of cybersecurity, teamwork, and leadership. • Analyze methods and techniques of cyber-attacks and cyber-defense. • Design, deploy, and maintain cybersecurity systems. • Identify applicable regulations and legislation in the field of cybersecurity. • Elaborate clear, concise, and reasoned documentation on aspects related to the field of cybersecurity. • List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to be applied. • Perform vulnerability and risk analysis processes. • Classify vulnerabilities, threats and risks within the organization to determine their importance, taking into account the context.				
Prerequisites	None	Co-requisites	None		

Course Content	• Introduction to Ethical hacking o Basic concepts o Regulations and associated legislation • Security assessments. o Types of assessments o Methodologies o Training • Ethical hacking process. o Deployment of scenario and realization of ethical hacking process.
Teaching Methodology	Flipped classroom, project-based learning
Bibliography	• CEH™ v12 - Certified Ethical Hacker - Study Guide o Topic 1. Chapter 1. o Topic 2. Chapter 2. o Topic 3. Chapters 2, 4, 5, 6, 7, 9, 10, 11 and 12. • Desmond, Brian, et al. Active Directory: Designing, Deploying, and Running Active Directory. " O'Reilly Media, Inc.", 2008. o Topic 3. Chapters 2, 4 and 5.
Assessment	Examinations 30% Assignments 60% Class Participation and Attendance 10% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">CyberDefense Techniques</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC212</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S1</td></tr>
<tr><td>Teacher's Name</td><td colspan="5">José Ramón Hoyos-Barceló and ?</td></tr>
<tr><td>ECTS</td><td>6</td><td>Lectures / week</td><td>1,5 Hours /14 weeks</td><td>Laboratories / week</td><td>1,5 Hours /14 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course integrates an introduction to different ways of protecting the underlying communication networks and the detection of and response to security incidents, with a focus on computer forensics and the collection, analysis and reporting of digital evidence in support of incident or criminal events.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Identify the main current problems in the field of cybersecurity in specific scenarios.
• Analyse in detail cybersecurity scenarios, solutions or systems in order to detect possible areas for improvement.
• Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or unfamiliar environments related to cybersecurity.
• Identify the different multidisciplinary aspects (legal, social, ethical) to be taken into account when dealing with a problem related to a cybersecurity scenario.
• Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account.
• Formulate value judgements on the basis of collected information that, while incomplete or limited, include critical reasoning on the social and ethical responsibilities of the application of methods, cryptographic techniques, software tools or methodologies to address cybersecurity-related problems.
• Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and to the target audience.</td></tr>
</table>

	• Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be conveyed with regard to a cybersecurity scenario. • Present your knowledge in a clear, concise and unambiguous manner, adapting to the time set for the presentation. • Analyse methods and techniques of cyber-attacks and cyber-defence. • Produce clear, concise and reasoned documentation on aspects related to the field of cybersecurity. • Identify the characteristics and functions of the elements that form part of the security architectures and services of systems, critical infrastructures and communications networks.		
Prerequisites	None	Co-requisites	None
Course Content	Defense tools and Incident Management Unit 1- Network defence and monitoring tools Unit 2- Incident management and disaster recovery, cyber incident reporting Computer Forensics Unit 3- Introduction to Computer Forensics Unit 4- Situation assessment and collection of evidence Unit 5- Evidence Analysis Unit 6- Computer expertise		
Teaching Methodology	Face-to-Face		
Bibliography	1. Guide to Computer Network Security, 5th edition, by Joseph Migga Kizza. Springer (3: Security Threats, 5 Cyber Crimes and Hackers, 8 Disaster Management) 2. Stallings, William, et al., Computer Security - Principles and Practice (2018) (1.1 Computer security concepts; 1.2 Theats, attacks and assets; 8: Intrusion detection, 9: Firewall and Intrusion Prevention Systems, 14: IT Security Management and Risk Assessment, 15: IT Security Controls, Plans and Procedures, 17 Human resource security.) 3. Digital Forensics Explained. Greg Gogolin. CRC Press/Taylor & Francis Group. 2021 (1. What is digital forensics, 2.Digital forensic approaches, 3. Digital forensics tool kit, 7 Incident response, 10 Social engineering, 11 Anti-forensics) 4. Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730. (full article)		

Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cybersecurity and Network Security				
Course Code	EMC213				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	Rafael Marín López, Óscar Cánovas				
ECTS	6 ECTS	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 hours/14 weeks
Course Purpose and Objectives	The goal of the course is to analyse, discuss different network security protocols at different layers ranging from link-layer to application layer. The course will also pay attention to non-cryptographic defence tools and standards related with network security.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity.				

	● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. ● Design solutions to cybersecurity problems using creative thinking. ● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. ● Analyze methods and techniques of cyber attacks and cyber defense. ● Prepare clear, concise and reasoned documentation on aspects related to the field of cybersecurity. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Describe the cryptographic primitives, the secure protocols and the software mechanisms that allow data protection. ● Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of secure software. ● Employ the use of cryptographic primitives, secure protocols and software models to protect data in a cybersecurity scenario. ● Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes. ● Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.		
Prerequisites	None	Co-requisites	None
Course Content	● Network protocols and vulnerabilities: adversary models, types of attack. ● Application-level security (public key and symmetric key management, application-level protection (SSH, S/MIME), application services security) ● Transport level security (TLS, DTLS, QUIC) ● Network level security (ACLs, IPv6 security, routing protocol security, VPNs) ● Link level security: wireless level security (IEEE 802.1X, EAP, RADIUS, DIAMETER, WPA) attacks on ethernet switches, MAC level attacks. ● Non-cryptographic defense tools (packet filtering, firewall, DMZ, IDS, IPS, etc.)		

	● Advanced security topics (SDN, NFV, IoT) ● Communication security standards (how security protocols are specified and documented)
Teaching Methodology	Face-to-Face
Bibliography	● W. Stalling CRYPTOGRAPHY AND NETWORK SECURITY, EIGHTH EDITION – 8th ○ Chapter 1. Computer and Network Security Concepts (Block I) ○ Chapter 18 Wireless Network Security (Block I) ○ Chapter 17 Transport-Layer Security (Block III) ○ Chapter 20 IP security (Block III) ○ Chapter 21 Network Endpoint Security (Block II)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Techniques for the Management of the Cybersecurity				
Course Code	EMC214				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	Manuel Gil Pérez				
ECTS	6	Lectures / week	3 Hours / 14 weeks	Laboratories / week	3 Hours / 14 weeks
Course Purpose and Objectives	The objective of this course is to cover aspects related to organisational security governance and the security project management, including the identification of security risks in the protected organisation together with potential countermeasures to apply for risk reduction.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Holistically identify the different problems related to a specific area of cybersecurity. • Identify the different multidisciplinary aspects (legal, social, ethical) to consider when dealing with a problem related to a cybersecurity scenario. • Plan autonomous work tasks and self-learning processes running at the scheduled times. • Enumerate and identify the different types of vulnerabilities, threats, and risks within the organisation, as well as possible solutions to be applied. • Describe the principles of risk management, how to apply them and possible tools to be used. • Describe the main elements and functions that are part of smart services, products, and infrastructures in the cybersecurity domain. • Explain the different aspects related to organisational security governance, security project management, design and implementation of products, services, and facilities in cybersecurity scenarios.				
Prerequisites	None	Co-requisites	None		
Course Content	Management of information security systems: • Unit 1. Information security legislation in Spain o National Security Scheme: objectives, requirements, and security measures				

	• Unit 2. Information Security Management Systems (ISMS) – *ISO 27000* • Unit 3. Implementation and evaluation of ISMS according to the stages of the Deming cycle: plan, do, check, act • Unit 4. Security and resilience plans – *ISO 22300 family* Analysis and management of security risks: • Unit 5. Analysis, assessment, and treatment of security risks o Security Master Plan • Unit 6. Methodologies for security risk analysis o NIST SP 800, MAGERIT / PILAR • Unit 7. Countermeasures for risk reduction Practices: • Case studies for applying security management tools • Implementation and audit of Information Security Management Systems (ISMS) o Audit automation and standardisation, following the ANA approach • Risk analysis and selection of countermeasures o Use of µPILAR for risk analysis and choice of safeguards, analysing the residual risk
Teaching Methodology	Face-to-Face
Bibliography	1. Gibson, Darril (2020). Managing Risk in Information Systems (Information Systems Security & Assurance). Jones and Bartlett Publishers, Inc. 2. Tiller, James S., O'Hanley, Richard (2013). Information Security Management Handbook, Volume 7 (6th Ed.). Auerbach Publications. 3. Spanish Ministry of Finance and Civil Service (2014). MAGERIT V.3: Methodology for Information Systems Risk Analysis and Management. Edita.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cryptography				
Course Code	EMC215				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	Leandro Marín Muñoz				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hour / 7 weeks
Course Purpose and Objectives	The objective of this course is to give a broad view of cryptography, studying both the mathematical and theoretical aspects as well as the aspects related to their implementation in special environments.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Solve problems related with theoretical and mathematical cyptology. • Evaluate the security of cryptographic methods. • Apply their knowledge about cryptology in research. • Understand the mathematical foundations of cybersecurity.				
Prerequisites	None	Co-requisites	None		
Course Content	Cryptographic security models. Secret sharing systems. Symmetric cryptography (block ciphers, stream ciphers, digital hash functions, message authentication codes, Merkle trees and block chains), public key cryptography (RSA-based, elliptic curve and lattice constructs, digital signatures), cryptographic protocols (authentication, key exchange, zero knowledge, secure multiparty computing), advanced aspects of cryptography (group/ring-based signatures, identity-based ciphers, homomorphic cryptography, side-channel attacks, implementations in environments with special requirements such us low power consumption, memory restrictions, etc.)"				
Teaching Methodology	Face-to-Face				

<table>
<tr><td>Bibliography</td><td>
<ul>
<li>Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. 2007. CRC Press. Chapter 3 (Private Key Cryptography) Chapter 5 (Block Ciphers) Chapter 10 (Public Key Encryption) Chapter 12 (Digital Signatures)</li>
<li>Henri Cohen. A Course in Computational Number Theory. 1993. Springer. Chapter 1 (Basic Number Theory) Chapter 8, 10 (Factorization) Chapter 9 (Primality Testing)</li>
<li>Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography. 2003. Springer. Chapter 2 (Elliptic Curves) Chapter 4 (Implementation Issues on ECC)</li>
<li>FIPS 197. Advanded Encryption Standard (AES) – NIST.</li>
<li>Craig Gentry. A Fully Homomorphic Encryption Scheme (Ph.D. Thesis). (only the introduction for homomorphic encryption)</li>
</ul>
</td></tr>
<tr><td>Assessment</td><td>
<table>
<tr><td>Examinations</td><td>60%</td></tr>
<tr><td>Class Participation and Attendance</td><td>10%</td></tr>
<tr><td>Assignments</td><td>30%</td></tr>
<tr><td></td><td>100%</td></tr>
</table>
</td></tr>
<tr><td>Language</td><td>English</td></tr>
</table>

<table>
<tr><td>Course Title</td><td colspan="5">Innovation and Entrepreneurship Seminar</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC216</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S1</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Responsible Antonio Skarmeta
Different participants based on seminars</td></tr>
<tr><td>ECTS</td><td>3</td><td>Lectures / week</td><td>3 Hours / 7 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective is to bring students closer to the most pressing problems and solutions at all times in industry, administration, defense and research. Through the different seminars proposed, students will have access to the experience of professionals of recognized prestige whose professional work is related to Cybersecurity in its legal, administrative, management and legal aspects. On the other hand, the more academic seminars will put students in contact with the state of the art in concepts, protocols, developments and tools on specific topics related to cybersecurity. Therefore, the seminars may be framed within any of the subjects of the master's degree</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account.
• Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario.
• Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity.
• Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes.
• Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td>Co-requisites</td><td colspan="2">None</td></tr>
<tr><td>Course Content</td><td colspan="5">Within the master's degree, seminars will be given that may change from year to year, as advised by a field as variable as cybersecurity.</td></tr>
</table>

	Yearly the planning of seminar will be defined
Teaching Methodology	Face-to-Face
Bibliography	
Assessment	Assignments 60% Class Participation and Attendance 40% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Cybersecurity Legal Framework</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC221</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 2nd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Julián Valero Torrijos</td></tr>
<tr><td>ECTS</td><td>3</td><td>Lectures / week</td><td>2 Hours / 7 weeks</td><td>Laboratories / week</td><td>1 Hours / 7 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5"><b>Objective:</b>
This course aims to provide students with an overview of the main legal aspects of cybersecurity, in particular from the perspective of European Union legislation. Specifically, it will provide the basic tools to identify the relevant rules, understand the basic legal concepts and then proceed to their application, considering the singularities of the digital environment.
<b>Description:</b>
Cybersecurity is nowadays a basic requirement for the development of digital services and contents, so that its legal framework has become an essential topic for IT sector professionals. This course will provide an overview of the legal framework of cybersecurity, taking into account its impact on fundamental rights and public freedoms, the intervention of public administrations in both the regulation of activities and their enforcement, as well as the implications from the perspective of criminal law.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Identify the regulations and legislation applicable in the field of cybersecurity.
• Understand the main legal concepts in the field of cibersecurity.
• Identify the main legal aspects to be taken into account when dealing with a problem related to a cybersecurity scenario.
• Produce clear, concise and reasoned documentation including legal requirements of cybersecurity.
• Define a risk management policy taking into account legal requirements.
• Apply the legal concepts and rules associated with cybersecurity scenarios.
• Design safety management processes for products, services and facilities from the perspective of their legal requirements.</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">• Identify new and emerging technologies, best practices, regulatory, legislative and ethical aspects related to cybersecurity and mechanisms to detect these changes.
• Adapt cybersecurity scenarios in line with new trends, best practices, standards, regulation and human aspects.
• Assess the legal implications and risks of adopting new technologies from the perspective of cybersecurity in concrete business scenarios.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">- General regulatory framework. European and Spanish regulation on cybersecurity and protection of critical infrastructures.
- Personal data protection regulation. Singularities in the public sector. The Spanish National Security Scheme.
- Cybersecurity and digital services. The singularities of financial services and payment tools.
- Trust services legal framework. Digital identity
- Criminal law and cybersecurity.</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face-to-Face and Online activities</td></tr>
<tr><td>Bibliography</td><td colspan="3"><b><u>EU LAW</u></b>
- Jozef Andraško, Matúš Mesarčík, Ondrej Hamuľák: “The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework”, AI & SOCIETY volume 36, p. 623–636 (2021)
- Dimitra Markopouloua, Vagelis Papakonstantinoua, Paulde Hert: “The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation”, Computer Law & Security Review, Volume 35, Issue 6, November (2019).
- Gloria González Fuster, Lina Jasmontaite: “Cybersecurity regulation in the European union: the digital, the critical and fundamental rights”, The ethics of cybersecurity. Springer, Cham, p. 97-115 (2020).
- Pier Giorgio Chiara: “The IoT and the new EU cybersecurity regulatory landscape”, International Review of Law, Computers & Technology, 36:2, 118-137 (2022).
<b><u>SPANISH LAW</u></b>
- Alamillo Domingo, A.: Identificación, firma y otras pruebas electrónicas: la regulación jurídica-administrativa de la</td></tr>
</table>

	acreditación de las transacciones electrónicas. Thomson-Reuters Aranzadi, 2018 - Beltrán, M. y Tejerina, O. (coords.): Aspectos jurídicos de la ciberseguridad. RA-MA, 2020 - Canals Ametller, D. (Dir.): Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales. Wolters Kluwer, 2021 - Fernández García, E.: “Derecho de la ciberseguridad de las infraestructuras críticas más allá de la perspectiva penalista”, Revista Jurídica de Castilla y León, núm. 56 2022 - Fondevila Antolín, J.: “Seguridad en la utilización de medios electrónicos: el Esquema Nacional de Seguridad”, en E. Gamero (dir.): Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del sector público. Tirant lo Blanch, 2017 - Galán, C.: “El derecho a la ciberseguridad”, en T. de la Quadra y J.L. Piñar (dirs.): Sociedad Digital y Derecho. Boletín Oficial del Estado, 2018 - Fuertes López, M.: Metamorfosis del Estado. Maremoto digital y ciberseguridad. Marcial Pons, 2022 - Llaneza González, P.: Identidad digital, Wolters-Kluwer Bosch, 2021 - Mallada Fernández, C. (coord.): Nuevos retos de la ciberseguridad en un contexto cambiante. Thomson-Reuters Aranzadi, 2019
Assessment	Examinations 45% Class Participation and Attendance 10% Assignments 45% 100%
Language	English

Course Title	Software Security and Secure Software Lifecycle				
Course Code	EMC222				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	José A. Ruipérez Valiente				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of this course is to provide a broad overview of the secure software design process and the secure software lifecycle (SDL), reviewing methods and frameworks to accomplish these goals. Moreover, it will also review some of the main families of vulnerabilities, in order to provide prevention and detection guidelines. It will provide examples specifically applied to verticals.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify in a holistic way the different problems within a specific area of cybersecurity • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that take into account multidisciplinary factors. • Identify management models of cybersecurity and associated processes to carry out the cybersecurity tracking and management within an organization • Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of software security. • Analyse the scenarios where it is needed to provide software and protection mechanisms of the organizations' data considering the existing norms. • Propose the use of cryptographic primitives, secure protocols, and methodologies for the development of secure software based on the current scenario considering both technical and business aspects. • Evaluate the data and software security based on employed cryptographic primitives, secure protocols and the vulnerability analysis carried out.				
Prerequisites	None	Co-requisites	None		

Course Content	• Unit 1: Secure software design o Security risk management o Security testing o Security coding techniques (code hardening) o Security requirements, validation and verification • Unit 2: Secure software lifecycle (SDL) o SDL frameworks (Microsoft, etc), adaptations (agile, mobile, etc) and assessment (SAMM, BSIMM, certifications , etc) • Unit 3: Prevention and detection of vulnerabilities o Prevention, detection and mitigation o Client and server side vulnerabilities • Unit 4: Secure software applied to vertical
Teaching Methodology	Face-to-Face
Bibliography	• [CS:P&P]: Computer Security: Principles and Practice. William Stallings and Lawrie Brown (4th edition). 2017. • [CCS]: Corporate Computer Security. Randall J. Boyle and Raymond R. Panko (5th edition). 2021. • [SiC]: Security in Computing. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies (5th edition). 2015. • [SR&ASD]: Secure, Resilient, and Agile Software Development. Mark S. Merkow. 2020 • [SDL]: The Security Development Lifecycle. Michael Howard and Steve Lipner. 2006. • [SSDF]: Secure Software Development Framework (SSDF). NIST Special Publication 800-218. Murugiah Souppaya, Karen Scarfone, and Donna Dodson, pp. 10-28, 2022. • [ETSI] Cyber security for consumer internet of things: Baseline requirements, ETSI EN 303 645, pp. 13-25, 2020. • [MSA] Microservices Security in Action: Design secure network and API endpoint security for Microservices applications, with examples using Java, Kubernetes, and Istio. W. N. Dias and P. Siriwardena, 2020 • [CC] Common Criteria for Information Technology Security Evaluation, Common Criteria, 2022. • [SOTA] State of the Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2, ECSO, 2017. **Unit 1** o [CS:P&P]: Chapter 10 Buffer Overflow. Chapter 11 Software Security. Chapter 14 IT Security Management and Risk Assessment.

	o [CCS]: Chapter 2 Planning and Policy. Chapter 8. Application security o [SiC]: Chapter 3 Programs and Programming, Chapter 4 The Web—User Side, Chapter 10 Management and Incidents o [SR&ASD] Chapter 8: Testing Part 1: Static Code Analysis, Chapter 9: Testing Part 2: Penetration Testing/Dynamic Analysis/IAST/RASP **Unit 2** o [SR&ASD] Chapter 5: Secure Design Considerations, Chapter 6: Security in the Design Sprint, Chapter 7: Defensive Programming, Chapter 10: Securing DevOps o [CS:P&P]: Chapter 13 Cloud and IoT Security. 12.8 Virtualization security o [CCS]: Chapter 4. Secure networks o [SiC]: Chapter 6 Networks, Chapter 8 Cloud Computing o [ETSI]: Full reference **Unit 3** o [SDL]: Part II: "The Security Development Lifecycle Process" o [SSDF]: Full reference. o [CS:P&P]: Chapter 15 IT Security Controls, Plans, and Procedures o [SR&ASD]: Chapter 11: Metrics and Models for AppSec Maturity o [MSA]: Chapter 1: Microservices security landscape **Unit 4** o [CC]: Part I: "Part 1: Introduction and general model" o [SOTA]: Full reference.	
Assessment	Examinations Assignments Class Participation and Attendance	45% 45% 10% 100%
Language	English	

<table>
<tr><td>Course Title</td><td colspan="5">Authentication and Authorization Infrastructures</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC223</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S2</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Gabriel López Millán</td></tr>
<tr><td>ECTS</td><td>3</td><td>Lectures / week</td><td>2 Hours / 7 weeks</td><td>Laboratories / week</td><td>1 Hours / 7 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective of this course is to introduce students to the concepts of authentication and authorization: models, trends, etc., and the main frameworks and standards about the management of Authentication and Authorization security architectures: SAML, Kerberos, etc.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
● Holistically identify the different problems related to a specific area of cybersecurity.
● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new environments related to cybersecurity.
● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new environment in the field of cybersecurity.
● Design a presentation that includes the main ideas to be communicated, and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario.
● Present their knowledge in a clear, concise, unambiguous way and adapt to the time established for the presentation.
● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership.
● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization.
● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks.
● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks.</td></tr>
</table>

	● Plan autonomous work tasks and self-learning processes running at the scheduled times. ● Learn about new trends, good practices, standards and regulations related to the field of cybersecurity.		
Prerequisites	None	Co-requisites	None
Course Content	● Topic 1. Authentication, Authorization and Accounting o Definition, models, etc. ● Topic 2. User authentication (passwords, biometrics, authentication tokens, behaviour, 2FA, etc.). o Management models, authentication and authorization processes. o Current trends in authentication processes. o Legislation and regulation. ● Topic 3. Authentication in distributed systems. o Description of the main distributed systems, such as Kerberos, SAML, OpenID Connect, etc. o Characteristics, functionality and evaluation of architectures for authentication ● Topic 4. Access control and authorization systems. o Description of the main access control and authentication systems, such as OAuth or XACML. o Characteristics, functionality and evaluation of architectures for access control and authorization. Topic. ● Topic 5. Accounting Management (privacy, logs, etc.) for the monitoring of systems and infrastructures.		
Teaching Methodology	Face-to-Face		
Bibliography	1. Stallings, William, et al., Computer Security - Principles and Practice (2018) . Chapters 3 and 4 (topics 1 and 2) 2. Stallings, William, Cryptography and Network Security - Principles and Practice, Global Edition (2017). Chapters 16 and 18 (topic 3).		

	3. Solving Identity Management in Modern Applications. Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. Yvonne Wilson and Abhishek Hingnikar. Apress. Chapters 7 and 10 (Topics 3 and 4).
Assessment	Examinations 45.% Assignments 45 % Class Participation and Attendance 10% 100%
Language	English

Course Title	Malware and Attack Technologies				
Course Code	EMC224				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Juan Antonio Martínez Navarro, Félix Gómez Marmol				
ECTS	6	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main malware and attacks technologies.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Taxonomy of malware. Dimensions and characteristics. ● Malicious activities of malware ● Malware analysis. Analysis techniques, analysis environments. Analysis evasion techniques. ● Malware detection. Identify presence, attack detection. ● Response to malware. Stopping operations. Identification.				
Prerequisites	None		Co-requisites		None
Course Content	● Unit 1: Malware Classification ● Unit 2: Malware Forensics				

	● Unit 3: Sandboxes and Multi-AV Scanners, automation and dynamic analysis
Teaching Methodology	Face-to-Face
Bibliography	● Michael Ligh, Steven Adair, Blake Harstein, Matthew Richard. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley. 2010 ○ Chapter 3 (Unit 1) ○ Chapters 4, 7, 8, 9 (Unit 3) ● Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. 2012. ○ Chapters 11, 12, 13 (Unit 1) ○ Chapter 2 (Unit 2) ○ Chapter 3 (Unit 3) ∉ ● Abhijit Mohanta, Anoop Sldanha. Malware Analysis and Detection Engineering. A Comprehensive Approach to Detect and Analyze Modern Malware. 2020 ○ Chapter 19 (Unit 1) ○ Chapter 24 (Unit 3) ● Dylan Barker. Malware Analysis Techniques. Tricks for the triage of adversarial software. 2021. ○ Chapter 2 (Unit 2) ○ Chapter 3, 5, 6 (Unit 3)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	CyberSecurity Lab				
Course Code	EMC225				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Different teachers based on the projects labs				
ECTS	6	Lectures / week	1 Hours / 4 weeks	Laboratories / week	2 Hours / 14 weeks
Course Purpose and Objectives	This subject will have a structure in which the students per group must solve problems in a group, forming a response team and where they have to collaborate techniques and tools learned in the previous subjects, so that they can put the integration into operation in a practical way. of different tools. The formation of teams will be done so that students with different profiles can interact so that the teams can cover different aspects of solving cybersecurity problems. It will focus on carrying out simulated attack and reaction exercises where different teams can play different roles.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios. • Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. • Collect and analyze research data to address new problems in the field of cybersecurity.				

	• Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. • Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. • Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. • Analyze methods and techniques of cyber attacks and cyber defense. • List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to apply. • Carry out vulnerability and risk analysis processes. • Discuss the functionality of the elements incorporated in the architectures and security services of systems, critical infrastructures and communication networks. • Deploy monitoring elements in architectures and security services, critical infrastructures and communication networks. • Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communication networks..		
Prerequisites	First semesters courses	Co-requisites	None
Course Content	The master courses responsible will provide each year a collection of projects to be solved based on the interaction of different challenges covering different components and technologies already presented to the students. Students will organize in groups that will covered different aspects of a cybersecurity system that will solve the challenge		
Teaching Methodology	Face-to-Face		
Bibliography	• References from the different courses related to the technologies and techniques to be used		
Assessment	Assignments Class Participation and Attendance	80% 20% 100%	
Language	English		

Course Title	5G, IoT and Cyber-Physical Systems Security				
Course Code	EMC226				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	Ramón J. Sánchez Iborra, Miguel Ángel Zamora, Benito Úbeda Miñarro				
ECTS	6	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main security aspects to be considered in novel and evolving scenarios such as Internet of Things (IoT) deployments, Cyber-Physical Systems (CPS), Industrial Control Systems (ICS), and 5G architectures.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little-known environment in the field of cybersecurity. ● Collect and analyse research data to address new problems in the field of cybersecurity. ● Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account.				

	● Design solutions to cybersecurity problems using creative thinking. ● Design, deploy and maintain cybersecurity systems. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Describe the main elements and functions that are part of intelligent services, products and infrastructures in cybersecurity fields. ● Analyse scenarios in the field of cybersecurity from the point of view of the organization's security governance, the management of cybersecurity and the security of products, services and facilities. ● Design security management processes for products, services and facilities from the perspective of their security and considering business aspects (regulation, regulations, economic, etc.). ● Critically evaluate the processes of security governance, security management, design of products, processes, services and intelligent infrastructures in cybersecurity fields, taking into account into account requirements, existing solutions, regulations, standards and good practices. ● Deploy monitoring elements in security architectures and services, critical infrastructures, and communications networks. ● Analyse the security information collected through monitoring processes of system security architectures, critical infrastructures, and communications networks. ● Design security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering technical, business (economic, legal, environmental, etc.) and innovation aspects. ● Assess security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering aspects technical, business (economic, legal, environmental, etc.) and innovation		
Prerequisites	None	Co-requisites	None
Course Content	● Unit 1: IoT security architecture and requirements. ● Unit 2: IoT Protocols and their security. ● Unit 3: Identity, privacy and Access Management in IoT. ● Unit 4: Security in Industrial IoT/CPS. ● Unit 5. Security in Cellular Architectures.		
Teaching Methodology	Face-to-Face		

Bibliography	● B. Russell, D. Van Duren, Practical Internet of Things Security, 2016, Packt Publishing ● Sravani Bhattacharjee, Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries (English Edition), 2018. ● Larry Peterson and Oguz Sunay, 5G Mobile Networks: A Systems Approach. Open Networking Foundation (free book). 2020.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Advanced Techniques in Cyber Intelligence				
Course Code	EMC227				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Jorge Bernal and Antonio Skarmeta				
ECTS	6	Lectures / week	1,5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks
Course Purpose and Objectives	**Objective:** This course aims to teach students the current techniques, methods and tools for a holistic data processing, analysis and management of cyber intelligence information and systems. Students will be exposed to practical cyber intelligence techniques and tools. **Description:** The course will deal with architectures, formats and techniques for cyber threat intelligence (CTI) information management, data gathering and exchange,				

	including confidential and privacy-preserving CTI sharing. In addition, the course will provide the foundations and mechanisms for data analysis of CTI information coming from different sources (e.g., osints, social networks) using techniques based on Artificial intelligence. The analysis will be put in practice for diverse purposes such as anomaly detection in complex distributed/federated scenarios.
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Design cybersecurity scenarios, solutions, or systems including original or innovative aspects. ● Holistically identify the different problems related to a specific area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity. ● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. ● Collect and analyze research data to address new problems in the field of cybersecurity. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario ● Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity. ● Design solutions to cybersecurity problems using creative thinking. ● Analyze methods and techniques of cyber attacks and cyber defense. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Deploy monitoring elements in security architectures and services, critical infrastructures and communications networks. ● Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communications networks.

Prerequisites	None	Co-requisites	None
Course Content	● Cyber intelligence information management ○ Architectures, phases and processes associated with cyber intelligence. ○ Automatic techniques for capturing, exchanging and managing cyber intelligence information. ○ Formats and representation of cyber intelligence information ○ Privacy and confidentiality in the exchange of cyber intelligence information. ● Advanced processing of cyber-intelligence information ○ Detection of cyber attacks and threats based on Artificial Intelligence. ○ Scalable and federated AI-based cyber intelligence systems. ○ Advanced computational techniques for anomaly detection. ○ Analysis of data from social networks and other sources for Cyber-intelligence ○ Design and management of cyber intelligence systems: practical cases		
Teaching Methodology	Face-to-Face		
Bibliography	• Michel Bazzel, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. ISBN-13 : 979-8761090064. Section II (topic cyber intelligence information management) • Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense. ISBN-13 : 978-1800209404 Chapter 12,13,14 (topic cyber-intelligence) • Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers. ISBN-13 : 978-1484272190. Chapters 2,3, 7 (topic cyber intelligence) • Parisi, Alessandro. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019. ISBN-10: 1789804027, ISBN-13: 9781789804027. Chapter 4,5 (topic Advance processing of cyber-intelligence) • Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. " OReilly Media, Inc.", 2018. ISBN-10: # 1491979909, ISBN-13: 978-1491979907 Chapter 3,4,6 (topic Advance processing of cyber-intelligence)		

Assessment	Examinations Class Participation and Attendance Assignments	60% 10% 30% 100%	
Language	English		

Course Title	Hardware Security				
Course Code	EMC228				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Benito Ubeda and Miguel Angel Zamora				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks

<table>
<tr><td>Course Purpose and Objectives</td><td colspan="3">This course aims to provide holistic hardware security training and education in the design of new IoT and CPS devices, focus mainly in security aspects. This course contains a background of modern hardware devices with security issues and protection mechanism. During the course people will learn the different aspects of hardware security, which encompasses security vulnerabilities, attacks and protection mechanisms. The different hardware attacks will be analysed with examples: side-channel attacks, physical attacks, countermeasures and protections.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="3">Upon successful completion of this course students should be able to:
• Identify the main current problems in the field of cybersecurity in specific scenarios.
• Analyze in detail scenarios, solutions or cybersecurity systems to detect possible aspects of improvement.
• Design scenarios, solutions, or cybersecurity systems including original or innovative aspects.
• Holistically identify the different problems related to a specific area of cybersecurity.
• Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity.
• Evaluate the methods, secure protocols, cryptographic techniques or software tools to be used to undertake the resolution of a problem in a new or little-known environment in the field of cybersecurity.
• Use the knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development.
• Collect and analyze research data to address new problems in the field of cybersecurity.
• Identify the main aspects to be communicated when presenting the results of a study or analysis related to cybersecurity and to the public to which it is addressed.
• Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario.
• Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation.
• Analyze methods and techniques of cyber attacks and cyber defense..</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">Introduction to the main sources of vulnerability in hardware devices through the physical layer.
Hardware security assessment. Main standards and their certification.
Secure hardware platforms: HSM modules, TPM, secure elements, smartcards, etc.</td></tr>
</table>

	Review of basic techniques related to hardware security: Invasive methods: Cloning and manipulation of hardware at the chip level. Non-invasive methods: Electromagnetic coupling Techniques for secure implementations. Secure boot and OTP Prog memories Anti-tamper systems. Safe items. Entropy sources through hardware devices: Physically Unclonable Functions (PUF), Random Number Generators.
Teaching Methodology	Face-to-Face
Bibliography	The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. Jasper van Woudenberg And Colin O'Flynn (Autor). Nov 2021. • Chapters 1,5,6,7,8 and 10. Hardware Security A Hands-on Learning Approach. Swarup Bhunia Mark Tehranipoor. October 2018. • Chapters 1,5,6,7,8 and 10. Emerging Topics in Hardware Security. Mark Tehranipoor. 2021
Assessment	Examination 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Reliable Distributed Systems
Course Code	EMC229
Course Type	Elective
Level	Master (2nd Cycle)
Year / Semester	Y1/S2

Teacher’s Name	Ramón J. Sánchez Iborra, Juan Antonio Martínez Navarro, Miguel Ángel Zamora, Benito Úbeda Miñarro				
ECTS	3	Lectures / week	1.5 Hours / 7 weeks	Laboratories / week	1.5 Hours / 7 weeks e
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main security aspects of distributed systems in two main scenarios: (i) p2p architectures and applications, and (ii) distributed Industrial Control Systems (ICS).				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyse in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Design cybersecurity scenarios, solutions, or systems including original or innovative aspects. ● Apply methods, protocols, cryptographic techniques, or software tools to solve problems in new or little-known environments related to cybersecurity. ● Identify the different multidisciplinary aspects (legal, social, ethical) to take into account when dealing with a problem related to a cybersecurity scenario. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Design solutions to cybersecurity problems using creative thinking. ● Design solutions to cybersecurity problems using creative thinking. ● Identify the regulations and applicable legislation in the field of cybersecurity. ● Prepare clear, concise, and reasoned documentation on aspects related to the field of cybersecurity. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures, and communications networks. ● Discuss the functionality of the elements incorporated in system security architectures and services, critical infrastructure and communications networks. ● Describe the cryptographic primitives, the secure protocols and the software mechanisms that allow data protection. ● Employ the use of cryptographic primitives, secure protocols, and software models to protect data in a cybersecurity scenario.				

	● Identify new and emerging technologies, good practices, regulatory, legislative, and human aspects related to cybersecurity and the mechanisms to detect these changes. ● Plans autonomous work tasks and self-learning processes, executing them in the scheduled times. planned.		
Prerequisites	None	Co-requisites	None
Course Content	● Unit 1: P2P basics, architectures, applications and their security. ● Unit 2: Distributed ICS systems and their security.		
Teaching Methodology	Face-to-Face		
Bibliography	• B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” Comput. Electr. Eng., vol. 90, p. 106897, Mar. 2021, doi: 10.1016/j.compeleceng.2020.106897. • A. Abdelmaboud et al., “Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions,” Electronics, vol. 11, no. 4, p. 630, Feb. 2022, doi: 10.3390/electronics11040630. • Pascal Ackerman, Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment, 2nd Edition, Chapters 1,4,5,6,7,14 and 17. 2021 • Charles J. Brooks, Practical industrial cybersecurity, ics, industriy 4.0 and IoT, Chapters 2,3 and 5. 2022		
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%		
Language	English		

<table>
<tr><td>Course Title</td><td colspan="5">Offensive and Defensive Cybersecurity</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC231</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2/1</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Mario Polino</td></tr>
<tr><td>ECTS</td><td>5</td><td>Lectures / week</td><td>4 Hours / 13 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course builds on the basic knowledge introduced by the "Computer Security" course to introduce advanced topics dealing with cybersecurity and offensive security in particular. For this reason the course uses a teaching approach that combines a set of evolving frontal lectures, combined with practical lab exercises where students will learn and apply offensive security research techniques</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students are expected to be able to:
• know several advanced exploitation and counter-exploitation techniques, both for in-memory exploitation and for web application vulnerabilities.
• analyze code for vulnerabilities,
• write practically working proof-of-concept exploits, and assess mitigation techniques in the context of (for instance) cybersecurity competitions or real-world enterprise red teaming.
• know how disassemblers, symbolic execution and reversing software works, and will be able to practically use them for binary analysis, malware analysis and exploitation.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">- Fundamentals of exploitation of buffer overflow and format string vulnerabilities
- Fundamentals of web exploitation
- Understanding of X86 assembly</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5">1 Software & Hardware vulnerabilities, exploitation techniques and</td></tr>
</table>

	mitigation •Exploitation techniques for software vulnerabilities by example (e.g. ROP chaining, common protection bypasses, heap exploitation, format string exploitation) •Hardware Vulnerabilities •Web application vulnerabilities: exploitation of DOM-based XSS, CSP bypass, race conditions and other advanced web vulnerabilities •Penetration testing and red teaming in enterprise environments 2 Reverse engineering and Malware analysis •Binary analysis fundamentals •Reverse engineering techniques •Symbolic execution •Anti-debugging, packing •Malware analysis examples Laboratory exercises will cover: - reverse engineering fundamentals and tools (Ghidra, gdb, angr) - exploitation challenges to solve with the advanced techniques demonstrated
Teaching Methodology	Face-to-Face
Bibliography	Chris Anley, John Heasman, Felix "FX" Linder, Gerardo Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes, Editore: John Wiley and sons, Anno edizione: 2007 Chris Eagle, The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, Editore: No Starch Reverse Engineering for Beginners https://beginners.re/
Assessment	Examinations 40 % Assignments 60% Class Participation and Attendance 0% 100%
Language	English

Course Title	Digital Forensics and Cybercrime				
Course Code	EMC232				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher's Name	Stefano Zanero				
ECTS	5	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	Cybercrime is one of the most significant, and by far the most prevalent threat to digital infrastructure. In this course we will analyze the main mechanism, characteristics and drivers of cybercrime (including its underground economy). We will then analyze the techniques for forensic analysis of digital devices (with a specific attention to the Italian legal context and two dedicated case studies, but with a general overview of methodologies applicable internationally). Network forensics and cloud forensics will also be introduced. Finally, since most cybercriminals try to directly monetize their attacks, attention will be devoted to fraud detection technologies, and to technologies for tracking movement of digital currencies and cryptocurrencies.				
Learning Outcomes	Upon successful completion of this course, students are expected to be able to: • know the basics of underground economy, and the different dynamics and modus operandi of cybercriminals. • know the basic procedures and requirements of forensic analysis, both in a general and abstract way and in the particular case of the Italian legal framework. • know the techniques to properly preserve and analyze digital evidence of various types and from various sources. • understand the basics of antiforensic techniques. • use forensic tools to acquire sources and analyze simple disk images.				
Prerequisites	Students should have attended a basic security course. An understanding of file system principles and of basic networking technologies is helpful.	Co-requisites	None		

Course Content	Cybercrime 1.General landscape and modus operandi of cyber criminals 2.The underground economy and crime-as-a-service 3.Financially-motivated malware 4.Tracking cryptocurrency transactions in malware investigations 2.Fraud detection and analysis 1.Fraud: definitions, typical examples 2.Detecting frauds: operational measures 3.Machine learning techniques for fraud detection and analysis 4.Case studies 3.Digital forensics principles 1.Forensic science: repeatability, falsifiability; Daubert test; Italian legal framework 2.Digital Forensics phases 4.Source acquisition 1.Digital crime scene preservation principles 2.Acquisition of digital media 3.Acquisitions from network systems and from the cloud 4.Acquisition of mobile devices 5.Peculiarities and special cases 5.Forensic analysis of mass storage 1.Disk geometry, file systems, metadata 2.Deleted files recovery (including carving and slack space) 3.Repeatability of analysis and integrity preservation 4.Forensic tool examples (with practical demonstrations) 5.Anti-forensic techniques 6.Digital investigations: evaluation of evidence and presentation 1.Methodical doubts 2.Analysis of common mistakes 3.Aspetti di etica professionale A small set (8 hrs) of optional classes in Italian will be dedicated to Italian legal principles to be applied in forensics: repeatability standards and the way analysis is performed in Italian courts, along with 2 case studies of Italian legal proceedings.

Teaching Methodology	Face-to-Face
Bibliography	*Keith J. Jones, Richard Bejtlich, Curtis W. Rose*, Real Digital Forensics: Computer Security and Incident Response, Editore: Addison-Wesley, Anno edizione: 2005, ISBN: 978-0321240699
Assessment	Examinations 100% Assignments 0% Class Participation and Attendance 0% 100%
Language	English

Course Title	Data Science and Security for Mobility				
Course Code	EMC233				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher's Name	Prof Matteo Matteucci				
ECTS	10	Lectures / week	8 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	Data science aims at developing processes to analyze and ultimately understand phenomena through data. It stands at the intersection of several broad areas (statistics, information science, and computer science) and it employs methods from machine learning, classification, clustering, data mining, data bases, visualization, and cloud computing. This course presents the structure of the typical data science pipeline and, for each step of the process, reviews the most relevant methods and algorithms used to analyze mobility data. The course also tackles cyber-security risk in mobility applications. The course follows a problem-driven approach in that the techniques are presented based on the type of data they can tackle may these be structured (tables), unstructured (plain text, xml files), graphs, or time-series. All the methods are discussed focusing on the fundamental theory underlying them and their peculiarity, next they are demonstrated using either Python notebooks, KNIME workflows, and R. Topics discussed during the course include, but are not limited to, data and data representation, data preparation, regression, classification, clustering, evaluation of classification and clustering models, methods to analyze text, graphs, time series, and cyber-security risk as regards to the mobility landscape. The course comprises frontal lectures (60 hours) and practical data science hands-on lab (40 hours). During the laboratory hours, students will learn how to apply the techniques discussed during the lectures and will work on the mandatory course projects, presented at the start of the course, which must be completed by the last lecture for the course. The final grade will be based on an oral/written exam and the mandatory data science project.				

Learning Outcomes	Knowledge and understanding (Dublin Descriptor 1) Students will learn to - Understand the structure a data science pipeline - The fundamental characteristics of the most important algorithms used in all the major steps of the pipeline - Identify architectural styles and patterns Applying knowledge and understanding (Dublin Descriptor 2) Given specific data mining process, students will be able to: - Analyze and comment on specific architectural choices - Highlight possible criticalities including security vulnerabilities - Identify existing biases - Apply the theory to assess the reliability of the results produced Making judgements (Dublin Descriptor 3) Given a data mining task, students will be able to: - Analyze and understand the goals, assumptions and requirements associated with that task - Select the best environment to implement each step of the data mining process - Select the best infrastructure Communication (Dublin Descriptor 4) Students will learn to: - Analyze the design choices that a data analytics solution entails - Present and critically discuss the results of a data science process Lifelong learning skills (Dublin Descriptor 5) Students will learn how to: - Develop simple projects on real-world data and how to critically analyze a proposed solution and the result it produced		
Prerequisites	None	Co-requisites	None
Course Content	Introduction to Data Science The Data Science Pipeline Understanding Data and its Representation Regression Classification Clustering Text Mining Graph Mining Time Series Data Exploration and Preprocessing Cyber-security Risks and Applications to Mobility		
Teaching Methodology	Face-to-Face		

Bibliography	Jure Leskovec, Anand Rajaraman, Jeffrey D. Ullman, Mining of Massive Datasets http://www.mmds.org Mohammed J. Zaki and Wagner Meira, Jr., Data Mining and Analysis: Fundamental Concepts and Algorithms http://www.dataminingbook.info/ Ian H. Witten , Eibe Frank, and Mark A. Hall, Data Mining: Practical Machine Learning Tools and Technique, ISBN: 978-0123748560 http://www.pearsonhighered.com/educator/academic/product/0,1144,0321321367,00.html Machine Learning and Security: Protecting Systems with Data and Algorithms, Editore: O'Reilly Media, ISBN: 978-1491979907 http://shop.oreilly.com/product/0636920065555.do
Assessment	Examinations 50 % Assignments 50% Class Participation and Attendance 0% 100%
Language	English

Course title	Resilience of Critical Infrastructures				
Course code	EMC234				
Course type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Year 2/Semester 1				
Teacher's name	Dr Greta Nasi				
ECTS	5	Lectures / week	2 Hours/14 weeks	Laboratories / week	None
Course purpose and objectives	All sectors of our societies, from aircraft traffic to healthcare, electric grid and finance have been undergoing unprecedented levels of digitalization with beneficial consequences on efficiency and flexibility of services provided. However, this dependence on and seamless integration of technology into the daily activities and operations exposes these systems to various manmade and natural threats, with possible negative consequences on their security and even well-being of citizens. The constantly evolving threat landscape pushes the current concept of protection towards a resilience status. Moreover, the high interdependency and complexity of sectors require a multidisciplinary approach to educating the workforce called to safeguard it. Putting this strategy into practice, in turn, requires an unprecedented partnership and information sharing between the public and private sectors at all levels.				
Learning outcomes	**Knowledge and Understanding:** After successful completion of the course, students will be able to: • identify the vulnerability of the critical sectors in our economies to cyber risks, and recognize how to tackle them from a public sector perspective in order to define policies and programs, as well as put in place actions required to govern it. More specifically, they should be able to: • *acquire hands-on knowledge in identifying physical and cybersecurity concerns in the critical infrastructure systems and their centrality in modern societies (principal threats and challenges, who owns them)* • gain understanding and critically analyse approaches and methods of risk assessment and mitigation of persistent threats and incidents (how are threats/risks assessed & mitigated, are they useful in paving the way to resilient systems?) • develop knowledge about the specificity and interrelatedness of various CI systems				

	Ability to apply Knowledge and Understanding: • Analyse trends in the global system connected to the evolution of cyber risk, interpret how they affect government activities and define policies, programs and road maps for governing it.		
Prerequisites	None	Co-Requisites	None
Course content	**Critical Infrastructure in the EU and the Italian context** • General overview on critical infrastructure sectors: CIs' definition, evolution and sectors • The evolution of CI in the cybersecurity era • Critical infrastructures' governance: US and EU as a model **Frameworks for critical infrastructure protection** • From threat-based to value-informed approaches to cybersecurity • Premises: brief analysis of the ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF) **Cyber Resilience in Healthcare** The state of health: key figures and relevance of the healthcare sector ● Health and cybersecurity: state of the art and threat landscape ● A holistic approach to managing risks: cyber resilience of the healthcare sector **Cyber Resilience in Water Management Systems** What is the water management ecosystem and why it is relevant ● Complex theory as an instrument to assess the risks ● The human factor as element of risk and mitigation **Cyber Resilience in the Information Technology & Telecommunications Sectors** • ICT and Telco: framing the industry • Key technologies and risks to govern • EU policies and actors in shaping cyber policies for the ICT and Telco **Trends in Cyber Resilience, Group Presentations and Wrap Up** • Trends in other key sectors • Group presentations • Wrap up of PART A		
Teaching methodology	Face-to-face lectures, guest speakers' talk, case studies, analysis of incidents. The learning experience of this course includes, in addition to face-to-face lectures, thought experiments, case discussions, real examples and interactions with guest speakers from different organizations.		

	Each lecture will include: a) An overview of the current dynamics and issues at stake; b) a practical exercise, that could be made by a guest speaker lecture, a case study, an instant group work; c) A wrap-up of the themes emerged
Bibliography	COUNCIL DIRECTIVE on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. European Commission 2008 EU Directive 2016/1148 EU Directive 2022/2555 ACN, NATIONAL CYBERSECURITY STRATEGY 2022 – 2026 Kaplan, J., Toomey, C., and Tyra A. (2019) Critical resilience: Adapting infrastructure to repel cyber threats. McKinsey & Company Genge, B., et al. (2015). "A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures." International Journal of Critical Infrastructure Protection 10: 3-17 ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF), ENISA April 2022 Agrafiotis, I., et al. (2018). "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." Journal of Cybersecurity 4(1) Erola, A. et al. (2022). " A system to calculate Cyber Value-at-Risk" in Computers & Security, V. 113 Martin, G., Martin, P., Hankin, C.C., Darzi, A., & Kinross, J.M. (2017). Cybersecurity and healthcare: how safe are we? British Medical Journal, 358. He Y, Aliyu A, Evans M, Luo C Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review J Med Internet Res 2021;23(4):e21747 doi: 10.2196/21747 Sanger, D. E. & S. LaFraniere (2020) "Cyberattacks Discovered on Vaccine Distribution Operations" The New York Times. Wetsman, N. (2020) "Woman dies during a ransomware a!ack on a German hospital" The Verge. Germano J.H. Cybersecurity Risk and responsibility in the water sector AWWA Florida Hack Exposes Danger to Water Systems

	ENISA Assessment of the EU security legislation. Ignatius A. (2020) Verizon’s CEO on peak traffic, cybersecurity, and leading a team from home. Harvard Business Review Perlroth N. (2021). “How the US lost to hackers”, The New York Times. McGuinness, D. (2017). “How a cyber attack transformed Estonia”, BBC News. DORA - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 Mee, P. & T. Schuermann (2018). “How a Cyber Attack could cause the next financial crisis”, Harvard Business Review.
Assessment	Grading methods involves multiple assessment methods including: - Group project presentation - Written exam for the part of the course
Language	English

Course Title	Cryptography and Architectures for Computer Security				
Course Code	EMC235				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher’s Name	Gerardo Pelosi				
ECTS	5	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	The course provides a systematic formation on the cryptographic techniques currently employed in communication and data storage. It focuses on the algorithms, the related HW/SW efficient architectures, and points out the new trends and crypto-schemes under development. It extends and closely examines how to effectively and correctly use cryptography in the broad field of computer security. The mathematical aspects of modern cryptography are presented, preceded by a comprehensive introdution to the needed notions of algebra. The most important cryptographic schemes are presented, together with their practical realization details, APIs and implementation vulnerabilities. Furthermore, the most common communication protocols (SSL/TLS, SSH, PGP, Kerberos, Onion Routing) and data storage protocols (IEEE P1619 standard used in Truecrypt) are described. Hardware and software architectures for efficient and implementation-secure realizations of cryptographic schemes are presented and detailed for real-world systems. The course interleaves mathematical topics and more engineering-oriented topics through merging theoretical and practical aspects. These concepts are relevant for a system designer in need to properly use the cryptographic technologies in system and application contexts, and to an hardware designer in need to secure digital architectures.				
Learning Outcomes	**Knowledge and understanding:** students will learn: 1) the design principles of historical and modern symmetric-key ciphers; in particular they will understand the concept of perfect secrecy and the principles underlying the round structures of block ciphers, the structure of stream ciphers and how to assess the resistance of a block cipher against the linear and differential cryptanalyses;				

	2) the notions of cryptographic hash functions and the principles underlying their most common constructions as well as how to effectively employ them given the requirements of a target application; 3) the notions of algebra related to cyclic groups, rings and finite fields that are at the core of asymmetric-key ciphers. 4) the inner working of RSA, ElGamal and Diffie-Hellmann cryptosystems as well as of their variants based on elliptic curve arithmetic; 5) the implementation criteria of asymmetric cryptosystems in the most common software and hardware systems; 6) how the cryptographic primitives are effectively employed in popular protocols employed for authentication, secure communication and secure data storage. **Applying Knowledge and understanding:** given a hardware or software system (or a composition thereof) requiring one or more security services to deal with data in trasfer or at rest, the student will be able to identify the composition of cryptographic primitives that best match the requirements motivating their choices. In addition, the acquired notions and knowledges will enable them to read and understand the description of more recent developments concerning secure protocols and applications. **Making judgements:** given a cryptographic application, students will be able to analyze and understand its security requirements and will be able to recommend the best configuration parameters and to suggest modifications to the system, keeping into account also implementation issues. **Communication:** students will learn how to clearly and concisely express in writing their technical assessments concerning theoretical and practical security solutions. **Lifelong learning skills:** students will learn how to properly choose and configure a cryptographic system, as well as assessing whether the cryptographic building blocks are properly used in complex systems and protocols.		
Prerequisites	Students should have attended a basic security course. An understanding of file system principles and of basic networking technologies is helpful.	Co-requisites	None
Course Content	**[Cryptography principles and algorithms]**		

	Security services: confidentiality, integrity, authentication and non-repudiation History of cryptography Foundations of modern cryptography Symmetric algorithms and modes of operation Elements of modern block cipher cryptanalysis Hash functions Asymmetric algorithms (RSA, ElGamal, Diffie-Hellman, Elliptic Curve based Cryptosystems) Elements of asymmetric cipher cryptanalysis **[Architectures and protocols]** Efficient asymmetric cipher implementations Public Key Infrastructure, Web of Trust and distributed notary schemes Secure (SSL/TLS, SSH) and anonymous (onion routing) communication protocols Secure data storage protocols: IEEE P1619 standard Secure authentication schemes, bruteforcing-safe password storage and Kerberos Security-aware device architectures: cryptographic accelerators and crypto-processors Primer on Side channel attack methodologies and countermeasures
Teaching Methodology	Face-to-Face
Bibliography	*Nigel P. Smart*, Cryptography, An Introduction : Third Edition, Anno edizione: 2008 http://people.cs.bris.ac.uk/~nigel/Crypto_Book/ *J. Katz and Y. Lindell,*, Introduction to Modern Cryptography, Editore: Chapman & Hall, Anno edizione: 2007 http://www.cs.umd.edu/~jkatz/imc.html
Assessment	Examinations 100 % Assignments 0% Class Participation and Attendance 0% 100%
Language	English

Course Title	Safety in Automation Systems				
Course Code	EMC236				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher's Name	Scattolini Riccardo				
ECTS	5	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	The first part of the course is aimed at allowing the student to learn and apply the main techniques for the hazard and reliability analysis of industrial systems, such as Preliminary Hazard Analysis, Failure Mode and Effect Analysis, Fault Tree Analysis. In the second part, the course focuses on the most widely used methods for the fault detection and diagnosis of complex systems. In particular, the main data-driven methods are discussed, such as control charts and principal component analysis. Analytical fault detection techniques based on state observers, parity space equations, recursive estimation algorithms are also presented. Finally, some methods for the design of fault tolerant control systems are described. All these methods are applied to some industrial test cases to witness their potentialities and limitations.				
Learning Outcomes	Lectures and exercise sessions will allow the students to: • Complete a functional and architectural analysis of the system, and to define the main reliability indices, operating modes, targets, risks. • Apply the main System Hazard Analysis techniques used in industry, to specific test cases. • Draw conclusions and propose modifications in the design phase to improve the safety. • Apply univariate and multivariate statistical analysis to detect on-line faults or operational changes of the system. • Design fault detection methods to improve the safety and implement predictive maintenance procedures. • Design fault tolerant control schemes. The laboratory training sessions will make use of computer simulation tools and will allow students to learn how to: • Simulate a dynamic system in safe and fault conditions.				

	• Implement fault detection algorithms. • Design and test fault tolerant control schemes.		
Prerequisites	Students are required to know: Basics of automatic control, observer design methods, model predictive control. Basics of model identification, filtering and data analysis.	Co-requisites	None
Course Content	Introduction to the safety analysis of industrial systems. Preliminary Hazard Analysis and HAZard and OPerability analysisin automation systems. Risk analysis techniques: Failure Mode and Effect Analysis, Fault Tree Analysis, Cause Consequence Analysis. Introduction to the fault detection problem: data-driven and analytical redundancy methods, qualitative approaches. Statistical Quality Control, control charts, principal component analysis. On-line diagnosis with parity space equations, state observers, parameter estimation. Design of fault tolerant control systems.		
Teaching Methodology	Face-to-Face		
Bibliography	A. Villemeur, Reliability, availability, maintainability and safety assessment, Editore: Wiley & Sons, Anno edizione: 1991 L.H. Chiang, E.L. Russel, R.D. Braatz, Fault detection and diagnosis in industrial systems, Editore: Springer, Anno edizione: 2001 J.J. Gertler, Fault Detection and diagnosis in engineering systems, Editore: Marcel Dekker, Anno edizione: 1998		
Assessment	Examinations Assignments Class Participation and Attendance	50% 50% 0% 100%	
Language	English		

Course Title	Computer Ethics				
Course Code	EMC237				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher's Name	Viola Schiaffonati				
ECTS	5	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	This course deals with the application of ethical theories to problems created, aggravated or transformed by computer technology. It is intended to give students a chance to reflect on the ethical, social, and cultural impact of computer technology by focusing on the issues faced by and brought about by computing professionals. The course includes lectures by the instructor and invited lecturers; class participation will be expected, and students should apply what they learn through readings and lectures by looking at current events through an ethical lens.				
Learning Outcomes	**Dublin Descriptors** **Expected learning outcomes** Knowledge and understanding Students will: • Acquire a broad perspective on the ethical and social impacts and implications of information technologies; • Be acquainted with normative ethics and normative argumentation; • Learn how to recognize and analyze ethical and social aspects and issues inherent in technology; • Be able to understand how technical problems are inherently connected to a social dimension within a socio-technical perspective. Applying knowledge and understanding Students will: • Be able to use critical skills in clarifying and ethically analyzing cases-studies involving information technology; • Be able to apply ethical theories to problems created, aggravated or transformed by computer technology; • Be able to explore and assess possibilities for solving or				

	diminishing existing and emerging ethical and social problems that attach information technology. Making judgements Students will be able: • To autonomously analyze the ethical theories to problems created, aggravated or transformed by computer technology; • To evaluate and select the appropriate knowledge in the effort of elaborating and justifying a philosophical argument on a topic autonomously selected. Communication Students will learn to: • Exercise and improve their skills in critical writing; • Present in an effective way the results of their independent research, being able to justify their choices. Lifelong learning skills Students will: • Be better prepared to their future professional life in an ethically and socially responsible way; • Be able to analyze problems through an ethical lens.		
Prerequisites		Co-requisites	None
Course Content	The course will cover different topics both from a theoretical and a more practical point of view. We will start with a broad analysis of the concept of **responsibility**, in particular in an **engineering perspective**, and of **normative ethics** and its tools. We will introduce **codes of conduct** with a detailed discussion about the ACM and IEEE Codes. We will discuss **ethical questions** in the **design of technology** with a focus on **Design Ethics** and its **Social Ethics paradigm**. Then **ethics in IT-configured societies** will be discussed **and technology as the instrumentation of human action** will be presented. Within this context we will focus: on **information flow**, **privacy**, and **surveillance**, on **digital intellectual property** and on **digital order**. Students will be supervised in the development of the **final project** (either written paper or class presentation) in order to meet the standards required by scientific publications.		
Teaching Methodology	Face-to-Face		
Bibliography	*van de Poel, L. Royakkers*, Ethics, technology and engineering: An		

	introduction, Editore: Wiley-Blackwell, Anno edizione: 2011 *Deborah Johnson*, Computer Ethics, Editore: Pearson, Anno edizione: 2009
Assessment	Examinations 50 % Assignments 50% Class Participation and Attendance 0% 100%
Language	English

Course Title	Artificial Neural Networks and Deep Learning				
Course Code	EMC238				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2/1				
Teacher’s Name	Prof Matteo Matteucci				
ECTS	5	Lectures / week	4 Hours / 13 weeks	Laboratories / week	None
Course Purpose and Objectives	Nowadays, deep neural networks can outperform traditional hand-crafted algorithms, achieving human performance in solving many complex tasks, such as natural language processing, text modeling, gene expression modeling, and image recognition. The course provides a broad introduction to neural networks (NN), starting from the traditional feedforward (FFNN) and recurrent (RNN) neural networks, till the most successful deep-learning models such as convolutional neural networks (CNN) and long short-term memories (LSTM). The course's major goal is to provide students with the theoretical background and the practical skills to understand and use NN and at the same time become familiar with Deep Learning for solving complex engineering problems. This goal is pursued in the course by Presenting major theoretical results underpinning NN (e.g., universal approx, vanishing/exploding gradient, etc.) Describing the most important algorithms for NN training (e.g., backpropagation, adaptive gradient algorithms, etc.) Illustrating the best practices on how to successfully train and use these models (e.g., dropout, data augmentation, etc.) Providing an overview of the most successful Deep Learning architectures (e.g., convolutional networks, autoencoders for embedding, long-short term memories for sequence to sequence learning, etc.) Providing an overview of the most successful applications with particular emphasis on models for solving visual recognition tasks.				
Learning Outcomes	Dublin Descriptors Expected learning outcomes				

	Knowledge and understanding Students will learn: · What are neural networks and the fundamental methods and techniques used for neural networks training · What are the fundamental architectures used in deep learning, such as convolutional neural networks and long-short term memories, and when to use them · What are the neural network architectures used in the different visual recognition tasks · What are the main differences between machine learning and deep learning Applying knowledge and understanding Given a specific data analysis problem, the student will be able to: · Identify which paradigm better describes a given problem · Identify which technique to start from with the analysis, apply it to model the data and evaluate its outcome · Implement fundamental deep learning algorithms for image and text analysis autonomously Making judgments Given a complex data analysis problem, students will be able to: · Identify the most relevant model to be applied in the specific problem · Identify the occurrence of overfitting by the model under analysis · Iteratively refine the selected model in order to balance performance, computational complexity and overfitting · Compare and select different models for the problem under analysis Communication The student will learn to: · Discuss in written form the pros and cons of different machine learning techniques for a specific problem Lifelong learning skills The student will learn to: · Face a real-life data analysis problem with a sound and complete methodological approach · Understand complex machine learning techniques beyond the fundamental ones presented during lectures · Develop new machine learning pipelines adapting to the specific problem at hand		
Prerequisites	This is a basic course that has no specific background	Co-requisites	None

	requirement but basic notions in calculus, linear algebra, and statistics. In particular, we expect students to be comfortable with derivatives to understand the relationship between backpropagation¸ gradient descent and non-linear optimization, and with the maximum likelihood principle.		
Course Content	Neural networks are mature, flexible, and powerful non-linear data-driven models that have successfully been applied to solve complex tasks in science and engineering. The advent of the deep learning paradigm, i.e., the use of (neural) network to simultaneously learn an optimal data representation and the corresponding model, has further boosted neural networks and the data-driven paradigm. These topics will be described in the course according to the following detailed program: •From the Perceptron to Neural Networks and the Feedforward architecture •Backpropagation and Neural Networks training algorithms, e.g., Adagrad, adam, etc. •Best practices in neural network training: overfitting and cross-validation, stopping criteria, weight decay, dropout, data resampling and augmentation. •Image Classification problem and Neural Networks •Recurrent Neural Networks and other relevant architectures such as (Sparse) Neural Autoencoders •Theoretical results: Neural Networks as universal approximation tools, vanishing and exploding gradients, etc.		

	•Introduction to the Deep Learning paradigm and its main differences with respect to classical Machine Learning •Convolutional Neural Networks (CNN) architecture •The breakthrough of CNN and their interpretation •CNN training and data-augmentation •Structural learning, Long-Short Term Memories, and their applications to text and speech •Autoencoders and data embedding, word2vec, variational autoencoders •Transfer Learning for pre-trained Deep models •Extended models including Fully Convolutional CNN, networks for image segmentation (U-net) and object detection (e.g., R-CNN, YOLO) •Generative Models (e.g., Generative Adversarial Networks)
Teaching Methodology	Face-to-Face
Bibliography	*Ian Goodfellow, Yoshua Bengio, and Aaron Courville*, Deep Learning, Editore: MIT Press, ISBN: 978-0262035613
Assessment	Examinations 70 % Assignments 30% Class Participation and Attendance 0% 100%
Language	English

TRACK 3

Course Title	Cyberattack Techniques and Ethical Hacking				
Course Code	EMC311				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	Antonio Ruiz Martínez, Félix Gómez Mármol				
ECTS	6 ECTS	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks
Course Purpose and Objectives	The goal of the course is to introduce students in attacking computer systems through an ethical hacking process. Students will know the different kind of security assessments that could be made and they will learn the different steps of a ethical hacking process through some laboratories where they will attack an scenario.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. • Collaborate when solving a problem in the field of cybersecurity, teamwork, and leadership. • Analyze methods and techniques of cyber-attacks and cyber-defense. • Design, deploy, and maintain cybersecurity systems. • Identify applicable regulations and legislation in the field of cybersecurity. • Elaborate clear, concise, and reasoned documentation on aspects related to the field of cybersecurity. • List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to be applied. • Perform vulnerability and risk analysis processes. • Classify vulnerabilities, threats and risks within the organization to determine their importance, taking into account the context.				
Prerequisites	None	Co-requisites	None		
Course Content	• Introduction to Ethical hacking o Basic concepts				

	o Regulations and associated legislation • Security assessments. o Types of assessments o Methodologies o Training • Ethical hacking process. o Deployment of scenario and realization of ethical hacking process.
Teaching Methodology	Flipped classroom, project-based learning
Bibliography	• CEH™ v12 - Certified Ethical Hacker - Study Guide o Topic 1. Chapter 1. o Topic 2. Chapter 2. o Topic 3. Chapters 2, 4, 5, 6, 7, 9, 10, 11 and 12. • Desmond, Brian, et al. Active Directory: Designing, Deploying, and Running Active Directory. " O'Reilly Media, Inc.", 2008. o Topic 3. Chapters 2, 4 and 5.
Assessment	Examinations 30% Assignments 60% Class Participation and Attendance 10% 100%
Language	English

Course Title	CyberDefense Techniques				
Course Code	EMC312				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	José Ramón Hoyos-Barceló and ?				
ECTS	6	Lectures / week	1,5 Hours /14 weeks	Laboratories / week	1,5 Hours /14 weeks
Course Purpose and Objectives	This course integrates an introduction to different ways of protecting the underlying communication networks and the detection of and response to security incidents, with a focus on computer forensics and the collection, analysis and reporting of digital evidence in support of incident or criminal events.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios. • Analyse in detail cybersecurity scenarios, solutions or systems in order to detect possible areas for improvement. • Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or unfamiliar environments related to cybersecurity. • Identify the different multidisciplinary aspects (legal, social, ethical) to be taken into account when dealing with a problem related to a cybersecurity scenario.				

	• Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. • Formulate value judgements on the basis of collected information that, while incomplete or limited, include critical reasoning on the social and ethical responsibilities of the application of methods, cryptographic techniques, software tools or methodologies to address cybersecurity-related problems. • Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and to the target audience. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be conveyed with regard to a cybersecurity scenario. • Present your knowledge in a clear, concise and unambiguous manner, adapting to the time set for the presentation. • Analyse methods and techniques of cyber-attacks and cyber-defence. • Produce clear, concise and reasoned documentation on aspects related to the field of cybersecurity. • Identify the characteristics and functions of the elements that form part of the security architectures and services of systems, critical infrastructures and communications networks.		
Prerequisites	None	Co-requisites	None
Course Content	Defense tools and Incident Management Unit 1- Network defence and monitoring tools Unit 2- Incident management and disaster recovery, cyber incident reporting Computer Forensics Unit 3- Introduction to Computer Forensics Unit 4- Situation assessment and collection of evidence Unit 5- Evidence Analysis Unit 6- Computer expertise		
Teaching Methodology	Face-to-Face		
Bibliography	1. Guide to Computer Network Security, 5th edition, by Joseph Migga Kizza. Springer (3: Security Threats, 5 Cyber Crimes and Hackers, 8 Disaster Management) 2. Stallings, William, et al., Computer Security - Principles and Practice (2018) (1.1 Computer security concepts; 1.2 Theats, attacks and assets; 8: Intrusion detection, 9: Firewall and Intrusion Prevention Systems, 14: IT Security Management and Risk Assessment, 15: IT Security Controls, Plans and Procedures, 17 Human resource security.)		

	3. Digital Forensics Explained. Greg Gogolin. CRC Press/Taylor & Francis Group. 2021 (1. What is digital forensics, 2.Digital forensic approaches, 3. Digital forensics tool kit, 7 Incident response, 10 Social engineering, 11 Anti-forensics) 4. Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730. (full article)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Cybersecurity and Network Security</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC313</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S1</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Rafael Marín López, Óscar Cánovas</td></tr>
<tr><td>ECTS</td><td>6 ECTS</td><td>Lectures / week</td><td>1.5 Hours / 14 weeks</td><td>Laboratories / week</td><td>1.5 hours/14 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The goal of the course is to analyse, discuss different network security protocols at different layers ranging from link-layer to application layer. The course will also pay attention to non-cryptographic defence tools and standards related with network security.</td></tr>
</table>

<table>
<tr><td>Learning Outcomes</td><td colspan="3">Upon successful completion of this course students should be able to:
● Identify the main current problems in the field of cybersecurity in specific scenarios.
● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement.
● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity.
● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity.
● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development.
● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario.
● Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation.
● Design solutions to cybersecurity problems using creative thinking.
● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership.
● Analyze methods and techniques of cyber attacks and cyber defense.
● Prepare clear, concise and reasoned documentation on aspects related to the field of cybersecurity.
● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks.
● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks.
● Describe the cryptographic primitives, the secure protocols and the software mechanisms that allow data protection.
● Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of secure software.
● Employ the use of cryptographic primitives, secure protocols and software models to protect data in a cybersecurity scenario.
● Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes.
● Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
</table>

Course Content	● Network protocols and vulnerabilities: adversary models, types of attack. ● Application-level security (public key and symmetric key management, application-level protection (SSH, S/MIME), application services security) ● Transport level security (TLS, DTLS, QUIC) ● Network level security (ACLs, IPv6 security, routing protocol security, VPNs) ● Link level security: wireless level security (IEEE 802.1X, EAP, RADIUS, DIAMETER, WPA) attacks on ethernet switches, MAC level attacks. ● Non-cryptographic defense tools (packet filtering, firewall, DMZ, IDS, IPS, etc.) ● Advanced security topics (SDN, NFV, IoT) ● Communication security standards (how security protocols are specified and documented)
Teaching Methodology	Face-to-Face
Bibliography	● W. Stalling CRYPTOGRAPHY AND NETWORK SECURITY, EIGHTH EDITION – 8th ○ Chapter 1. Computer and Network Security Concepts (Block I) ○ Chapter 18 Wireless Network Security (Block I) ○ Chapter 17 Transport-Layer Security (Block III) ○ Chapter 20 IP security (Block III) ○ Chapter 21 Network Endpoint Security (Block II) ∉
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Techniques for the Management of the Cybersecurity</td></tr>
<tr><td>Course Code</td><td colspan="5">EMC314</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S1</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Manuel Gil Pérez</td></tr>
<tr><td>ECTS</td><td>6</td><td>Lectures / week</td><td>3 Hours / 14 weeks</td><td>Laboratories / week</td><td>3 Hours / 14 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective of this course is to cover aspects related to organisational security governance and the security project management, including</td></tr>
</table>

	the identification of security risks in the protected organisation together with potential countermeasures to apply for risk reduction.		
Learning Outcomes	Upon successful completion of this course students should be able to: • Holistically identify the different problems related to a specific area of cybersecurity. • Identify the different multidisciplinary aspects (legal, social, ethical) to consider when dealing with a problem related to a cybersecurity scenario. • Plan autonomous work tasks and self-learning processes running at the scheduled times. • Enumerate and identify the different types of vulnerabilities, threats, and risks within the organisation, as well as possible solutions to be applied. • Describe the principles of risk management, how to apply them and possible tools to be used. • Describe the main elements and functions that are part of smart services, products, and infrastructures in the cybersecurity domain. • Explain the different aspects related to organisational security governance, security project management, design and implementation of products, services, and facilities in cybersecurity scenarios.		
Prerequisites	None	Co-requisites	None
Course Content	Management of information security systems: • Unit 1. Information security legislation in Spain o National Security Scheme: objectives, requirements, and security measures • Unit 2. Information Security Management Systems (ISMS) – *ISO 27000* • Unit 3. Implementation and evaluation of ISMS according to the stages of the Deming cycle: plan, do, check, act • Unit 4. Security and resilience plans – *ISO 22300 family* Analysis and management of security risks: • Unit 5. Analysis, assessment, and treatment of security risks o Security Master Plan • Unit 6. Methodologies for security risk analysis o NIST SP 800, MAGERIT / PILAR • Unit 7. Countermeasures for risk reduction Practices: • Case studies for applying security management tools		

	• Implementation and audit of Information Security Management Systems (ISMS) o Audit automation and standardisation, following the ANA approach • Risk analysis and selection of countermeasures o Use of µPILAR for risk analysis and choice of safeguards, analysing the residual risk
Teaching Methodology	Face-to-Face
Bibliography	4. Gibson, Darril (2020). Managing Risk in Information Systems (Information Systems Security & Assurance). Jones and Bartlett Publishers, Inc. 5. Tiller, James S., O'Hanley, Richard (2013). Information Security Management Handbook, Volume 7 (6th Ed.). Auerbach Publications. 6. Spanish Ministry of Finance and Civil Service (2014). MAGERIT V.3: Methodology for Information Systems Risk Analysis and Management. Edita.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cryptography
Course Code	EMC315
Course Type	Compulsory
Level	Master (2nd Cycle)
Year / Semester	1st Year / 1st Semester

Teacher's Name	Leandro Marín Muñoz				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hour / 7 weeks
Course Purpose and Objectives	The objective of this course is to give a broad view of cryptography, studying both the mathematical and theoretical aspects as well as the aspects related to their implementation in special environments.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Solve problems related with theoretical and mathematical cyptology. • Evaluate the security of cryptographic methods. • Apply their knowledge about cryptology in research. • Understand the mathematical foundations of cybersecurity.				
Prerequisites	None	Co-requisites	None		
Course Content	Cryptographic security models. Secret sharing systems. Symmetric cryptography (block ciphers, stream ciphers, digital hash functions, message authentication codes, Merkle trees and block chains), public key cryptography (RSA-based, elliptic curve and lattice constructs, digital signatures), cryptographic protocols (authentication, key exchange, zero knowledge, secure multiparty computing), advanced aspects of cryptography (group/ring-based signatures, identity-based ciphers, homomorphic cryptography, side-channel attacks, implementations in environments with special requirements such us low power consumption, memory restrictions, etc.)"				
Teaching Methodology	Face-to-Face				
Bibliography	● Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. 2007. CRC Press. Chapter 3 (Private Key Cryptography) Chapter 5 (Block Ciphers) Chapter 10 (Public Key Encryption) Chapter 12 (Digital Signatures) ● Henri Cohen. A Course in Computational Number Theory. 1993. Springer. Chapter 1 (Basic Number Theory) Chapter 8, 10 (Factorization) Chapter 9 (Primality Testing) ● Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography. 2003. Springer. Chapter 2 (Elliptic Curves) Chapter 4 (Implementation Issues on ECC) ● FIPS 197. Advanded Encryption Standard (AES) – NIST. ● Craig Gentry. A Fully Homomorphic Encryption Scheme (Ph.D. Thesis). (only the introduction for homomorphic encryption)				

Assessment	Examinations	60%
	Class Participation and Attendance	10%
	Assignments	30%
		100%
Language	English	

Course Title	Innovation and Entrepreneurship Seminar

Course Code	EMC316				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher’s Name	Responsible Antonio Skarmeta Different participants based on seminars				
ECTS	3	Lectures / week	3 Hours / 7 weeks	Laboratories / week	
Course Purpose and Objectives	The objective is to bring students closer to the most pressing problems and solutions at all times in industry, administration, defense and research. Through the different seminars proposed, students will have access to the experience of professionals of recognized prestige whose professional work is related to Cybersecurity in its legal, administrative, management and legal aspects. On the other hand, the more academic seminars will put students in contact with the state of the art in concepts, protocols, developments and tools on specific topics related to cybersecurity. Therefore, the seminars may be framed within any of the subjects of the master's degree				
Learning Outcomes	Upon successful completion of this course students should be able to: • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. • Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity. • Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes. • Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.				
Prerequisites	None	Co-requisites	None		
Course Content	Within the master's degree, seminars will be given that may change from year to year, as advised by a field as variable as cybersecurity. Yearly the planning of seminar will be defined				

Teaching Methodology	Face-to-Face
Bibliography	
Assessment	Assignments 60% Class Participation and Attendance 40% 100%
Language	English

Course Title	Cybersecurity Legal Framework

<table>
<tr><td>Course Code</td><td colspan="5">EMC321</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 2nd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Julián Valero Torrijos</td></tr>
<tr><td>ECTS</td><td>3</td><td>Lectures / week</td><td>2 Hours / 7 weeks</td><td>Laboratories / week</td><td>1 Hours / 7 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5"><b>Objective:</b>
This course aims to provide students with an overview of the main legal aspects of cybersecurity, in particular from the perspective of European Union legislation. Specifically, it will provide the basic tools to identify the relevant rules, understand the basic legal concepts and then proceed to their application, considering the singularities of the digital environment.
<b>Description:</b>
Cybersecurity is nowadays a basic requirement for the development of digital services and contents, so that its legal framework has become an essential topic for IT sector professionals. This course will provide an overview of the legal framework of cybersecurity, taking into account its impact on fundamental rights and public freedoms, the intervention of public administrations in both the regulation of activities and their enforcement, as well as the implications from the perspective of criminal law.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Identify the regulations and legislation applicable in the field of cybersecurity.
• Understand the main legal concepts in the field of cibersecurity.
• Identify the main legal aspects to be taken into account when dealing with a problem related to a cybersecurity scenario.
• Produce clear, concise and reasoned documentation including legal requirements of cybersecurity.
• Define a risk management policy taking into account legal requirements.
• Apply the legal concepts and rules associated with cybersecurity scenarios.
• Design safety management processes for products, services and facilities from the perspective of their legal requirements.
• Identify new and emerging technologies, best practices, regulatory, legislative and ethical aspects related to cybersecurity and mechanisms to detect these changes.</td></tr>
</table>

	• Adapt cybersecurity scenarios in line with new trends, best practices, standards, regulation and human aspects. • Assess the legal implications and risks of adopting new technologies from the perspective of cybersecurity in concrete business scenarios.		
Prerequisites	None	Co-requisites	None
Course Content	- General regulatory framework. European and Spanish regulation on cybersecurity and protection of critical infrastructures. - Personal data protection regulation. Singularities in the public sector. The Spanish National Security Scheme. - Cybersecurity and digital services. The singularities of financial services and payment tools. - Trust services legal framework. Digital identity - Criminal law and cybersecurity.		
Teaching Methodology	Face-to-Face and Online activities		
Bibliography	**EU LAW** - Jozef Andraško, Matúš Mesarčík, Ondrej Hamuľák: “The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework”, AI & SOCIETY volume 36, p. 623–636 (2021) - Dimitra Markopouloua, Vagelis Papakonstantinoua, Paulde Hert: “The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation”, Computer Law & Security Review, Volume 35, Issue 6, November (2019). - Gloria González Fuster, Lina Jasmontaite: “Cybersecurity regulation in the European union: the digital, the critical and fundamental rights”, The ethics of cybersecurity. Springer, Cham, p. 97-115 (2020). - Pier Giorgio Chiara: “The IoT and the new EU cybersecurity regulatory landscape”, International Review of Law, Computers & Technology, 36:2, 118-137 (2022). **SPANISH LAW** - Alamillo Domingo, A.: Identificación, firma y otras pruebas electrónicas: la regulación jurídica-administrativa de la acreditación de las transacciones electrónicas. Thomson-Reuters Aranzadi, 2018		

	- Beltrán, M. y Tejerina, O. (coords.): Aspectos jurídicos de la ciberseguridad. RA-MA, 2020 - Canals Ametller, D. (Dir.): Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales. Wolters Kluwer, 2021 - Fernández García, E.: "Derecho de la ciberseguridad de las infraestructuras críticas más allá de la perspectiva penalista", Revista Jurídica de Castilla y León, núm. 56 2022 - Fondevila Antolín, J.: "Seguridad en la utilización de medios electrónicos: el Esquema Nacional de Seguridad", en E. Gamero (dir.): Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del sector público. Tirant lo Blanch, 2017 - Galán, C.: "El derecho a la ciberseguridad", en T. de la Quadra y J.L. Piñar (dirs.): Sociedad Digital y Derecho. Boletín Oficial del Estado, 2018 - Fuertes López, M.: Metamorfosis del Estado. Maremoto digital y ciberseguridad. Marcial Pons, 2022 - Llaneza González, P.: Identidad digital, Wolters-Kluwer Bosch, 2021 - Mallada Fernández, C. (coord.): Nuevos retos de la ciberseguridad en un contexto cambiante. Thomson-Reuters Aranzadi, 2019
Assessment	Examinations 45% Class Participation and Attendance 10% Assignments 45% 100%
Language	English

Course Title	Software Security and Secure Software Lifecycle				
Course Code	EMC322				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	José A. Ruipérez Valiente				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of this course is to provide a broad overview of the secure software design process and the secure software lifecycle (SDL), reviewing methods and frameworks to accomplish these goals. Moreover, it will also review some of the main families of vulnerabilities, in order to provide prevention and detection guidelines. It will provide examples specifically applied to verticals.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify in a holistic way the different problems within a specific area of cybersecurity • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that take into account multidisciplinary factors. • Identify management models of cybersecurity and associated processes to carry out the cybersecurity tracking and management within an organization • Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of software security. • Analyse the scenarios where it is needed to provide software and protection mechanisms of the organizations' data considering the existing norms. • Propose the use of cryptographic primitives, secure protocols, and methodologies for the development of secure software based on the current scenario considering both technical and business aspects. • Evaluate the data and software security based on employed cryptographic primitives, secure protocols and the vulnerability analysis carried out.				
Prerequisites	None	Co-requisites	None		
Course Content	• Unit 1: Secure software design o Security risk management o Security testing				

	o Security coding techniques (code hardening) o Security requirements, validation and verification • Unit 2: Secure software lifecycle (SDL) o SDL frameworks (Microsoft, etc), adaptations (agile, mobile, etc) and assessment (SAMM, BSIMM, certifications , etc) • Unit 3: Prevention and detection of vulnerabilities o Prevention, detection and mitigation o Client and server side vulnerabilities • Unit 4: Secure software applied to vertical
Teaching Methodology	Face-to-Face
Bibliography	• [CS:P&P]: Computer Security: Principles and Practice. William Stallings and Lawrie Brown (4th edition). 2017. • [CCS]: Corporate Computer Security. Randall J. Boyle and Raymond R. Panko (5th edition). 2021. • [SiC]: Security in Computing. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies (5th edition). 2015. • [SR&ASD]: Secure, Resilient, and Agile Software Development. Mark S. Merkow. 2020 • [SDL]: The Security Development Lifecycle. Michael Howard and Steve Lipner. 2006. • [SSDF]: Secure Software Development Framework (SSDF). NIST Special Publication 800-218. Murugiah Souppaya, Karen Scarfone, and Donna Dodson, pp. 10-28, 2022. • [ETSI] Cyber security for consumer internet of things: Baseline requirements, ETSI EN 303 645, pp. 13-25, 2020. • [MSA] Microservices Security in Action: Design secure network and API endpoint security for Microservices applications, with examples using Java, Kubernetes, and Istio. W. N. Dias and P. Siriwardena, 2020 • [CC] Common Criteria for Information Technology Security Evaluation, Common Criteria, 2022. • [SOTA] State of the Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2, ECSO, 2017. **Unit 1** o [CS:P&P]: Chapter 10 Buffer Overflow. Chapter 11 Software Security. Chapter 14 IT Security Management and Risk Assessment. o [CCS]: Chapter 2 Planning and Policy. Chapter 8. Application security o [SiC]: Chapter 3 Programs and Programming, Chapter 4 The Web—User Side, Chapter 10 Management and Incidents

	o [SR&ASD] Chapter 8: Testing Part 1: Static Code Analysis, Chapter 9: Testing Part 2: Penetration Testing/Dynamic Analysis/IAST/RASP **Unit 2** o [SR&ASD] Chapter 5: Secure Design Considerations, Chapter 6: Security in the Design Sprint, Chapter 7: Defensive Programming, Chapter 10: Securing DevOps o [CS:P&P]: Chapter 13 Cloud and IoT Security. 12.8 Virtualization security o [CCS]: Chapter 4. Secure networks o [SiC]: Chapter 6 Networks, Chapter 8 Cloud Computing o [ETSI]: Full reference **Unit 3** o [SDL]: Part II: “The Security Development Lifecycle Process” o [SSDF]: Full reference. o [CS:P&P]: Chapter 15 IT Security Controls, Plans, and Procedures o [SR&ASD]: Chapter 11: Metrics and Models for AppSec Maturity o [MSA]: Chapter 1: Microservices security landscape **Unit 4** o [CC]: Part I: “Part 1: Introduction and general model” o [SOTA]: Full reference.	
Assessment	Examinations Assignments Class Participation and Attendance 	45% 45% 10% 100%
Language	English	

Course Title	Authentication and Authorization Infrastructures				
Course Code	EMC323				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	Gabriel López Millán				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of this course is to introduce students to the concepts of authentication and authorization: models, trends, etc., and the main frameworks and standards about the management of Authentication and Authorization security architectures: SAML, Kerberos, etc.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Holistically identify the different problems related to a specific area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new environment in the field of cybersecurity. ● Design a presentation that includes the main ideas to be communicated, and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Present their knowledge in a clear, concise, unambiguous way and adapt to the time established for the presentation. ● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks.				

	● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Plan autonomous work tasks and self-learning processes running at the scheduled times. ● Learn about new trends, good practices, standards and regulations related to the field of cybersecurity.		
Prerequisites	None	Co-requisites	None
Course Content	● Topic 1. Authentication, Authorization and Accounting o Definition, models, etc. ● Topic 2. User authentication (passwords, biometrics, authentication tokens, behaviour, 2FA, etc.). o Management models, authentication and authorization processes. o Current trends in authentication processes. o Legislation and regulation. ● Topic 3. Authentication in distributed systems. o Description of the main distributed systems, such as Kerberos, SAML, OpenID Connect, etc. o Characteristics, functionality and evaluation of architectures for authentication ● Topic 4. Access control and authorization systems. o Description of the main access control and authentication systems, such as OAuth or XACML. o Characteristics, functionality and evaluation of architectures for access control and authorization. Topic. ● Topic 5. Accounting Management (privacy, logs, etc.) for the monitoring of systems and infrastructures.		
Teaching Methodology	Face-to-Face		

Bibliography	1. Stallings, William, et al., Computer Security - Principles and Practice (2018) . Chapters 3 and 4 (topics 1 and 2) 2. Stallings, William, Cryptography and Network Security - Principles and Practice, Global Edition (2017). Chapters 16 and 18 (topic 3). 3. Solving Identity Management in Modern Applications. Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. Yvonne Wilson and Abhishek Hingnikar. Apress. Chapters 7 and 10 (Topics 3 and 4).
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Malware and Attack Technologies				
Course Code	EMC324				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Juan Antonio Martínez Navarro, Félix Gómez Marmol				
ECTS	6	Lectures / week	1.5 Hours / 14 weeks	Laboratories / week	1.5 Hours / 14 weeks e
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main malware and attacks technologies.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Taxonomy of malware. Dimensions and characteristics. ● Malicious activities of malware ● Malware analysis. Analysis techniques, analysis environments. Analysis evasion techniques. ● Malware detection. Identify presence, attack detection. ● Response to malware. Stopping operations. Identification.				
Prerequisites	None	Co-requisites	None		

Course Content	● Unit 1: Malware Classification ● Unit 2: Malware Forensics ● Unit 3: Sandboxes and Multi-AV Scanners, automation and dynamic analysis
Teaching Methodology	Face-to-Face
Bibliography	● Michael Ligh, Steven Adair, Blake Harstein, Matthew Richard. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley. 2010 ○ Chapter 3 (Unit 1) ○ Chapters 4, 7, 8, 9 (Unit 3) ● Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. 2012. ○ Chapters 11, 12, 13 (Unit 1) ○ Chapter 2 (Unit 2) ○ Chapter 3 (Unit 3) ● ● Abhijit Mohanta, Anoop Sldanha. Malware Analysis and Detection Engineering. A Comprehensive Approach to Detect and Analyze Modern Malware. 2020 ○ Chapter 19 (Unit 1) ○ Chapter 24 (Unit 3) ● Dylan Barker. Malware Analysis Techniques. Tricks for the triage of adversarial software. 2021. ○ Chapter 2 (Unit 2) ○ Chapter 3, 5, 6 (Unit 3)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	CyberSecurity Lab				
Course Code	EMC325				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Different teachers based on the projects labs				
ECTS	6	Lectures / week	1 Hours / 4 weeks	Laboratories / week	2 Hours / 14 weeks
Course Purpose and Objectives	This subject will have a structure in which the students per group must solve problems in a group, forming a response team and where they have to collaborate techniques and tools learned in the previous subjects, so that they can put the integration into operation in a practical way. of different tools. The formation of teams will be done so that students with different profiles can interact so that the teams can cover different aspects of solving cybersecurity problems. It will focus on carrying out simulated attack and reaction exercises where different teams can play different roles.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios.				

	• Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. • Collect and analyze research data to address new problems in the field of cybersecurity. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. • Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. • Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. • Analyze methods and techniques of cyber attacks and cyber defense. • List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to apply. • Carry out vulnerability and risk analysis processes. • Discuss the functionality of the elements incorporated in the architectures and security services of systems, critical infrastructures and communication networks. • Deploy monitoring elements in architectures and security services, critical infrastructures and communication networks. • Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communication networks..		
Prerequisites	First semesters courses	Co-requisites	None
Course Content	The master courses responsible will provide each year a collection of projects to be solved based on the interaction of different challenges covering different components and technologies already presented to the students. Students will organize in groups that will covered different aspects of a cybersecurity system that will solve the challenge		
Teaching Methodology	Face-to-Face		
Bibliography	• References from the different courses related to the technologies and techniques to be used		
Assessment	Assignments Class Participation and Attendance	80% 20% 100%	
Language	English		

Course Title	5G, IoT and Cyber-Physical Systems Security				
Course Code	EMC326				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Ramón J. Sánchez Iborra, Miguel Ángel Zamora, Benito Úbeda Miñarro				
ECTS	6	Lectures / week	1.6 Hours / 14 weeks	Laboratories / week	1.6 Hours / 14 weeks e
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main security aspects to be considered in novel and evolving scenarios such as Internet of Things (IoT) deployments, Cyber-Physical Systems (CPS), Industrial Control Systems (ICS), and 5G architectures.				

Learning Outcomes	Upon successful completion of this course students should be able to: ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little-known environment in the field of cybersecurity. ● Collect and analyse research data to address new problems in the field of cybersecurity. ● Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. ● Design solutions to cybersecurity problems using creative thinking. ● Design, deploy and maintain cybersecurity systems. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Describe the main elements and functions that are part of intelligent services, products and infrastructures in cybersecurity fields. ● Analyse scenarios in the field of cybersecurity from the point of view of the organization's security governance, the management of cybersecurity and the security of products, services and facilities. ● Design security management processes for products, services and facilities from the perspective of their security and considering business aspects (regulation, regulations, economic, etc.). ● Critically evaluate the processes of security governance, security management, design of products, processes, services and intelligent infrastructures in cybersecurity fields, taking into account into account requirements, existing solutions, regulations, standards and good practices. ● Deploy monitoring elements in security architectures and services, critical infrastructures, and communications networks. ● Analyse the security information collected through monitoring processes of system security architectures, critical infrastructures, and communications networks. ● Design security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering technical, business (economic, legal, environmental, etc.) and innovation aspects. ● Assess security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering aspects technical, business (economic, legal, environmental, etc.) and innovation		
Prerequisites	None	Co-requisites	None
Course Content	● Unit 1: IoT security architecture and requirements. ● Unit 2: IoT Protocols and their security. ● Unit 3: Identity, privacy and Access Management in IoT. ● Unit 4: Security in Industrial IoT/CPS. ● Unit 5. Security in Cellular Architectures.		

Teaching Methodology	Face-to-Face
Bibliography	● IoT in 5 Days. ● A. D’Hondt, H. Bahmad, and J. Vanhee, “Mobile and Embedded Computing LINGI2146 Report ‘RPL Attacks Framework’”, 2016. ● Comparison of CoAP Security Protocols John Preuß Mattsson, Francesca Palombini , Mališa Vučinić. (full document) ● Terminology and processes for initial security setup of IoT devices ● THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World Internet Society 2015. (full document) ● Object Security for Constrained RESTful Environments (OSCORE) G. Selander, J. Mattsson, F. Palombini and L. Seitz July 2019. (Section 1 to 4, and Appendix A) ● Ephemeral Diffie-Hellman Over COSE (EDHOC) G. Selander, J. Preuß Mattsson and F. Palombini IETF Internet Draft. (Section 1 to 4) ● Sravani Bhattacharjee, Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries (English Edition), Chapters 1 and 4. 2018. ● Shancang Li, Li Da Xu, Securing the internet of things. Elsevier Syngress. Chapters 1 and 2. 2017. ● Larry Peterson and Oguz Sunay, 5G Mobile Networks: A Systems Approach. Open Networking Foundation (free book). Full book. 2020.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Advanced Techniques in Cyber Intelligence
Course Code	EMC327
Course Type	Elective

Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Jorge Bernal and Antonio Skarmeta				
ECTS	6	Lectures / week	1,6 Hours / 14 weeks	Laboratories / week	1,6 Hours / 14 weeks
Course Purpose and Objectives	**Objective:** This course aims to teach students the current techniques, methods and tools for a holistic data processing, analysis and management of cyber intelligence information and systems. Students will be exposed to practical cyber intelligence techniques and tools. **Description:** The course will deal with architectures, formats and techniques for cyber threat intelligence (CTI) information management, data gathering and exchange, including confidential and privacy-preserving CTI sharing. In addition, the course will provide the foundations and mechanisms for data analysis of CTI information coming from different sources (e.g., osints, social networks) using techniques based on Artificial intelligence. The analysis will be put in practice for diverse purposes such as anomaly detection in complex distributed/federated scenarios.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Design cybersecurity scenarios, solutions, or systems including original or innovative aspects. ● Holistically identify the different problems related to a specific area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity. ● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. ● Collect and analyze research data to address new problems in the field of cybersecurity. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience.				

	● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario ● Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity. ● Design solutions to cybersecurity problems using creative thinking. ● Analyze methods and techniques of cyber attacks and cyber defense. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Deploy monitoring elements in security architectures and services, critical infrastructures and communications networks. ● Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communications networks.		
Prerequisites	None	Co-requisites	None
Course Content	● Cyber intelligence information management ○ Architectures, phases and processes associated with cyber intelligence. ○ Automatic techniques for capturing, exchanging and managing cyber intelligence information. ○ Formats and representation of cyber intelligence information ○ Privacy and confidentiality in the exchange of cyber intelligence information. ● Advanced processing of cyber-intelligence information ○ Detection of cyber attacks and threats based on Artificial Intelligence. ○ Scalable and federated AI-based cyber intelligence systems. ○ Advanced computational techniques for anomaly detection. ○ Analysis of data from social networks and other sources for Cyber-intelligence ○ Design and management of cyber intelligence systems: practical cases		
Teaching Methodology	Face-to-Face		

Bibliography	• Michel Bazzel, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. ISBN-13 : 979-8761090064. Section II (topic cyber intelligence information management) • Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense. ISBN-13 : 978-1800209404 Chapter 12,13,14 (topic cyber-intelligence) • Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers. ISBN-13 : 978-1484272190. Chapters 2,3, 7 (topic cyber intelligence) • Parisi, Alessandro. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019. ISBN-10: 1789804027, ISBN-13: 9781789804027. Chapter 4,5 (topic Advance processing of cyber-intelligence) • Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. " OReilly Media, Inc.", 2018. ISBN-10: # 1491979909, ISBN-13: 978-1491979907 Chapter 3,4,6 (topic Advance processing of cyber-intelligence)
Assessment	Examinations 60% Class Participation and Attendance 10% Assignments 30% 100%
Language	English

Course Title	Human factors in security, privacy and rights on the Internet				
Course Code	EMC328				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Antonio Ruiz Martínez,				
ECTS	3	Lectures / week	1.5 Hours / 7 weeks	Laboratories / week	1.5 Hours / 7 weeks
Course Purpose and Objectives	The course covers the influence of human factors in cybersecurity and privacy and rights issues on the Internet. We will present main techniques and technologies to protect users' privacy and we will see tendencies in human factors, privacy and rights on the Internet.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Holistically identify the various problems related to a particular area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or unfamiliar environments related to cybersecurity. ● Identify the different multidisciplinary aspects (legal, social, ethical) to be taken into account when dealing with a problem related to a cybersecurity scenario. ● Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow taking into account multidisciplinary aspects. ● Plan autonomous work tasks and self-learning processes executing them in the foreseen times. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and to the target audience. ● Present their knowledge in a clear, concise and unambiguous way, adapting to the time established for the presentation. ● Prepare clear, concise and reasoned documentation on aspects related to the field of cybersecurity. ● Describe cryptographic primitives, secure protocols and software mechanisms that allow data protection.				

<table>
<tr><td></td><td colspan="3">● Employ the use of cryptographic primitives, secure protocols and software models to protect data in cybersecurity scenarios.
● Analyze scenarios where it is necessary to provide software and mechanisms to protect the organization's data in compliance with existing regulations.
● Identify new and emerging technologies, best practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">• Topic 1. Human Aspects of Cybersecurity
• Topic 2. Privacy and rights on the Internet
• Topic 3. Privacy techniques and technologies
o Primitives and protocols
o Technologies
• Topic 4. Trends in Human Factors in Security, Privacy and Rights on the Internet</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face-to-Face, Flipped classroom, use case, laboratories</td></tr>
<tr><td>Bibliography</td><td colspan="3">Information Privacy Engineering and Privacy by Design - Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.
o Topic 1. Chapters 2, 3, and 12.
o Topic 2. Chapter 14.
o Topic 3. Chapters 7, 8 and 9.
o Topic 4. Chapter 9

Privacy and Data Protection Challenges in the Distributed Era.
Topic 1. Chapter 2.
Topic 4. Chapter 3, 5, and 10.</td></tr>
<tr><td>Assessment</td><td colspan="3">Examinations 45%
Assignments 45%
Class Participation and Attendance 10%
100%</td></tr>
<tr><td>Language</td><td colspan="3">English</td></tr>
</table>

Course Title	Advanced Aspects of Cybersecurity Management				
Course Code	EMC329				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	Antonio Skarmeta and Jorge Bernal				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of the course is to prepare students to understand Cybersecurity governance as the process of establishing the architecture that ensures a company's security programs align with business objectives, comply with regulations and standards (such as PCI security standards), and achieve objectives for managing security and risk. As a supplement to the course on Techniques for the Management of Cybersecurity, in this one we focus more on the application of methodology and the use case analysis in order to define cybersecurity governance approaches and solutions to different incidents and situations.				

Learning Outcomes	Upon successful completion of this course students should be able to: ● Collect and analyze research data to address new problems in the field of cybersecurity. ● Design, deploy and maintain cybersecurity systems. ● Identify the applicable regulations and legislation in the field of cybersecurity. ● Evaluate and define the different measures to be applied (contingency plans, etc.) based on vulnerabilities, threats and risks, considering both technical and business (economic and political) aspects. ● Analyze forensic reports, and define action plans and their application. ● Define the scope and impact caused by a specific cyber incident.		
Prerequisites	EMC314	Co-requisites	None
Course Content	ICT and cybersecurity elements and assets ● Types of assets ● Valuation Dimensions ● Assessment criteria ● Threats and Safeguards Cybersecurity operations intelligence ● ID ● Protection ● Detection ● Response ● Recovery Design and Planning of a Cybersecurity Systems ● Cybersecurity Planning ● Business continuity, disaster recovery and incident management ● Security program management ● Definition of an information protection model in an ISMS (Information Security Management System) ● Legal aspects and regulations applicable to the exchange of data and their impact on the design of the systems ● Advanced intelligence on cyber threats Best practices in design and deployment ● Cyber Threat Hunting ● CTI with privacy preservation ● Cyber exercises and simulation platforms		

Teaching Methodology	Face-to-Face
Bibliography	1. Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology. Chapter 1-3, and annex 2. CISSP Certified Information Systems Security Professional (ISC)2 2021. Chapter 1,3,5,8 3. NIST Cybersecurity Framework V1.1 Chapter 1-3 4. Practical Use Cases https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis-1/file.html
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	CyberSecurity Lab II				
Course Code	EMC331				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher's Name	Norbert Tihanyi				
ECTS	6	Lectures / week	-	Laboratories / week	6 Hours / 14 weeks
Course Purpose and Objectives	The subject covers the fundamentals of random number generators and their related applications, principles of penetration testing and malware analysis. Well-known attacks against PKI infrastructures will be demonstrated during the course. The subject covers the basic principles of modern Kleptography.				
Learning Outcomes	Upon successful completion of this course students should be able to: • have comprehensive and up-to-date knowledge and understanding of the general theories and the related concepts of Random Number Generation and analysis. • become familiar with the basic principles of modern malware analysis methods.				

	• have extensive knowledge on how to analyze source codes to find hidden vulnerabilities • Have extensive knowledge on finding backdoors in PKI infrastructure and certificates.		
Prerequisites	None	Co-requisites	None
Course Content	• PKI systems / RSA / Diffie-Hellman key exchange protocols • Pollard P-1, Pollard rho factorization methods • Recovering private keys from public keys using factorization methods (case-studies) • Hash functions and their applications • Random Number Generators and their applications (LCG, LSFR, Mersenne Twister) • NIST Special Publication 800-22		
Teaching Methodology	Face-to-Face		
Bibliography	• Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C • Jean-Philippe Aumasson : Serious Cryptography: A Practical Introduction to Modern Encryption • Christof Paar and Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners • National Institute of Standards and Technology, “A statistical test suite for random and pseudorandom number generators for cryptographic applications, Special Publication 800-22. • David Jonhston: Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers		
Assessment	Examinations Assignments Class Participation and Attendance	0% 90% 10% 100%	
Language	English		

Course Title	Advanced cryptography				
Course Code	EMC332				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher's Name	Péter Ligeti				
ECTS	6	Lectures / week	2 Hours / 14 weeks	Laboratories / week	4 Hours / 14 weeks
Course Purpose and Objectives	The course covers various topics beyond traditional cryptography and the necessary theoretical background. The following concepts are introduced: perfect and computational security, hardness assumptions, provable security.				
Learning Outcomes	Upon successful completion of this course students should be able to: • have comprehensive and up-to-date knowledge and understanding of the general theories, contexts, facts, and the related concepts of IT, particularly – depending on their chosen specialization – in the areas of program design, synthesis and verification, logical programming, programming languages, computing models, computer architectures, operating systems, computer networks, distributed systems, database				

	management systems, information theory, code theory, and cryptography. - have comprehensive and up-to-date knowledge of the principles, methods, and procedures for designing, developing, operating, and controlling IT processes, particularly – depending on their chosen specialization – in the areas of program design methods; design, construction and management of complex software systems and databases in modern database management systems; service-oriented program design; the design, construction and management of information systems; the design and development of tools and services for the internet; the design, development and management of database systems; the design, construction and management of distributed systems, cryptography, data security and data protection.		
Prerequisites	None	Co-requisites	None
Course Content	- secure multiparty computation - oblivious transfer - elliptic curve cryptography - Yao's garbled circuit - secret sharing - generalized signature schemes		
Teaching Methodology	Face-to-Face		
Bibliography	- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. Chapman & Hall/Crc Cryptography and Network Security Series, 2007. ISBN: 1584885513 - Bruce Schneier: Applied Cryptography – Protocols, Algorithms, and Source Code in C, ISBN 978-1-119-09672-6		
Assessment	Examinations 40% Assignments 50% Class Participation and Attendance 10% 100%		
Language	English		

Course Title	Data Science Lab II				
Course Code	EMC333				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher’s Name	Tomáš Horváth				
ECTS	6	Lectures / week	2 Hours / 14 weeks	Laboratories / week	4 Hours / 14 weeks
Course Purpose and Objectives	During the lab, students will work in teams on data science tasks on real data gathered from industrial as well as academic partners of the Faculty of Informatics. The tasks will concern both basic and applied research, under the supervision of experienced data scientists, necessary for delivering the results in a desired quality. The projects will follow suitable industrial data science methodologies such that, for example, the CRISP-DM process. Emphasis will be given on delivering prototype solutions to the determined tasks concerning, but not limited to, data pre-processing, data transformation, data visualization, modeling (model selection, hyper-parameter tuning, model combination, etc.), model evaluation as well as deployment, real-time data analytics for descriptive and predictive mining, anomaly detection,				

<table>
<tr><td></td><td colspan="3">just to name a few. The concrete tasks will be determined by the industrial partners and they will play an important role also in the evaluation of the delivered solutions/prototypes. If applicable, teams will participate in data mining challenges (e.g. Kaggle).</td></tr>
<tr><td>Learning Outcomes</td><td colspan="3">Upon successful completion of this course students should be able to:
• Establish connections between different types of data, and are able to extract information and solve problems based on data transformation in a multidisciplinary environment.
• Their English language proficiency reaches the level essential for pursuing their studies and reading technical literature in English, for understanding and processing technical texts and performing professional tasks that this qualification entitles them to do, as well as for continuous professional development.
• Formalise complex classification, modelling and forecasting problems in various scientific disciplines, identify the necessary theoretical and practical methods and solve them.
• Construct transformation steps for raw data for a given task.
• Put data into context and correlate with other information, thereby combining different modalities.
• Participate – both orally and in writing – in professional discussions and debates, present and interpret their results, write reports, as well as understand and utilize scientific and technical literature both in their mother tongue and (at least) in English.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">• Delivering prototype solutions to the determined tasks
• Data pre-processing, data transformation
• Data visualization
• Data modeling (model selection, hyper-parameter tuning, model combination, etc.),
• Model evaluation
• Model deployment,
• Real-time data analytics for descriptive and predictive mining
• Anomaly detection</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face-to-Face and project-based</td></tr>
<tr><td>Bibliography</td><td colspan="3">• Ian H. Witten, Eibe Frank, Mark A. Hall (2011). Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.
• Pang-Ning Tan, Michael Steinbach, Vipin Kumar (2005). Introduction to Data Mining. Addison Wesley.</td></tr>
</table>

Assessment	Examinations Assignments Class Participation and Attendance	0% 90% 10% 100%
Language	English	

Course Title	Introduction to Data Security Lab				
Course Code	EMC334				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher's Name	Imre Lendák				
ECTS	4	Lectures / week	2 Hours / 14 weeks	Laboratories / week	2 Hours / 14 weeks
Course Purpose and Objectives	The students will be equipped with relevant data security knowledge to undertake applied data science projects in which they develop and deploy explainable and trustworthy machine learning solutions while taking into account any sensitive data involved in any project stages.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Posses relevant knowledge about the latest developments and challenges in the field of data security. • Posses an up-to-date knowledge of the relevant general theories in data security, as well as their connections with other professional and/or scientific domains. • Be a skilful user of the relevant scientific terminology in English.				

Prerequisites	None	Co-requisites	None
Course Content	• Cyberspace, cybersecurity, cybercrime; • Data inventory and backup; • Identity and access management; • Data encryption; • Data loss prevention; • Data privacy vs machine learning; • Data security standards; • Cyber insurance		
Teaching Methodology	Face-to-Face		
Bibliography	• Janine Kremling, Amanda M. Sharp Parker (2017). Cyberspace, Cybersecurity, and Cybercrime. SAGE Publications. • Roger A. Grimes (2019). A Data-Driven Computer Defense: A Way to Improve Any Computer Defense. • Clarence, David Freeman (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media; 1st edition. • W. Curtis Preston (2021). Modern Data Protection: Ensuring Recoverability of All Modern Workloads. O'Reilly Media; 1st edition. • Jay Jacobs, Bob Rudis (2014). Data-driven Security. Wiley.		
Assessment	Examinations Assignments Class Participation and Attendance	40% 60% 10% 100%	
Language	English		

Course Title	Introduction to Data Science				
Course Code	EMC335				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher’s Name	Tomáš Horváth				
ECTS	5	Lectures / week	2 Hours / 14 weeks	Laboratories / week	3 Hours / 14 weeks
Course Purpose and Objectives	The course navigates through the basic concepts and principles behind the main data science models and techniques. Descriptive techniques such as clustering and frequent pattern mining are explained in more details while, in case of predictive techniques, the focus is put mainly on the concepts of a model, its parameters and hyper-parameters as well as the quality and validation of models including overfitting-underfitting and the bias.-variance trade-offs. Data quality and pre-processing issues related to various data types and modeling problems are also tackled. Finally, basic recommendation techniques and the CRISP-DM methodology are contained in the course as well.				
Learning Outcomes	Upon successful completion of this course students should be able to: • They know the main application areas of data science, the challenges associated and the possible solutions, as well as the limitations of the application of the related techniques.				

<table>
<tr><td></td><td colspan="3">• They can establish connections between different types of data, and are able to extract information and solve problems based on data transformation in a multidisciplinary environment.
• They are able to construct transformation steps for raw data for a given task.
• They know the dependencies between data elements as well as the structurability and types of data. When technology changes, they are able to detach data analysis strategies from technology.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">• Clustering: k-means, agglomerative, DBSCAN, cluster validation;
• Frequent Pattern Mining: itemsets, association rules, quality measures;
• Linear Classification and Regression: model, parameters and hyper-parameters, validation, overfitting-underfitting and the bias-variance trade-off;
• Introduction to traditional prediction techniques (as black-box functions);
• data quality and pre-processing: noise, missing values, data transformation, normalization;
• the CRISP-DM process;
• recommendation techniques;</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face-to-Face and project-based</td></tr>
<tr><td>Bibliography</td><td colspan="3">• Peter Flach (2012). Machine Learning: The Art and Science of Algorithms that Make Sense of Data. Cambridge University Press.
• Jiawei Han, Micheline Kamber, Jian Pei (2011). Data Mining: Concepts and Techniques. Morgan Kaufmann.
• Pang-Ning Tan, Michael Steinbach, Vipin Kumar (2005). Introduction to Data Mining. Addison Wesley.</td></tr>
<tr><td>Assessment</td><td colspan="3"><table><tr><td>Examinations</td><td>50%</td></tr><tr><td>Assignments</td><td>50%</td></tr><tr><td>Class Participation and Attendance</td><td>0%</td></tr><tr><td></td><td>100%</td></tr></table></td></tr>
<tr><td>Language</td><td colspan="3">English</td></tr>
</table>

Course Title	Open-Source Technologies for Data Science				
Course Code	EMC336				
Course Type	Optional				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher’s Name	Imre Lendák				
ECTS	6	Lectures / week	3 Hours / 14 weeks	Laboratories / week	3 Hours / 14 weeks
Course Purpose and Objectives	This course equips students with knowledge about the most well-known or otherwise relevant open-source tools and technologies designed for data ingestion, storage, analytics and visualization. This will allow the students to make well-founded, correct design decisions when building data intensive systems after transitioning to the job market.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Discuss the latest developments in the field of open-source technologies for data analytics with a specific focus on solutions which can be utilized in real-time data analytics use cases. • Describe (1) the relevant terminology used in the field of open-source technologies, (2) and (2) its relations with neighboring professional and/or research domains. • Skillfully use relevant scientific terminology in English. • formalize and describe complex problems in the field of data mining.				

	• design, develop and maintain data mining software solutions and environments based on open-source technogologies. • assess the business and innovative value of open-source data storage, analytics and visualization solutions, as well as to validate and convey the results of those to customers in different industry domains.		
Prerequisites	None	Co-requisites	None
Course Content	• Data ingestion and storage: Cassandra, InfluxDB és HBase; • Big data analytics: Spark és ElasticSearch; • Stream analytics: Kafka és Flink; • Graph analytics: GraphX; • Data visualization and reporting technologies: Tableau, Kibana, seaborn;		
Teaching Methodology	Face-to-Face		
Bibliography	• Neha Narkhede, Gwen Shapira, Todd Palino (2017). Kafka: The Definitive Guide: Real-Time Data and Stream Processing at Scale. O'Reilly Media, 1st Edition. • Tom White (2015). Hadoop: The Definitive Guide: Storage and Analysis at Internet Scale. O'Reilly Media, 4th Edition. • Jeff Carpenter, Eben Hewitt (2020). Cassandra: The Definitive Guide: Distributed Data at Web Scale. O'Reilly Media, 3rd Edition. • Bill Chambers, Matei Zaharia (2018). Spark: The Definitive Guide: Big Data Processing Made Simple. O'Reilly Media, 1st Edition. • Tyler Akidau, Slava Chernyak, Reuven Lax (2018). Streaming Systems: The What, Where, When, and How of Large-Scale Data Processing. O'Reilly Media, 1st Edition.		
Assessment	Examinations Assignments Class Participation and Attendance	40% 50% 10% 100%	
Language	English		

Course Title	Stream Mining L+Pr.				
Course Code	EMC337				
Course Type	Optional				
Level	Master (2nd Cycle)				
Year / Semester	Year 2 of 2 / Semester 3 of 4				
Teacher's Name	Péter Kiss				
ECTS	6	Lectures / week	3 Hours / 14 weeks	Laboratories / week	3 Hours / 14 weeks
Course Purpose and Objectives	The course is devoted to processing and mining data streams in which data, arriving at high speed, are processed under various space and time constraints. Typically, data is processed with one pass by the algorithm taking into account that data may evolve over time. The course will cover topics of data stream clustering and classification. Frequent pattern mining from data streams, change detection and forecasting in data streams, and indexing and distributed mining of data streams.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Posses complex and up-to-date knowledge of stream mining techniques necessary to conduct research in this field. • Discuss (1) the relevant stream mining terminology, (2) the general theory of stream mining, as well as (3) its relations with neighbouring research domains. • Skilfully use of the relevant scientific terminology in English.				

	• Formalize and describe complex problems in the field of stream mining. • Design, develop and maintain stream mining software solutions and environments. • Assess the business and innovative value of stream mining solutions, as well as to validate and convey the results of stream mining solutions to customers in different industry domains.		
Prerequisites	None	Co-requisites	None
Course Content	• Sketches and standing queries • Clustering data streams; • Data stream classification; • Frequent pattern mining in data streams; • Change detection in stream mining; • Streaming systems: windows, watermarks, triggers and correctness;		
Teaching Methodology	Face-to-Face		
Bibliography	• Albert Bifet, Ricard Gavalda, Geoff Holmes, Bernhard Pfahringer (2018). Machine Learning for Data Streams: with Practical Examples in MOA. The MIT Press. • A. G. Psaltis. Streaming Data: Understanding the real-time pipeline. Manning Publications, 2016. • Gerardus Blokdyk (2018). Data stream mining. CreateSpace Independent Publishing Platform. • Joao Gama (2010). Knowledge Discovery from Data Streams. Chapman & Hall. • Tyler Akidau, Slava Chernyak, Reuven Lax (2018). Streaming Systems: The What, Where, When, and How of Large-Scale Data Processing. O'Reilly Media, 1st Edition.		
Assessment	Examinations Assignments Class Participation and Attendance	50% 30% 10% 100%	
Language	English		

Course Title	Master Thesis				
Course Code	EMC341				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 4th Semester				
Teacher’s Name	TBA				
ECTS	30	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	The course’s purpose is to provide guidance on how to write a successful Master’s Thesis. It aims to provide skills in research methods in the general field of Computer Science. It also aims to equip the student with the tools required to manage a project as large as a Master’s thesis, through providing project management techniques. Finally, it aims to prepare the student for independent work as a recipient of a Master’s degree.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Demonstrate written and oral technical research skills. • Select and justify a research topic, and use various resources to carry out a literature search. • Design, execute, interpret and report results from empirical research projects. • Manage a project and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources.				

	• Identify real-world problems to which academic concepts and methods can be realistically applied to improve or resolve the problem situation. • Select and use effectively the methods and techniques appropriate for particular cases, and plan and manage their work. • Evaluate a proposed solution and prove its worth to the client. • Critically evaluate the project and the proposed solution, as well as recognize and describe legal, social or ethical obligations stemming from the project.		
Prerequisites	Successful completion of all core courses	Co-requisites	None
Course Content	The student selects a topic from the Thesis Topics Catalogue or following consultations with the future mentor. Topics are assigned on a First-Come, First-Served basis, given that the students have passed all the pre-requisite courses for a specific topic. The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors.		
Teaching Methodology	Face-to-face or electronic meetings with the academic supervisor and optionally with the industrial supervisor for industrial Master theses. The supervisors provide feedback and thereby ensure high thesis quality.		
Bibliography	Any material suitable for the subfield in which the student is undertaking the thesis will be specified by the instructor. Conference and journal papers published in the recent past are preferred.		
Assessment	**ASSESSMENT:** The Master thesis defense consists of two elements of equal importance: (1) a short oral presentation of the thesis and (2) an oral examination in at least two topics covered by the courses which the student attended during his/her studies. Written Thesis: 50% Final exam (2 topics): 50% The final grade is calculated as an average of the thesis and oral examination in two chosen topics.		
Language	English		

TRACK 4

Course Title	Cyberattack Techniques and Ethical Hacking				
Course Code	EMC411				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	Antonio Ruiz Martínez, Félix Gómez Mármol				
ECTS	6 ECTS	Lectures / week	1.6 Hours / 14 weeks	Laboratories / week	1.6 Hours / 14 weeks
Course Purpose and Objectives	The goal of the course is to introduce students in attacking computer systems through an ethical hacking process. Students will know the different kind of security assessments that could be made and they will learn the different steps of a ethical hacking process through some laboratories where they will attack an scenario.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. • Collaborate when solving a problem in the field of cybersecurity, teamwork, and leadership. • Analyze methods and techniques of cyber-attacks and cyber-defense. • Design, deploy, and maintain cybersecurity systems.				

	• Identify applicable regulations and legislation in the field of cybersecurity. • Elaborate clear, concise, and reasoned documentation on aspects related to the field of cybersecurity. • List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to be applied. • Perform vulnerability and risk analysis processes. • Classify vulnerabilities, threats and risks within the organization to determine their importance, taking into account the context.		
Prerequisites	None	Co-requisites	None
Course Content	• Introduction to Ethical hacking o Basic concepts o Regulations and associated legislation • Security assessments. o Types of assessments o Methodologies o Training • Ethical hacking process. o Deployment of scenario and realization of ethical hacking process.		
Teaching Methodology	Flipped classroom, project-based learning		
Bibliography	• CEH™ v12 - Certified Ethical Hacker - Study Guide o Topic 1. Chapter 1. o Topic 2. Chapter 2. o Topic 3. Chapters 2, 4, 5, 6, 7, 9, 10, 11 and 12. • Desmond, Brian, et al. Active Directory: Designing, Deploying, and Running Active Directory. " O'Reilly Media, Inc.", 2008. o Topic 3. Chapters 2, 4 and 5.		
Assessment	Examinations Assignments Class Participation and Attendance 	30% 60% 10% 100%	
Language	English		

Course Title	CyberDefense Techniques				
Course Code	EMC412				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher's Name	José Ramón Hoyos-Barceló				
ECTS	6	Lectures / week	1,5 Hours /14 weeks	Laboratories / week	1,5 Hours /14 weeks
Course Purpose	This course integrates an introduction to different ways of protecting the underlying communication networks and the detection of and response to				

and Objectives	security incidents, with a focus on computer forensics and the collection, analysis and reporting of digital evidence in support of incident or criminal events.		
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios. • Analyse in detail cybersecurity scenarios, solutions or systems in order to detect possible areas for improvement. • Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or unfamiliar environments related to cybersecurity. • Identify the different multidisciplinary aspects (legal, social, ethical) to be taken into account when dealing with a problem related to a cybersecurity scenario. • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. • Formulate value judgements on the basis of collected information that, while incomplete or limited, include critical reasoning on the social and ethical responsibilities of the application of methods, cryptographic techniques, software tools or methodologies to address cybersecurity-related problems. • Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and to the target audience. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be conveyed with regard to a cybersecurity scenario. • Present your knowledge in a clear, concise and unambiguous manner, adapting to the time set for the presentation. • Analyse methods and techniques of cyber-attacks and cyber-defence. • Produce clear, concise and reasoned documentation on aspects related to the field of cybersecurity. • Identify the characteristics and functions of the elements that form part of the security architectures and services of systems, critical infrastructures and communications networks.		
Prerequisites	None	Co-requisites	None
Course Content	Defense tools and Incident Management Unit 1- Network defence and monitoring tools Unit 2- Incident management and disaster recovery, cyber incident reporting Computer Forensics		

	Unit 3- Introduction to Computer Forensics Unit 4- Situation assessment and collection of evidence Unit 5- Evidence Analysis Unit 6- Computer expertise
Teaching Methodology	Face-to-Face
Bibliography	1. Guide to Computer Network Security, 5th edition, by Joseph Migga Kizza. Springer (3: Security Threats, 5 Cyber Crimes and Hackers, 8 Disaster Management) 2. Stallings, William, et al., Computer Security - Principles and Practice (2018) (1.1 Computer security concepts; 1.2 Theats, attacks and assets; 8: Intrusion detection, 9: Firewall and Intrusion Prevention Systems, 14: IT Security Management and Risk Assessment, 15: IT Security Controls, Plans and Procedures, 17 Human resource security.) 3. Digital Forensics Explained. Greg Gogolin. CRC Press/Taylor & Francis Group. 2021 (1. What is digital forensics, 2.Digital forensic approaches, 3. Digital forensics tool kit, 7 Incident response, 10 Social engineering, 11 Anti-forensics) 4. Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730. (full article)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cybersecurity and Network Security
Course Code	EMC413
Course Type	Compulsory

Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher’s Name	Rafael Marín López, Óscar Cánovas				
ECTS	6 ECTS	Lectures / week	1.6 Hours / 14 weeks	Laboratories / week	1.6 hours/14 weeks
Course Purpose and Objectives	The goal of the course is to analyse, discuss different network security protocols at different layers ranging from link-layer to application layer. The course will also pay attention to non-cryptographic defence tools and standards related with network security.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity. ● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. ● Design solutions to cybersecurity problems using creative thinking. ● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. ● Analyze methods and techniques of cyber attacks and cyber defense. ● Prepare clear, concise and reasoned documentation on aspects related to the field of cybersecurity. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks.				

	● Describe the cryptographic primitives, the secure protocols and the software mechanisms that allow data protection. ● Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of secure software. ● Employ the use of cryptographic primitives, secure protocols and software models to protect data in a cybersecurity scenario. ● Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes. ● Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.		
Prerequisites	None	Co-requisites	None
Course Content	● Network protocols and vulnerabilities: adversary models, types of attack. ● Application-level security (public key and symmetric key management, application-level protection (SSH, S/MIME), application services security) ● Transport level security (TLS, DTLS, QUIC) ● Network level security (ACLs, IPv6 security, routing protocol security, VPNs) ● Link level security: wireless level security (IEEE 802.1X, EAP, RADIUS, DIAMETER, WPA) attacks on ethernet switches, MAC level attacks. ● Non-cryptographic defense tools (packet filtering, firewall, DMZ, IDS, IPS, etc.) ● Advanced security topics (SDN, NFV, IoT) ● Communication security standards (how security protocols are specified and documented)		
Teaching Methodology	Face-to-Face		
Bibliography	● W. Stalling CRYPTOGRAPHY AND NETWORK SECURITY, EIGHTH EDITION – 8th ○ Chapter 1. Computer and Network Security Concepts (Block I) ○ Chapter 18 Wireless Network Security (Block I) ○ Chapter 17 Transport-Layer Security (Block III) ○ Chapter 20 IP security (Block III) ○ Chapter 21 Network Endpoint Security (Block II)		

Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Techniques for the Management of the Cybersecurity				
Course Code	EMC414				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher’s Name	Manuel Gil Pérez				
ECTS	6	Lectures / week	3 Hours / 14 weeks	Laboratories / week	3 Hours / 14 weeks
Course Purpose and Objectives	The objective of this course is to cover aspects related to organisational security governance and the security project management, including the identification of security risks in the protected organisation together with potential countermeasures to apply for risk reduction.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Holistically identify the different problems related to a specific area of cybersecurity. • Identify the different multidisciplinary aspects (legal, social, ethical) to consider when dealing with a problem related to a cybersecurity scenario. • Plan autonomous work tasks and self-learning processes running at the scheduled times. • Enumerate and identify the different types of vulnerabilities, threats, and risks within the organisation, as well as possible solutions to be applied. • Describe the principles of risk management, how to apply them and possible tools to be used. • Describe the main elements and functions that are part of smart services, products, and infrastructures in the cybersecurity domain. • Explain the different aspects related to organisational security governance, security project management, design and implementation of products, services, and facilities in cybersecurity scenarios.				
Prerequisites	None	Co-requisites	None		
Course Content	Management of information security systems: • Unit 1. Information security legislation in Spain o National Security Scheme: objectives, requirements, and security measures				

	• Unit 2. Information Security Management Systems (ISMS) – *ISO 27000* • Unit 3. Implementation and evaluation of ISMS according to the stages of the Deming cycle: plan, do, check, act • Unit 4. Security and resilience plans – *ISO 22300 family* Analysis and management of security risks: • Unit 5. Analysis, assessment, and treatment of security risks o Security Master Plan • Unit 6. Methodologies for security risk analysis o NIST SP 800, MAGERIT / PILAR • Unit 7. Countermeasures for risk reduction Practices: • Case studies for applying security management tools • Implementation and audit of Information Security Management Systems (ISMS) o Audit automation and standardisation, following the ANA approach • Risk analysis and selection of countermeasures o Use of µPILAR for risk analysis and choice of safeguards, analysing the residual risk
Teaching Methodology	Face-to-Face
Bibliography	7. Gibson, Darril (2020). Managing Risk in Information Systems (Information Systems Security & Assurance). Jones and Bartlett Publishers, Inc. 8. Tiller, James S., O'Hanley, Richard (2013). Information Security Management Handbook, Volume 7 (6th Ed.). Auerbach Publications. 9. Spanish Ministry of Finance and Civil Service (2014). MAGERIT V.3: Methodology for Information Systems Risk Analysis and Management. Edita.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cryptography				
Course Code	EMC415				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	Leandro Marín Muñoz				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hour / 7 weeks
Course Purpose and Objectives	The objective of this course is to give a broad view of cryptography, studying both the mathematical and theoretical aspects as well as the aspects related to their implementation in special environments.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Solve problems related with theoretical and mathematical cyptology. • Evaluate the security of cryptographic methods. • Apply their knowledge about cryptology in research. • Understand the mathematical foundations of cybersecurity.				
Prerequisites	None	Co-requisites	None		
Course Content	Cryptographic security models. Secret sharing systems. Symmetric cryptography (block ciphers, stream ciphers, digital hash functions, message authentication codes, Merkle trees and block chains), public key cryptography (RSA-based, elliptic curve and lattice constructs, digital signatures), cryptographic protocols (authentication, key exchange, zero knowledge, secure multiparty computing), advanced aspects of cryptography (group/ring-based signatures, identity-based ciphers, homomorphic cryptography, side-channel attacks, implementations in environments with special requirements such us low power consumption, memory restrictions, etc.)"				
Teaching Methodology	Face-to-Face				

Bibliography	● Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. 2007. CRC Press. Chapter 3 (Private Key Cryptography) Chapter 5 (Block Ciphers) Chapter 10 (Public Key Encryption) Chapter 12 (Digital Signatures) ● Henri Cohen. A Course in Computational Number Theory. 1993. Springer. Chapter 1 (Basic Number Theory) Chapter 8, 10 (Factorization) Chapter 9 (Primality Testing) ● Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography. 2003. Springer. Chapter 2 (Elliptic Curves) Chapter 4 (Implementation Issues on ECC) ● FIPS 197. Advanded Encryption Standard (AES) – NIST. ● Craig Gentry. A Fully Homomorphic Encryption Scheme (Ph.D. Thesis). (only the introduction for homomorphic encryption)
Assessment	Examinations 60% Class Participation and Attendance 10% Assignments 30% 100%
Language	English

Course Title	Innovation and Entrepreneurship Seminar				
Course Code	EMC416				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S1				
Teacher’s Name	Responsible Antonio Skarmeta Different participants based on seminars				
ECTS	3	Lectures / week	3 Hours / 7 weeks	Laboratories / week	
Course Purpose and Objectives	The objective is to bring students closer to the most pressing problems and solutions at all times in industry, administration, defense and research. Through the different seminars proposed, students will have access to the experience of professionals of recognized prestige whose professional work is related to Cybersecurity in its legal, administrative, management and legal aspects. On the other hand, the more academic seminars will put students in contact with the state of the art in concepts, protocols, developments and tools on specific topics related to cybersecurity. Therefore, the seminars may be framed within any of the subjects of the master's degree				
Learning Outcomes	Upon successful completion of this course students should be able to: • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario.				

	• Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity. • Identify new and emerging technologies, good practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes. • Differentiate the most relevant aspects of new trends, good practices, standards, laws and human aspects with respect to those that already exist.		
Prerequisites	None	Co-requisites	None
Course Content	Within the master's degree, seminars will be given that may change from year to year, as advised by a field as variable as cybersecurity. Yearly the planning of seminar will be defined		
Teaching Methodology	Face-to-Face		
Bibliography			
Assessment	Assignments 60% Class Participation and Attendance 40% 100%		
Language	English		

Course Title	Cybersecurity Legal Framework				
Course Code	EMC421				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Julián Valero Torrijos				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	**Objective:** This course aims to provide students with an overview of the main legal aspects of cybersecurity, in particular from the perspective of European Union legislation. Specifically, it will provide the basic tools to identify the relevant rules, understand the basic legal concepts and then proceed to their application, considering the singularities of the digital environment. **Description:** Cybersecurity is nowadays a basic requirement for the development of digital services and contents, so that its legal framework has become an essential topic for IT sector professionals. This course will provide an overview of the legal framework of cybersecurity, taking into account its impact on fundamental rights and public freedoms, the intervention of public administrations in both the regulation of activities and their enforcement, as well as the implications from the perspective of criminal law.				

Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the regulations and legislation applicable in the field of cybersecurity. • Understand the main legal concepts in the field of cibersecurity. • Identify the main legal aspects to be taken into account when dealing with a problem related to a cybersecurity scenario. • Produce clear, concise and reasoned documentation including legal requirements of cybersecurity. • Define a risk management policy taking into account legal requirements. • Apply the legal concepts and rules associated with cybersecurity scenarios. • Design safety management processes for products, services and facilities from the perspective of their legal requirements. • Identify new and emerging technologies, best practices, regulatory, legislative and ethical aspects related to cybersecurity and mechanisms to detect these changes. • Adapt cybersecurity scenarios in line with new trends, best practices, standards, regulation and human aspects. • Assess the legal implications and risks of adopting new technologies from the perspective of cybersecurity in concrete business scenarios.		
Prerequisites	None	Co-requisites	None
Course Content	- General regulatory framework. European and Spanish regulation on cybersecurity and protection of critical infrastructures. - Personal data protection regulation. Singularities in the public sector. The Spanish National Security Scheme. - Cybersecurity and digital services. The singularities of financial services and payment tools. - Trust services legal framework. Digital identity - Criminal law and cybersecurity.		
Teaching Methodology	Face-to-Face and Online activities		
Bibliography	**<u>EU LAW</u>** - Jozef Andraško, Matúš Mesarčík, Ondrej Hamuľák: “The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework”, AI & SOCIETY volume 36, p. 623–636 (2021) - Dimitra Markopouloua, Vagelis Papakonstantinoua, Paulde Hert: “The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection		

Regulation”, Computer Law & Security Review, Volume 35, Issue 6, November (2019).

- Gloria González Fuster, Lina Jasmontaite: “Cybersecurity regulation in the European union: the digital, the critical and fundamental rights”, The ethics of cybersecurity. Springer, Cham, p. 97-115 (2020).
- Pier Giorgio Chiara: “The IoT and the new EU cybersecurity regulatory landscape”, International Review of Law, Computers & Technology, 36:2, 118-137 (2022).

SPANISH LAW

- Alamillo Domingo, A.: Identificación, firma y otras pruebas electrónicas: la regulación jurídica-administrativa de la acreditación de las transacciones electrónicas. Thomson-Reuters Aranzadi, 2018
- Beltrán, M. y Tejerina, O. (coords.): Aspectos jurídicos de la ciberseguridad. RA-MA, 2020
- Canals Ametller, D. (Dir.): Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales. Wolters Kluwer, 2021
- Fernández García, E.: “Derecho de la ciberseguridad de las infraestructuras críticas más allá de la perspectiva penalista”, Revista Jurídica de Castilla y León, núm. 56 2022
- Fondevila Antolín, J.: “Seguridad en la utilización de medios electrónicos: el Esquema Nacional de Seguridad”, en E. Gamero (dir.): Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del sector público. Tirant lo Blanch, 2017
- Galán, C.: “El derecho a la ciberseguridad”, en T. de la Quadra y J.L. Piñar (dirs.): Sociedad Digital y Derecho. Boletín Oficial del Estado, 2018
- Fuertes López, M.: Metamorfosis del Estado. Maremoto digital y ciberseguridad. Marcial Pons, 2022
- Llaneza González, P.: Identidad digital, Wolters-Kluwer Bosch, 2021
- Mallada Fernández, C. (coord.): Nuevos retos de la ciberseguridad en un contexto cambiante. Thomson-Reuters Aranzadi, 2019

Assessment	Examinations	45%
	Class Participation and Attendance	10%
	Assignments	45%
		100%

Language	English

Course Title	Software Security and Secure Software Lifecycle				
Course Code	EMC422				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	José A. Ruipérez Valiente				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of this course is to provide a broad overview of the secure software design process and the secure software lifecycle (SDL), reviewing methods and frameworks to accomplish these goals. Moreover, it will also review some of the main families of vulnerabilities, in order to provide prevention and detection guidelines. It will provide examples specifically applied to verticals.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify in a holistic way the different problems within a specific area of cybersecurity • Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that take into account multidisciplinary factors. • Identify management models of cybersecurity and associated processes to carry out the cybersecurity tracking and management within an organization				

	• Differentiate the different security properties offered by cryptographic primitives, the protocols that make use of them and the methods for the development of software security. • Analyse the scenarios where it is needed to provide software and protection mechanisms of the organizations' data considering the existing norms. • Propose the use of cryptographic primitives, secure protocols, and methodologies for the development of secure software based on the current scenario considering both technical and business aspects. • Evaluate the data and software security based on employed cryptographic primitives, secure protocols and the vulnerability analysis carried out.		
Prerequisites	None	Co-requisites	None
Course Content	• Unit 1: Secure software design o Security risk management o Security testing o Security coding techniques (code hardening) o Security requirements, validation and verification • Unit 2: Secure software lifecycle (SDL) o SDL frameworks (Microsoft, etc), adaptations (agile, mobile, etc) and assessment (SAMM, BSIMM, certifications , etc) • Unit 3: Prevention and detection of vulnerabilities o Prevention, detection and mitigation o Client and server side vulnerabilities • Unit 4: Secure software applied to vertical		
Teaching Methodology	Face-to-Face		

Bibliography	• [CS:P&P]: Computer Security: Principles and Practice. William Stallings and Lawrie Brown (4th edition). 2017. • [CCS]: Corporate Computer Security. Randall J. Boyle and Raymond R. Panko (5th edition). 2021. • [SiC]: Security in Computing. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies (5th edition). 2015. • [SR&ASD]: Secure, Resilient, and Agile Software Development. Mark S. Merkow. 2020 • [SDL]: The Security Development Lifecycle. Michael Howard and Steve Lipner. 2006. • [SSDF]: Secure Software Development Framework (SSDF). NIST Special Publication 800-218. Murugiah Souppaya, Karen Scarfone, and Donna Dodson, pp. 10-28, 2022. • [ETSI] Cyber security for consumer internet of things: Baseline requirements, ETSI EN 303 645, pp. 13-25, 2020. • [MSA] Microservices Security in Action: Design secure network and API endpoint security for Microservices applications, with examples using Java, Kubernetes, and Istio. W. N. Dias and P. Siriwardena, 2020 • [CC] Common Criteria for Information Technology Security Evaluation, Common Criteria, 2022. • [SOTA] State of the Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2, ECSO, 2017. **Unit 1** o [CS:P&P]: Chapter 10 Buffer Overflow. Chapter 11 Software Security. Chapter 14 IT Security Management and Risk Assessment. o [CCS]: Chapter 2 Planning and Policy. Chapter 8. Application security o [SiC]: Chapter 3 Programs and Programming, Chapter 4 The Web—User Side, Chapter 10 Management and Incidents o [SR&ASD] Chapter 8: Testing Part 1: Static Code Analysis, Chapter 9: Testing Part 2: Penetration Testing/Dynamic Analysis/IAST/RASP **Unit 2** o [SR&ASD] Chapter 5: Secure Design Considerations, Chapter 6: Security in the Design Sprint, Chapter 7: Defensive Programming, Chapter 10: Securing DevOps o [CS:P&P]: Chapter 13 Cloud and IoT Security. 12.8 Virtualization security o [CCS]: Chapter 4. Secure networks o [SiC]: Chapter 6 Networks, Chapter 8 Cloud Computing

	o [ETSI]: Full reference **Unit 3** o [SDL]: Part II: “The Security Development Lifecycle Process” o [SSDF]: Full reference. o [CS:P&P]: Chapter 15 IT Security Controls, Plans, and Procedures o [SR&ASD]: Chapter 11: Metrics and Models for AppSec Maturity o [MSA]: Chapter 1: Microservices security landscape **Unit 4** o [CC]: Part I: “Part 1: Introduction and general model” o [SOTA]: Full reference.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Authentication and Authorization Infrastructures
Course Code	EMC423
Course Type	Compulsory
Level	Master (2nd Cycle)

Year / Semester	Y1/S2				
Teacher's Name	Gabriel López Millán				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of this course is to introduce students to the concepts of authentication and authorization: models, trends, etc., and the main frameworks and standards about the management of Authentication and Authorization security architectures: SAML, Kerberos, etc.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Holistically identify the different problems related to a specific area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new environment in the field of cybersecurity. ● Design a presentation that includes the main ideas to be communicated, and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Present their knowledge in a clear, concise, unambiguous way and adapt to the time established for the presentation. ● Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Plan autonomous work tasks and self-learning processes running at the scheduled times. ● Learn about new trends, good practices, standards and regulations related to the field of cybersecurity.				
Prerequisites	None	Co-requisites	None		
Course Content	● Topic 1. Authentication, Authorization and Accounting				

	o Definition, models, etc. ● Topic 2. User authentication (passwords, biometrics, authentication tokens, behaviour, 2FA, etc.). o Management models, authentication and authorization processes. o Current trends in authentication processes. o Legislation and regulation. ● Topic 3. Authentication in distributed systems. o Description of the main distributed systems, such as Kerberos, SAML, OpenID Connect, etc. o Characteristics, functionality and evaluation of architectures for authentication ● Topic 4. Access control and authorization systems. o Description of the main access control and authentication systems, such as OAuth or XACML. o Characteristics, functionality and evaluation of architectures for access control and authorization. Topic. ● Topic 5. Accounting Management (privacy, logs, etc.) for the monitoring of systems and infrastructures.
Teaching Methodology	Face-to-Face
Bibliography	1. Stallings, William, et al., Computer Security - Principles and Practice (2018) . Chapters 3 and 4 (topics 1 and 2) 2. Stallings, William, Cryptography and Network Security - Principles and Practice, Global Edition (2017). Chapters 16 and 18 (topic 3). 3. Solving Identity Management in Modern Applications. Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0. Yvonne Wilson and Abhishek Hingnikar. Apress. Chapters 7 and 10 (Topics 3 and 4).
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%

Languag e	English

Course Title	Malware and Attack Technologies

<table>
<tr><td>Course Code</td><td colspan="5">EMC424</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">Y1/S2</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Juan Antonio Martínez Navarro, Félix Gómez Marmol</td></tr>
<tr><td>ECTS</td><td>6</td><td>Lectures / week</td><td>1.6 Hours / 14 weeks</td><td>Laboratories / week</td><td>1.6 Hours / 14 weeks e</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The objective of this course is to provide students with a wide perspective of the main malware and attacks technologies.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
● Taxonomy of malware. Dimensions and characteristics.
● Malicious activities of malware
● Malware analysis. Analysis techniques, analysis environments. Analysis evasion techniques.
● Malware detection. Identify presence, attack detection.
● Response to malware. Stopping operations. Identification.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5">● Unit 1: Malware Classification
● Unit 2: Malware Forensics
● Unit 3: Sandboxes and Multi-AV Scanners, automation and dynamic analysis</td></tr>
<tr><td>Teaching Methodology</td><td colspan="5">Face-to-Face</td></tr>
<tr><td>Bibliography</td><td colspan="5">● Michael Ligh, Steven Adair, Blake Harstein, Matthew Richard. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley. 2010
○ Chapter 3 (Unit 1)
○ Chapters 4, 7, 8, 9 (Unit 3)</td></tr>
</table>

	● Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. 2012. ○ Chapters 11, 12, 13 (Unit 1) ○ Chapter 2 (Unit 2) ○ Chapter 3 (Unit 3) ● ● Abhijit Mohanta, Anoop Sldanha. Malware Analysis and Detection Engineering. A Comprehensive Approach to Detect and Analyze Modern Malware. 2020 ○ Chapter 19 (Unit 1) ○ Chapter 24 (Unit 3) ● Dylan Barker. Malware Analysis Techniques. Tricks for the triage of adversarial software. 2021. ○ Chapter 2 (Unit 2) ○ Chapter 3, 5, 6 (Unit 3)
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	CyberSecurity Lab				
Course Code	EMC425				
Course Type	Compulsory				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Different teachers based on the projects labs				
ECTS	6	Lectures / week	1 Hours / 4 weeks	Laboratories / week	2 Hours / 14 weeks
Course Purpose and Objectives	This subject will have a structure in which the students per group must solve problems in a group, forming a response team and where they have to collaborate techniques and tools learned in the previous subjects, so that they can put the integration into operation in a practical way. of different tools. The formation of teams will be done so that students with different profiles can interact so that the teams can cover different aspects of solving cybersecurity problems. It will focus on carrying out simulated attack and reaction exercises where different teams can play different roles.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios. • Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. • Collect and analyze research data to address new problems in the field of cybersecurity. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. • Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. • Collaborate when solving a problem in the field of cybersecurity, teamwork and leadership. • Analyze methods and techniques of cyber attacks and cyber defense.				

	• List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to apply. • Carry out vulnerability and risk analysis processes. • Discuss the functionality of the elements incorporated in the architectures and security services of systems, critical infrastructures and communication networks. • Deploy monitoring elements in architectures and security services, critical infrastructures and communication networks. • Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communication networks..		
Prerequisites	First semesters courses	Co-requisites	None
Course Content	The master courses responsible will provide each year a collection of projects to be solved based on the interaction of different challenges covering different components and technologies already presented to the students. Students will organize in groups that will covered different aspects of a cybersecurity system that will solve the challenge		
Teaching Methodology	Face-to-Face		
Bibliography	• References from the different courses related to the technologies and techniques to be used		
Assessment	Assignments Class Participation and Attendance	80% 20% 100%	
Language	English		

Course Title	5G, IoT and Cyber-Physical Systems Security				
Course Code	EMC426				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Ramón J. Sánchez Iborra, Miguel Ángel Zamora, Benito Úbeda Miñarro				
ECTS	6	Lectures / week	1.6 Hours / 14 weeks	Laboratories / week	1.6 Hours / 14 weeks e
Course Purpose and Objectives	The objective of this course is to provide students with a wide perspective of the main security aspects to be considered in novel and evolving scenarios such as Internet of Things (IoT) deployments, Cyber-Physical Systems (CPS), Industrial Control Systems (ICS), and 5G architectures.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little-known environment in the field of cybersecurity. ● Collect and analyse research data to address new problems in the field of cybersecurity. ● Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow multidisciplinary aspects to be taken into account. ● Design solutions to cybersecurity problems using creative thinking. ● Design, deploy and maintain cybersecurity systems. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Describe the main elements and functions that are part of intelligent services, products and infrastructures in cybersecurity fields.				

	● Analyse scenarios in the field of cybersecurity from the point of view of the organization's security governance, the management of cybersecurity and the security of products, services and facilities. ● Design security management processes for products, services and facilities from the perspective of their security and considering business aspects (regulation, regulations, economic, etc.). ● Critically evaluate the processes of security governance, security management, design of products, processes, services and intelligent infrastructures in cybersecurity fields, taking into account into account requirements, existing solutions, regulations, standards and good practices. ● Deploy monitoring elements in security architectures and services, critical infrastructures, and communications networks. ● Analyse the security information collected through monitoring processes of system security architectures, critical infrastructures, and communications networks. ● Design security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering technical, business (economic, legal, environmental, etc.) and innovation aspects. ● Assess security architectures and services for systems, critical infrastructures and communications networks that are in accordance with the organization's policies, considering aspects technical, business (economic, legal, environmental, etc.) and innovation		
Prerequisites	None	Co-requisites	None
Course Content	● Unit 1: IoT security architecture and requirements. ● Unit 2: IoT Protocols and their security. ● Unit 3: Security in Industrial IoT/CPS. ● Unit 4: Security in Cellular Architectures.		
Teaching Methodology	Face-to-Face		

Bibliography	● IoT in 5 Days. ● A. D’Hondt, H. Bahmad, and J. Vanhee, “Mobile and Embedded Computing LINGI2146 Report ‘RPL Attacks Framework’”, 2016. ● Comparison of CoAP Security Protocols John Preuß Mattsson, Francesca Palombini , Mališa Vučinić. (full document) ● Terminology and processes for initial security setup of IoT devices ● THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World Internet Society 2015. (full document) ● Object Security for Constrained RESTful Environments (OSCORE) G. Selander, J. Mattsson, F. Palombini and L. Seitz July 2019. (Section 1 to 4, and Appendix A) ● Ephemeral Diffie-Hellman Over COSE (EDHOC) G. Selander, J. Preuß Mattsson and F. Palombini IETF Internet Draft. (Section 1 to 4) ● Sravani Bhattacharjee, Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries (English Edition), Chapters 1 and 4. 2018. ● Shancang Li, Li Da Xu, Securing the internet of things. Elsevier Syngress. Chapters 1 and 2. 2017. ● Larry Peterson and Oguz Sunay, 5G Mobile Networks: A Systems Approach. Open Networking Foundation (free book). Full book. 2020.
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Advanced Techniques in Cyber Intelligence
Course Code	EMC427
Course Type	Elective
Level	Master (2nd Cycle)
Year / Semester	Y1/S2

Teacher’s Name	Jorge Bernal and Antonio Skarmeta				
ECTS	6	Lectures / week	1,6 Hours / 14 weeks	Laboratories / week	1,6 Hours / 14 weeks
Course Purpose and Objectives	**Objective:** This course aims to teach students the current techniques, methods and tools for a holistic data processing, analysis and management of cyber intelligence information and systems. Students will be exposed to practical cyber intelligence techniques and tools. **Description:** The course will deal with architectures, formats and techniques for cyber threat intelligence (CTI) information management, data gathering and exchange, including confidential and privacy-preserving CTI sharing. In addition, the course will provide the foundations and mechanisms for data analysis of CTI information coming from different sources (e.g., osints, social networks) using techniques based on Artificial intelligence. The analysis will be put in practice for diverse purposes such as anomaly detection in complex distributed/federated scenarios.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyze in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Design cybersecurity scenarios, solutions, or systems including original or innovative aspects. ● Holistically identify the different problems related to a specific area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. ● Evaluate the methods, secure protocols, cryptographic techniques or software tools to use to undertake the resolution of a problem in a new or little known environment in the field of cybersecurity. ● Use knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. ● Collect and analyze research data to address new problems in the field of cybersecurity. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario				

	● Identify, organize and plan the technologies to study and/or bibliographic resources to analyze to address a specific problem within the field of cybersecurity. ● Design solutions to cybersecurity problems using creative thinking. ● Analyze methods and techniques of cyber attacks and cyber defense. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures and communications networks. ● Discuss the functionality of the elements incorporated in the security architectures and services of systems, critical infrastructures and communications networks. ● Deploy monitoring elements in security architectures and services, critical infrastructures and communications networks. ● Analyze the security information collected through monitoring processes of system security architectures, critical infrastructures and communications networks.		
Prerequisites	None	Co-requisites	None
Course Content	● Cyber intelligence information management ○ Architectures, phases and processes associated with cyber intelligence. ○ Automatic techniques for capturing, exchanging and managing cyber intelligence information. ○ Formats and representation of cyber intelligence information ○ Privacy and confidentiality in the exchange of cyber intelligence information. ● Advanced processing of cyber-intelligence information ○ Detection of cyber attacks and threats based on Artificial Intelligence. ○ Scalable and federated AI-based cyber intelligence systems. ○ Advanced computational techniques for anomaly detection. ○ Analysis of data from social networks and other sources for Cyber-intelligence ○ Design and management of cyber intelligence systems: practical cases		
Teaching Methodology	Face-to-Face		
Bibliography	• Michel Bazzel, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. ISBN-13 : 979-8761090064. Section II (topic cyber intelligence information management)		

	• Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense. ISBN-13 : 978-1800209404 Chapter 12,13,14 (topic cyber-intelligence) • Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers. ISBN-13 : 978-1484272190. Chapters 2,3, 7 (topic cyber intelligence) • Parisi, Alessandro. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019. ISBN-10: 1789804027, ISBN-13: 9781789804027. Chapter 4,5 (topic Advance processing of cyber-intelligence) • Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. " OReilly Media, Inc.", 2018. ISBN-10: # 1491979909, ISBN-13: 978-1491979907 Chapter 3,4,6 (topic Advance processing of cyber-intelligence)	
Assessment	Examinations Class Participation and Attendance Assignments	60% 10% 30% 100%
Language	English	

Course Title	Human factors in security, privacy and rights on the Internet				
Course Code	EMC428				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Antonio Ruiz Martínez,				
ECTS	3 ECTS	Lectures / week	1.5 Hours / 7 weeks	Laboratories / week	1.5 Hours / 7 weeks
Course Purpose and Objectives	The course covers the influence of human factors in cybersecurity and privacy and rights issues on the Internet. We will present main techniques and technologies to protect users' privacy and we will see tendencies in human factors, privacy and rights on the Internet.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Holistically identify the various problems related to a particular area of cybersecurity. ● Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or unfamiliar environments related to cybersecurity. ● Identify the different multidisciplinary aspects (legal, social, ethical) to be taken into account when dealing with a problem related to a cybersecurity scenario. ● Apply methods, cryptographic techniques, software tools or methodologies related to cybersecurity that allow taking into account multidisciplinary aspects. ● Plan autonomous work tasks and self-learning processes executing them in the foreseen times. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and to the target audience. ● Present their knowledge in a clear, concise and unambiguous way, adapting to the time established for the presentation. ● Prepare clear, concise and reasoned documentation on aspects related to the field of cybersecurity. ● Describe cryptographic primitives, secure protocols and software mechanisms that allow data protection.				

<table>
<tr><td></td><td colspan="3">● Employ the use of cryptographic primitives, secure protocols and software models to protect data in cybersecurity scenarios.
● Analyze scenarios where it is necessary to provide software and mechanisms to protect the organization's data in compliance with existing regulations.
● Identify new and emerging technologies, best practices, regulatory, legislative and human aspects related to cybersecurity and the mechanisms to detect these changes.</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="3">• Topic 1. Human Aspects of Cybersecurity
• Topic 2. Privacy and rights on the Internet
• Topic 3. Privacy techniques and technologies
o Primitives and protocols
o Technologies
• Topic 4. Trends in Human Factors in Security, Privacy and Rights on the Internet</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face-to-Face, Flipped classroom, use case, laboratories</td></tr>
<tr><td>Bibliography</td><td colspan="3">• Information Privacy Engineering and Privacy by Design - Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.
o Topic 1. Chapters 2, 3, and 12.
o Topic 2. Chapter 14.
o Topic 3. Chapters 7, 8 and 9.
o Topic 4. Chapter 9
• Privacy and Data Protection Challenges in the Distributed Era.
o Topic 1. Chapter 2.
o Topic 4. Chapter 3, 5, and 10.</td></tr>
<tr><td>Assessment</td><td colspan="3">Examinations 45%
Assignments 45%
Class Participation and Attendance 10%
100%</td></tr>
<tr><td>Language</td><td colspan="3">English</td></tr>
</table>

Course Title	Hardware Security				
Course Code	EMC429				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher's Name	Benito Ubeda and Miguel Angel Zamora				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	This course aims to provide holistic hardware security training and education in the design of new IoT and CPS devices, focus mainly in security aspects. This course contains a background of modern hardware devices with security issues and protection mechanism. During the course people will learn the different aspects of hardware security, which encompasses security vulnerabilities, attacks and protection mechanisms. The different hardware attacks will be analysed with examples: side-channel attacks, physical attacks, countermeasures and protections.				

Learning Outcomes	Upon successful completion of this course students should be able to: • Identify the main current problems in the field of cybersecurity in specific scenarios. • Analyze in detail scenarios, solutions or cybersecurity systems to detect possible aspects of improvement. • Design scenarios, solutions, or cybersecurity systems including original or innovative aspects. • Holistically identify the different problems related to a specific area of cybersecurity. • Apply methods, protocols, cryptographic techniques or software tools to solve problems in new or little-known environments related to cybersecurity. • Evaluate the methods, secure protocols, cryptographic techniques or software tools to be used to undertake the resolution of a problem in a new or little-known environment in the field of cybersecurity. • Use the knowledge to investigate new technologies and methodologies applied to the field of cybersecurity and thus contribute to its development. • Collect and analyze research data to address new problems in the field of cybersecurity. • Identify the main aspects to be communicated when presenting the results of a study or analysis related to cybersecurity and to the public to which it is addressed. • Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. • Present their knowledge in a clear, concise, unambiguous way and adapting to the time established for the presentation. • Analyze methods and techniques of cyber attacks and cyber defense.		
Prerequisites	None	Co-requisites	None
Course Content	Introduction to the main sources of vulnerability in hardware devices through the physical layer. Hardware security assessment. Main standards and their certification. Secure hardware platforms: HSM modules, TPM, secure elements, smartcards, etc. Review of basic techniques related to hardware security: Invasive methods: Cloning and manipulation of hardware at the chip level. Non-invasive methods: Electromagnetic coupling Techniques for secure implementations. Secure boot and OTP Prog memories Anti-tamper systems.		

	Safe items. Entropy sources through hardware devices: Physically Unclonable Functions (PUF), Random Number Generators.
Teaching Methodology	Face-to-Face
Bibliography	The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. Jasper van Woudenberg And Colin O'Flynn (Autor). Nov 2021. • Chapters 1,5,6,7,8 and 10. Hardware Security A Hands-on Learning Approach. Swarup Bhunia Mark Tehranipoor. October 2018. • Chapters 1,5,6,7,8 and 10. Emerging Topics in Hardware Security. Mark Tehranipoor. 2021
Assessment	Examination 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Reliable Distributed Systems				
Course Code	EMC4210				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	Ramón J. Sánchez Iborra, Juan Antonio Martínez Navarro, Miguel Ángel Zamora, Benito Úbeda Miñarro				
ECTS	3	Lectures / week	1.6 Hours / 7 weeks	Laboratories / week	1.6 Hours / 7 weeks e
Course Purpose	The objective of this course is to provide students with a wide perspective of the main security aspects of distributed systems in two main scenarios: (i) p2p				

and Objectives	architectures and applications, and (ii) distributed Industrial Control Systems (ICS).		
Learning Outcomes	Upon successful completion of this course students should be able to: ● Identify the main current problems in the field of cybersecurity in specific scenarios. ● Analyse in detail cybersecurity scenarios, solutions or systems to detect possible areas for improvement. ● Design cybersecurity scenarios, solutions, or systems including original or innovative aspects. ● Apply methods, protocols, cryptographic techniques, or software tools to solve problems in new or little-known environments related to cybersecurity. ● Identify the different multidisciplinary aspects (legal, social, ethical) to take into account when dealing with a problem related to a cybersecurity scenario. ● Identify the main aspects to communicate when presenting the results of a study or analysis related to cybersecurity and the target audience. ● Design a presentation that includes the main ideas to be communicated and the audiovisual materials that will reinforce the messages to be transmitted regarding a cybersecurity scenario. ● Design solutions to cybersecurity problems using creative thinking. ● Design solutions to cybersecurity problems using creative thinking. ● Identify the regulations and applicable legislation in the field of cybersecurity. ● Prepare clear, concise, and reasoned documentation on aspects related to the field of cybersecurity. ● Identify cybersecurity management models and associated processes to carry out the monitoring and management of cybersecurity within an organization. ● Identify the characteristics and functions of the elements that are part of the security architectures and services of systems, critical infrastructures, and communications networks. ● Discuss the functionality of the elements incorporated in system security architectures and services, critical infrastructure and communications networks. ● Describe the cryptographic primitives, the secure protocols and the software mechanisms that allow data protection. ● Employ the use of cryptographic primitives, secure protocols, and software models to protect data in a cybersecurity scenario. ● Identify new and emerging technologies, good practices, regulatory, legislative, and human aspects related to cybersecurity and the mechanisms to detect these changes. ● Plans autonomous work tasks and self-learning processes, executing them in the scheduled times. planned.		
Prerequisites	None	Co-requisites	None

Course Content	● Unit 1: P2P basics, architectures, applications and their security. ● Unit 2: Distributed ICS systems and their security.
Teaching Methodology	Face-to-Face
Bibliography	• B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” Comput. Electr. Eng., vol. 90, p. 106897, Mar. 2021, doi: 10.1016/j.compeleceng.2020.106897. • A. Abdelmaboud et al., “Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions,” Electronics, vol. 11, no. 4, p. 630, Feb. 2022, doi: 10.3390/electronics11040630. • Pascal Ackerman, Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment, 2nd Edition, Chapters 1,4,5,6,7,14 and 17. 2021 • Charles J. Brooks, Practical industrial cybersecurity, ics, industriy 4.0 and IoT, Chapters 2,3 and 5. 2022
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Advanced Aspects of Cybersecurity Management
Course Code	EMC4211
Course Type	Elective

Level	Master (2nd Cycle)				
Year / Semester	Y1/S2				
Teacher’s Name	Antonio Skarmeta and Jorge Bernal				
ECTS	3	Lectures / week	2 Hours / 7 weeks	Laboratories / week	1 Hours / 7 weeks
Course Purpose and Objectives	The objective of the course is to prepare students to understand Cybersecurity governance as the process of establishing the architecture that ensures a company's security programs align with business objectives, comply with regulations and standards (such as PCI security standards), and achieve objectives for managing security and risk. As a supplement to the course on Techniques for the Management of Cybersecurity, in this one we focus more on the application of methodology and the use case analysis in order to define cybersecurity governance approaches and solutions to different incidents and situations.				
Learning Outcomes	Upon successful completion of this course students should be able to: ● Collect and analyze research data to address new problems in the field of cybersecurity. ● Design, deploy and maintain cybersecurity systems. ● Identify the applicable regulations and legislation in the field of cybersecurity. ● Evaluate and define the different measures to be applied (contingency plans, etc.) based on vulnerabilities, threats and risks, considering both technical and business (economic and political) aspects. ● Analyze forensic reports, and define action plans and their application. ● Define the scope and impact caused by a specific cyber incident.				
Prerequisites	EMC414	Co-requisites	None		
Course Content	ICT and cybersecurity elements and assets ● Types of assets ● Valuation Dimensions ● Assessment criteria ● Threats and Safeguards Cybersecurity operations intelligence ● ID ● Protection ● Detection ● Response ● Recovery				

	Design and Planning of a Cybersecurity Systems ● Cybersecurity Planning ● Business continuity, disaster recovery and incident management ● Security program management ● Definition of an information protection model in an ISMS (Information Security Management System) ● Legal aspects and regulations applicable to the exchange of data and their impact on the design of the systems ● Advanced intelligence on cyber threats Best practices in design and deployment ● Cyber Threat Hunting ● CTI with privacy preservation ● Cyber exercises and simulation platforms
Teaching Methodology	Face-to-Face
Bibliography	1. Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology. Chapter 1-3, and annex 2. CISSP Certified Information Systems Security Professional (ISC)2 2021. Chapter 1,3,5,8 3. NIST Cybersecurity Framework V1.1 Chapter 1-3 4. Practical Use Cases https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis-1/file.html
Assessment	Examinations 45% Assignments 45% Class Participation and Attendance 10% 100%
Language	English

Course Title	Cybersecurity Architecture and Operations
Course Code	EMC431

Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Nikos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify the various components of a comprehensive cybersecurity architecture within an organization. • Describe and classify controls that meet specific control objectives and to treat identified risks. • Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc. • Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover. • Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others. • Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control. • Evaluate and select appropriate architectural and operational options according to the organizational risk environment.				
Prerequisites	None	Co-requisites			
Course Content	Introduction: Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication.				

	Processes: User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others. Phases: Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover. Identify: Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process. Protect: Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening. Detect: Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicatiors of compromise (IOC). Respond: Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls. Recover: Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes. Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.
Teaching Methodology	Face – to – face
Bibliography	*Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.* *Santos, O., Developing Cybersecurity Programs and Policies. Pearson.*

	“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor) *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker* *ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management* *ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements* *Contreras, J., 2013. Developing a Framework to Improve Critical Infrastructure Cybersecurity (Response to NIST Request for Information Docket No. 130208119-3119-01). SSRN Electronic Journal.* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	EMC432				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Yianna Danidou				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course provides an overview of the broad and constantly emerging field of cybersecurity policy, governance, law and compliance. The importance of the role of security policy is discussed.				
Learning Outcomes	Upon succesful completion of this course, students should be able to: • State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security. • State and interpret the different components of a comprehensive organizational cybersecurity policy. • State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment. • Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function. • Recognize and explain major applicable legislation and regulatory framework (local, European, international). • Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.				
Prerequisites	None		Co-requisites		

Course Content	Introduction: Concepts of cybersecurity, its relationship with network and information security, cybercrime, cyberdefence, and related definitions. Concepts of policy, governance, related law and compliance, and the relationships between them. Principles: Information security components and concepts, confidentiality, integrity, availability. Policy: definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures. Governance: Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation. Law: Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations. IT and Law: Introduction, Terminology, and the Nature of Cyberspace and Threats. Cyber-regulation and cyber-regulatory theory. Cyberproperty and Intellectual Property. Cyber-rights, Speech Harm, Crime and Control. Roles of International Law, the State, and the Private Sector in Cyberspace. Authentication and Identity Management. Speech, Privacy and Anonymity in Cyberspace. Trust. Compliance: Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.
Teaching Methodology	Face – to – face
Bibliography	*“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *“Information Security Governance: A Practical Development and Implementation Approach”*, by Krag Brotby

	“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”, by Scott E. Donaldson *“Cyber Security and IT Infrastructure Protection”*, by John R. Vacca *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Cybersecurity Risk Analysis and Management				
Course Code	EMC433				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Nikos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental concepts of cybersecurity risk analysis and management, as well as its position as the foundation for cybersecurity protective mechanisms. It covers a wide range of principles and processes related to risk management and sets the scene for the development of comprehensive cybersecurity controls to protect an organizations assets according to the risk appetite of senior management.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities • Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc. • Recognise the difference between vulnerabilities and threats. • Classify and describe a number of different risk assessment/management methodologies. • Classify and describe different assets and their values (including tangible and intangible assets). • Identify and explain various threat sources and the impacts that their materialization may manifest. • Describe the risk management process, as it pertains to the protection of assets. • Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.				
Prerequisites	None	Co-requisites			

Course Content	Introduction: Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme. Principles: Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. Assets: Tangible and intangible assets in the cyber world (hardware / software / data, classification, criticality based on the importance and value to organization (not just monetary), dependencies, potential for critical national infrastructure. Vulnerabilities: Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information. Threats: Cyber threat categorization, sources, motivation, type, technical vs. non technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood. Risk analysis: Risk as a combination of possible impact of a threat exploiting a vulnerability and the probability of such an impact occurring, evaluation of cyber risks, categorization, qualitative and quantitative risk analysis, pre-requisites for meaningful quantitative cyber risk assessment, methodologies, risk register. Risk management: Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organisation's environment, building an organisation's cybersecurity control environment from the results of risk analysis, introduction to basic cybersecurity controls. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical uses challenges of risk analysis and management in real environments.
Teaching Methodology	Face – to – face
Bibliography	*"Effective Cybersecurity: A Guide to Using Best Practices and Standards 1st Edition, by Willian Stallings* *"Cyber-Risk Management" by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen*

	Samimi, A., 2020. Risk Management in Information Technology. Progress in Chemical and Biochemical Research, pp.130-134. *“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *Tarek, M., Mohamed, E.K., Hussain, M.M. and Basuony, M.A., 2017. The implication of information technology on the audit profession in developing country. International Journal of Accounting & Information Management.* *“How to Measure Anything in Cybersecurity Risk”*, by Douglas W. Hubbard and Richard Seiersen *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”*, by Anne Kohnke and Dan Shoemaker
Assessment	Final Examination 50% Midterm Examination 40% Attendance/Participation 10%
Language	English

Course Title	Master Thesis				
Course Code	EMC441				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Yianna Danidou				
ECTS	30	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	The course's purpose is to provide guidance on how to write a successful Master's Thesis. It aims to provide skills in research methods, regardless of the student's subfield of study (as long as it is in the general field of Computer Science). It also aims to equip the student with the tools required to manage a project as large as a Master's thesis, through providing project management techniques. Finally, it aims to prepare the student for independent work as a recipient of a Master's degree.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Demonstrate written and oral technical research skills. • Select and justify a research topic, and use various resources to carry out a literature search. • Design, execute, interpret and report results from empirical research projects. • Manage a project and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources. • Identify real-world problems to which academic concepts and methods can be realistically applied to improve or resolve the problem situation. • Select and use effectively the methods and techniques appropriate for particular cases, and plan and manage their work. • Evaluate a proposed solution and prove its worth to the client. • Critically evaluate the project and the proposed solution, as well as recognize and describe legal, social or ethical obligations stemming from the project.				
Prerequisites	Successful completion of all core courses	Co-requisites	None		
Course Content	Part A: Research Methods: The nature of research:				

Definitions and types of research; research process; topic selection and scope; feasibility and value.

The literature search:
Sources of information; differentiating between types of sources; primary, secondary and tertiary sources; using the library and digital databases to conduct efficient literature reviews; searching the Internet; role of the supervisor.

Project management:
Methods, techniques and tools for research design, and data collection.

Analysis and synthesis:
Statistical and qualitative techniques for data analysis; use of appropriate software. Reliability and validity of research projects.

Presentation of research findings:
Project structure; conventions on citation and quotations; style of writing a report.

Part B: Thesis:

The student selects a topic from the Thesis Topics Catalogue which becomes available on the first day of the first week of the semester. Students receive the catalogue via a personal email sent to them by the course instructor, and they are also available on the departmental website. Once the students receive the topics, they have two weeks (by the second Friday of the semester) to choose a topic. Topics are assigned on a First-Come, First-Served basis, given that the students have passed all the pre-requisite courses for a specific topic. Once a topic is selected and agreed upon with the associated supervisor, the course follows the weekly breakdown structure as that is provided in the study guide. See Master Thesis study guide for further details.

The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. The roles and responsibilities are outlined below:

Student:

- To identify and scope a suitable problem
- Explain the value of the research
- To plan and control the project
- To carry out the necessary work
- To review and evaluate the work done
- To prepare and present the project deliverables
- To initiate and maintain contact with the academic supervisor

	Academic Supervisor: • To comment on the suitability of the selected project • To discuss the mapping of the project onto the course requirements • To discuss and approve the intended deliverables • To suggest starting points for consideration of background research • To discuss the nature of the thesis and comment on early drafts • To provide advice on issues associated with the project such as design, implementation, and proof of concept as appropriate. • To attend any presentation or demonstration of the project **Program-specific content** As this course is taught in a variety of Master's programs offered by the department of Computer Science, the last part of the course will discuss specific research methods for each discipline. The specific topics will be provided by the instructor of the course according to the specific needs of the audience.
Teaching Methodology	For Part A: Research Methods there will be research seminars and a number of face–to–face sessions with the instructor. For Part B: Face-to-face
Bibliography	Any material suitable for the subfield in which the student is undertaking the thesis will be specified by the instructor. Howard, K. & Sharp, J.A., The Management of a Student Research Project, Gower Turk, C. & Kirkman, J., Effective Writing: Improving Scientific, Technical and Business Communication, Chapman & Hall J. Zobel., Writing for Computer Science, Springer. W. Navidi, Statistics for Engineers and Scientists, McGraw-Hill Science/Engineering/Math; Latest Edition. Statistical Methods for Engineers, by Geoffrey Vining and Scott M. Kowalski, Thomson, Brooks/Cole, Latest Edition. J.G. Paradis, M., Zimmerman,The MIT Guide to Science and Engineering Communication, The MIT Press. D. Madsen, Successful Dissertations and Theses: A guide to graduate student research from proposal to completion, Jossey Bass.

	Edgar, T. W. and Manz, D. O. Research Methods for Cyber Security. Cambridge, MA: Syngress. Argyrous, G. . Statistics for Research: with a guide to SPSS. Los Angeles, CA: Sage. King, R. S. Research Methods for Information Systems, Dallas, TX: Mercury Learning & Information Cohen, P. R. Empirical Methods for Artificial Intelligence, Cambridge, MA: The MIT Press.
Assessment	**ASSESSMENT STRATEGY:** The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. However, each project must involve deliverables falling into the following general categories: (a) A proposed solution to a real-world problem. (b) A proof of concept, which demonstrates the validity of the proposed solution. (c) Clear indication of knowledge of relevant work by others in the field. (d) The selection and application of appropriate theoretical concepts and methods. (e) A project thesis of between 12,000 to 16,000 words. Projects will be marked in two ways. Firstly, according to the following scheme: • Project justification including its relationship to the current state of the art 10% 20 marks • Ability to select and use appropriate methods and techniques 10% 20 marks • The clarity, coherence and succinctness with which the solution is developed 30% 60 marks • Novelty. Does the work improve significantly the current state of the art? 30% 60 marks • Ability to critically review the project and assess its implications for future work in view of the project recommendations and conclusions 10% 20 marks

	• Project Management: Ability to plan and control the project 10% 20 marks ______ _________ 100% 200 marks In addition students are reminded about presentation issues: Is the document format (including spelling) of good quality? Is it well organized into appropriate sections? Is the style of language used appropriate for an academic report? **ASSESSMENT:** Written Thesis: 80% Oral Presentation 20%
Language	English

ANNEX III

TABLE X: MAPPING RESEARCH STRENGTHS OF EACH PARTNER

A/A	Name and Surname	Discipline / Specialization	Teaching courses in the programme of study under evaluation (Master in Cybersecurity)		
			Code	**Course title**	**Research strengths**
EUC					
1.	Yianna Danidou	Computer Science, Cybercrime, Cybersecurity, Law and IT	EMC111 EMC113/EMC432	Introduction to Cybersecurity Cybersecurity Policy, Governance, Law and Compliance	Cybersecurity education Cybersecurity and legal implications
2.	Konstantinos Vavousis	Cyber Security	EMC112 EMC122	Communications and Network Security Ethical Hacking and Penetration Testing	Ethical Hacking and Penetration Testing Cybesecurity maturity models
3.	Nikos Tsalis	Information Security	EMC121/EMC431 EMC123/EMC433 EMC124	Cybersecurity Architecture and Operations Cybersecurity Risk Analysis and Management Data Privacy in the Era of Data Mining and AI	Cybersecurity risk analysis Data privacy

4.	Dimitrios Baltatzis	Information Security	EMC125	Incident Response and Forensic Analysis	Incident Response and Forensic Analysis Cyber threat analysis

UMU					
1.	Antonio Skarmeta	Cybersecurity, IoT and 5G	EMC216/ EMC316/ EMC416 EMC227/ EMC327/ EMC427 EMC329/ EMC4211	Innovation and Entrepreneurship Seminar Advanced Techniques in Cyber Intelligence Advanced Aspects of Cybersecurity Management	Internet of things and 5G security, IoT communications, routing, and network security. Security lifecycle management issues, Threat analysis and Cybersecurity governance
2.	Ramon Sánchez Iborra	IoT, wireless networks, quality of service	EMC226/ EMC326/ EMC426 EMC229	5G, IoT and Cyber-Physical Systems Security Reliable Distributed Systems	Wireless Communications, Next-generation Mobile Network
3.	Gabriel López Millán	Network Security, Identity Management, Authentication and Authorization Infrastructures	EMC223/ EMC323/ EMC423	Authentication and Authorization Infrastructures	AAA and network management, identity

					management and two-factor authentication mechanisms
4.	José A. Ruipérez Valiente	Software Development, Programming, Cybersecurity	EMC222/ EMC322/ EMC422	Software Security and Secure Software lifecycle	Human oriented security and interfaces for privacy and security
5.	José Ramón Hoyos-Barceló	Software engineering, Computer Forensics, Model-driven engineering	EMC212/ EMC312/ EMC412	Cyberdefense Techniques	DevSecOps, test and validation of software security
6.	Julián Valero Torrijos	Innovation, Law & Technology	EMC221/ EMC321/ EMC421	Cybersecurity Legal Framework	Legal impact of cybersecurity,Data protection
7.	Leandro Marín Muñoz	Applied Mathematics and Cryptography	EMC215/ EMC315/ EMC415	Cryptography	Cryptography, hardware security
8.	Benito Ubeda-Miñarro	Cross-Cutting Issues in Cybersecurity	EMC226 EMC228	5G, IoT and Cyber-Physical Systems Security Hardware Security	Embedded systems for 5G and security,
9.	Rafael Marín López	Network Security, IoT security, Authentication and Authorization Infrastructures	EMC213/ EMC313/ EMC413	Cybersecurity and Network Security	Secure bootstrapping and network services
10.	Jorge Bernal Bernabe	Cybersecurity, Data science, privacy	EMC227/ EMC327/ EMC427 EMC329/ EMC4211	Advanced Techniques in Cyber Intelligence Advanced Aspects of Cybersecurity Management	AI-based security and mitigation, federated learning and intrusion detection
11.	Manuel Gil Pérez	Cybersecurity, risk management	EMC214/ EMC314/ EMC414	Techniques for the Management of the Cybersecurity	Offensive security and threat modeling, and risk analysis

12.	Miguel Angel Zamora Izquierdo	Cross-Cutting Issues in Cybersecurity	EMC228/ EMC429 EMC229/ EMC4210	Hardware Security Reliable Distributed Systems	Industrial Internet of Things, security for constrained devices
13.	Oscar Cánovas	Identity Management, Authentication and Authorization Infrastructures	EMC213/ EMC313/ EMC413	Cybersecurity and Network Security	network security protocols for Internet, wireless security, IP layer security and transport security
14.	Felix Gómez Marmol	Social security, malware and secure systems	EMC211/ EMC311/ EMC411	Cyberattack Techniques and Ethical Hacking	Ethical hacking and secure software design
15.	Juan Antonio Martínez	IoT, wireless networks, cyber defense	EMC224/ EMC324/ EMC424	Malware and Attack Technologies	wireless security and Intrusion detection, malware analysis
16.	Antonio Ruiz	Security and Privacy	EMC211/ EMC311/ EMC411 EMC328/ EMC428	Cyberattack Techniques and Ethical Hacking Human Factors in Security, Privacy and Rights on the Internet	Privacy preserving techniques, privacy compliance, and user interactions

BUT					
1.	Jiří Hošek	Wireless communication technologies, IoT, industrial automation	EMC131	Mobile Network Communication Systems	Teleinformatics – Wireless communications, and Internet of Things
2.	Sara Ricci	Cryptography, Data Privacy and Security, Applied Mathematics	EMC132 EMC133	Foundations of Cryptography Modern Cryptography	Cryptography, Applied Mathematics, Privacy Enhancing technologies, and Data Privacy
3.	Radim Burget	Machine learning, AI, Data Processing	EMC136 EMC134	Data Structures and Algorithms Parallel Data Processing	Data science, Data Processing, and AI
4.	Jaroslav Koton	Modern networking technologies, digital signal processing, integrated circuits design	EMC137	Modern Network Technologies	Communication systems, Quality of Service, Signal processing
5.	Petr Münster	Fibre optics, quantum communications, cybersecurity	EMC138	Optical Networks	Data Science and machine learning
6.	Petr Dzurenda	Cryptography, network security, OS security	EMC132 EMC133	Foundations of Cryptography Modern Cryptography	Cryptography, network security, OS security
7.	Vojtěch Myška	Machine learning, information systems, high-performance computing	EMC134	Parallel Data Processing	Machine learning, information systems, high-performance computing
8.	Patrik Dobiáš	Information security	EMC133	Modern Cryptography	Hardware-Accelerated Cryptography

9.	Radek Možný	Industrial Internet of Things, Cellular Internet of Things, Sub-6GHz 5G wireless technologies	EMC131	Mobile Network Communication Systems	Industrial Internet of Things, Cellular Internet of Things, Sub-6GHz 5G wireless technologies
10.	Ondřej Krajsa	Computer networks, wireless sensor systems, embedded hardware	EMC137	Modern Network Technologies	Computer networks, wireless sensor systems, embedded hardware
11.	Pavel Mašek	PhD in Telecommunications	EMC131	Mobile Network Communication Systems	Wireless Communications, Industrial Internet of Things, Next-generation Mobile Network
12.	Petr Číka	Multimedia, cyber security	EMC141 EMC135	Diploma Thesis Semestral Thesis	Cryptography and Internet of Things

POLIMI					
1.	Mario Polino	Cybersecurity	EMC231	Offensive and defensive cybersecurity	Offensive security and threat modeling, malware analysis
2.	Stefano Zanero	Cybersecurity	EMC232	Digital Forensics and cybercrime	Intrusion detection, malware analysis, security of cyberphysical systems; national security issues
3.	Greta Nasi	Cyber risk, government innovation and competitiveness.	EMC234	Resilience Of Critical Infrastructures	Security policy, government
4.	Gerardo Pelosi	Cryptography	EMC235	Cryptography And Architectures For Computer Security	Cryptography (hardware and algorithm design)
5.	Riccardo Scattolini	Automation	EMC236	Safety In Automation Systems	Safety in control systems (automotive and other domains)
6.	Viola Schiaffonati	Philosophy of Science	EMC237	Computer Ethics	Ethics of scientific research and algorithmic ethics
7.	Prof Matteo Matteucci	Artificial Intelligence and Robotics	EMC238 EMC233	Artificial Neural Networks and Deep Learning Data Science and Security for Mobility	Applications of machine learning to physical, autonomous systems

ELTE					
1.	Imre Lendák	Critical infrastructure security, applied data science	EMC334 EMC336	Introduction to Data Security Lab Open-Source Technologies for Data Science	Industrial control system security, critical infrastructure protection, open-source technologies in infrastructure monitoring, AI security, applied cryptography
2.	Jiyan Mahmud Salim	Applied data science, anomaly detection	EMC337	Stream mining	Anomaly detection, applied open-source systems in large-scale monitoring solutions, low-level TCP
3.	Ikrame Nouar	Applied data science	EMC336	Open-source technologies for real-time data analytics	Intrusion detection systems, anomaly detection, applied open-source systems in large-scale monitoring solutions
4.	Péter Kiss	Data science, federated learning, history	EMC337	Stream mining	Applied data science, stream mining, AI security, data science & privacy
5.	Tomáš Horváth	Data science	EMC333 EMC335	Data Science Lab II. Introduction to Data Science	Applied data science, recommender systems
6.	Norbert Tihanyi	Cybersecurity, cryptography	EMC331	Cyber security Lab II.	Theoretical cryptography, formal verification, generative AI in security

7.	Péter Ligeti	Applied cryptography	EMC332	Advanced cryptography	Theoretical cryptography, privacy-aware computation, crypto hacking, post-quantum cryptography