Cybersecurity

Code: 105779
ECTS Credits: 6

2024/2025

Degree	Type	Year
2502501 Prevention and Integral Safety and Security	FB	2

Contact

Name: Jose Cañabate Perez

Email: josep.canabate@uab.cat

Teachers

Laura Casas Diaz

Teaching groups languages

You can view this information at the end of this document.

Prerequisites

There are no prerequisites.

The teaching of the subject will be taught taking into account the perspective of the Sustainable Development Goals.

Objectives and Contextualisation

- Know the basic computer concepts and the functioning of an information system that can affect the security of organizations or people.

- Know the physical components of a computer system or computer and networks.

- Know the process of auditing information systems.

- Analyze the Government and the Management of Information Technologies.

- Study the fundamental aspects of Information Security Management.

- Analyze the main standards of Information Security.

- Know the fundamental concepts of Cybersecurity.

- Analyze the typologies of technological crime, electronic evidence and Forensic Readiness.

Competences

- Act with ethical responsibility and respect for fundamental rights and duties, diversity and democratic values.
- Apply specific software tools to solve problems specific to security.
- Be able to communicate efficiently in English, both orally and in writing.
- Carry out scientific thinking and critical reasoning in matters of preventions and security.
- Contribute to decisions on investment in prevention and security.
- Efficiently manage technology in security operations.
- Evaluate the technical, social and legal impact of new scientific discoveries and new technological developments.
- Generate innovative and competitive proposals in research and in professional activity developing curiosity and creativity.
- Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
- Make efficient use of ITC in the communication and transmission of results.
- Show respect for diversity and the plurality of ideas, people and situations.
- Students must be capable of applying their knowledge to their work or vocation in a professional way and they should have building arguments and problem resolution skills within their area of study.
- Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
- Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
- Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
- Students must have and understand knowledge of an area of study built on the basis of general secondary education, and while it relies on some advanced textbooks it also includes some aspects coming from the forefront of its field of study.

Learning Outcomes

1. Apply the basis of statistics, economics and finance, in the applicable legal framework and the informatics necessary to undertake prevention and security.
2. Apply tools and develop specific software for solving the problems that are particular to security, the environment, quality and social corporate responsibility.
3. Be able to communicate efficiently in English, both orally and in writing.
4. Carry out scientific thinking and critical reasoning in matters of preventions and security.
5. Critically analyse the principles, values and procedures that govern professional practice.
6. Evaluate the technical, social and legal impact of new scientific discoveries and new technological developments.
7. Explain the explicit and implicit deontological code for the area of knowledge.
8. Formulate strategies of company management.
9. Generate innovative and competitive proposals in research and in professional activity developing curiosity and creativity.
10. Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
11. Make efficient use of ITC in the communication and transmission of results.
12. Propose projects and actions in accordance with the principles of ethical responsibility and respect for fundamental rights and responsiblities, diversity and values democráticos.
13. Show respect for diversity and the plurality of ideas, people and situations.
14. Students must be capable of applying their knowledge to their work or vocation in a professional way and they should have building arguments and problem resolution skills within their area of study.
15. Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.

16. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
17. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
18. Students must have and understand knowledge of an area of study built on the basis of general secondary education, and while it relies on some advanced textbooks it also includes some aspects coming from the forefront of its field of study.

Content

The course syllabus covers a broad spectrum of essential concepts and practices in the field of cybersecurity and information technology. It begins with an introduction to the course methodology, providing students with a solid foundation in the fundamental concepts of IT and information security. As the course progresses, known cybersecurity incidents, various types of cyberthreats, and the role of artificial intelligence in detecting and responding to these incidents are explored. Cyberdefense strategies and national plans designed to protect critical infrastructures are also discussed.

The course also covers state and European regulations related to cybersecurity, as well as technological crime and the importance of electronic evidence in the investigation of computer crimes. In addition, it teaches how to prepare an organization for digital forensic investigations, including the protection of information assets and the application of internationally recognized cybersecurity standards. Finally, it addresses the protection of critical infrastructures and the development of business continuity plans to ensure that an organization can continue to operate during and after disruptive incidents. This comprehensive approach prepares students to meet cybersecurity challenges effectively and competently.

BLOCK 1

Topic 1. Introduction and methodology of the subject.
Topic 2. Basic concepts of information technologies.
Topic 3. Basic concepts of information security and cybersecurity.

BLOCK 2
Topic 4. Known cybersecurity events
Topic 5. Cyberthreats: definition and types
Topic 6. Artificial Intelligence and cybersecurity.
Topic 7. Cyberdefense and national cybersecurity plans.

BLOCK 3
Topic 8. State and European regulations on cybersecurity.
Topic 9. Technological crime.
Topic 10. Electronic evidence.
Topic 11. Forensic Readiness and Digital Forensic Investigation.

BLOCK 4
Topic 12. Protection of information system assets.
Topic 13. Analysis of the main cybersecurity standards.
Topic 14. Critical infrastructures and Business Continuity Plan.

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			

Videoconference with the active participation of the students	12	0.48
Type: Supervised		
RESOLUTION OF DOUBTS ON SUBJECT AND PRACTICES	6	0.24
Type: Autonomous		
PRACTICAL CASES PREPARATION	60	2.4
RISC SCENARIOS STUDY AND RESOLUTION	60	2.4

Teaching language: Spanish.

Bearing in mind that the modality of the class is Online, with the objective of reaching the learning objectives described in this Guide we will develop a methodology that combines individual study from the Manual, and the readings that will be presented in each subject, in addition de algunos documentales. Each subject will have a question forum, and a "Contributions" Forum will be established where students can introduce readings, articles, websites, documentaries, and all types of materials and resources related to the subject. On the other hand, the resolution of two practical cases related to the subjects studied in the subject must be carried out. It should be noted that due to the Online model, students will have to prepare the materials independently (documents, readings, videos, etc.) and Online forums and sessions will be dedicated to deepening the topics discussed as well as resolving possible doubts.

On the other hand, the subject will use Problem-Based Learning for the development of part of its evaluation activities. Problem-based learning (PBL) is an educational methodology that uses real problems as a starting point for the acquisition and integration of new knowledge. In the context of cybersecurity, this approach is particularly well suited due to the dynamic and multifaceted nature of cyber risks. Here we describe how this methodology can be applied to cyber security risk scenarios. In an ABP environment, students are presented with a cybersecurity risk scenario. This could be a ransomware attack on a company, a data breach in a financial organization, or a targeted phishing campaign. The problem must be complex and open, allowing multiple approaches and solutions. The students are organized in small collaborative groups. Each group works independently to analyze and understand the problem presented. Collaboration encourages the exchange of ideas, discussion and the confrontation of different points of view, which enriches the learning process. Students identify what they know and what they need to learn to address the problem. This involves active research, where students seek relevant information about cybersecurity, including attack and defense techniques, applicable regulations, and best practices. The research may include the review of academic literature, analysis of previous case studies, and consultation with experts in the field. With the information collected, the students analyze the problem in depth, identifying the exploited vulnerabilities and the possible consequences. Based on this analysis, they develop strategies and action plans to mitigate the risk and prevent future incidents. Finally, it should be noted that this process requires critical thinking and the application of technical and theoretical knowledge acquired during the course.

Annotation: Within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continous Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes

FINAL EXAM	50%	2	0.08	1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18
PARTICIPATE IN FORUMS AND CLASS	10%	5	0.2	2, 14, 15, 16, 17, 18
PRACTICAL EVALUATION ACTIVITIES	40%	5	0.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18

The assessment of the subject will be carried out by:

1. CONTINUOUS ASSESSMENT

- Completion of four Continuous Assessment Practices (40%)

Individual Work:
Consists of two PACs.

PAC 1: On basic concepts of cybersecurity.

PAC 2. On basic concepts of cryptology.

Group work:
Consists of two group PACs:

PAC 3: Definitions and main characteristics of an Advanced and Persistent Threat (APT).

PAC 4: Risk scenario related to an Advanced and Persistent Threat (APT).

- Participation in discussion forums and classes (10%)

To overcome this section, each student will have to make a quality participation in each discussion forum (there will be 4 forums, divided by thematic areas). Therefore, each student is expected to: a minimum of 4 quality contributions (that is to say, providing ideas and comments that go beyond what is found in the manuals, including bibliography and references) Upon completion, each student will have to enter a minimum of 4 contributions in the intended section for the purposes of the subject. Each intervention in the forum and each contribution represents 10% of the evaluation of this section, the qualification will be established based on criteria of quality, originality, coherence and interaction, if cap. Any extra contributions or interventions will be valued positively, but remember that they cannot exceed 1 point that this section has in relation to the overall grade.

- Multiple choice test on the entire syllabus (50%)

It will consist of a 30-question multiple choice test on the syllabus with four possible options. The correct question adds 1 out of 30, the incorrect question subtracts 0.25 out of 30, the unanswered question neither adds nor subtracts.

REVIEW OF THE FINAL QUALIFICATION: A day and time for review will be arranged with the professors within amaximum period of 48 hours. after the publication of the final qualifications.

RECOVERY

If the subject is not passed according to the criteria previously established (continuous assessment), a recovery test may be taken on the date scheduled at the time, which will cover all the program content.

To participate in the re-examination, the student must have been previously assessed in a set of activities, the weight of which is equivalent to a minimum of two thirds of the total grade for the subject. However, the grade that will appear on the student's record is a maximum of 5 - Pass.

Students who need to change an assessment date must submit a justified request using the document that will be found in the EPSI Tutoring Moodle space.

PLAGIARISM

Without prejudice to other disciplinary measures that are deemed appropriate, and in accordance with current academic regulations, "in cases where the student commits any irregularity that could lead to a significant variation in the qualification of a certificate of evaluation, this evaluation report will be graded with a 0, independently of the disciplinary process that is to be instructed. In cases where various irregularities occur in the evaluation reports of a subject, the final grade for this subject will be 0. .

The tests/exams may be written and/or oral at the discretion of the teacher.

If during the correction there are indications that an activity or work has been carried out with responses assisted by artificial intelligence, the teacher may complement the activity with a personal interview to corroborate the authorship of the text.

NOT EVALUABLE:

Students will be evaluated as long as they have completed a set of activities, the weight of which is equivalent to a minimum of 2/3 of the total grade for the subject. If the value of the activities carried out does not reach this limit, the subject teacher may consider the student as non-assessable.

2. SINGLE EVALUATION.

Students who opt for the single assessment will take the following tests.

- Carrying out four practices (40%)

PAC 1: On basic concepts of cybersecurity.

PAC 2. On basic concepts of cryptology.

PAC 3: Definitions and main characteristics of an Advanced and Persistent Threat (APT).

PAC 4: Risk scenario related to an Advanced and Persistent Threat (APT).

- Making text comments on a cybersecurity topic related to the program (10%)

- Multiple choice exam on the entire syllabus (50%)

It will consist of a multiple choice exam of 30 questions on the syllabus with four possible options. The correct question adds 1 out of 30, the incorrect question subtracts 0.25 out of 30, the unanswered question neither adds nor subtracts.

Recovery: "The same recovery system will be applied for continuous assessment."

Not assessable: "The non-assessable criteria for continued assessment will be applied."

Review of the final qualification: "The review of the final qualification follows the same procedure as for continuous assessment."

Bibliography

Alonso Lecuit, Javier (2021). "Directiva NIS2: valoraciones y posiciones desde el sector privado", CIBER elcano No. 65 - abril de 2021: Entidades críticas y resileiencia en la UE | Directiva NIS2 (available in http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_

Communications-Electronics Security Group (2011). *Digital Continuity to Support Forensic Readiness.* London: The National Archives.

Doménech Pascual, G. (2006) *Derechos fundamentales y riesgos tecnológicos: el derecho del ciudadano a ser protegido por los poderes públicos*. Madrid: Centro de Estudios Constitucionales.

Fojon, E., Coz J. R., Linares, S., Miralles, R. (sin fechar) *La Ciberseguridad Nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia.* ISMS FORUM: Madrid.

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática*. Madrid: Ra-Ma Editorial.

ISACA (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* ISACA: Rolling Meadows.

ISACA (2014). *Manual de preparación para el examen de* CISM*.* ISACA: Rolling Meadows.

ISACA (2014).*CSX Cybersecurity Fundamentals Study Guide*. ISACA: Rolling Meadows.

ISACA (2014). *Transforming Cybersecurity*. ISACA: Rolling Meadows.

ISACA (2014). *Responding to Targeted Cyberattacks*. ISACA: Rolling Meadows.

ISACA (2016). *Manual de preparación para el examen de* CISA*.* ISACA: Rolling Meadows.

Martín Ávila, A.; Quinto Zumarraga, F. de. (2003). *Manual de seguridad en Internet: soluciones técnicas y jurídicas*. A Coruña: Netbiblo.

Ortiz Plaza, Roberto; Nuñez Baroja, Andrés (2021). "De la concienciación al riesgo humano en la ciberseguridad", Revista SIC: ciberseguridad, seguridad de la información y privacidad, ISSN 1136-0623, Vol. 30, Nº. 143 (Febrero 2021), 2021 (Ejemplar dedicado a: Ciberataques en 2021. Tiempos modernos), págs. 72-73

Piattini Velthuis, M., Peso Navarro, E. del, Peso M. del (2011). *Auditoría de tecnologías y sistemas de información.* Madrid: Ra-Ma Editorial.

Rowlingson R. (2004). "A Ten Step Process for Forensic Readiness". *International Journal of Digital Evidence* (Volume 2, Issue 3)

Velasco Núñez, E. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley (*Nº 8183)

Velasco Núñez, E. (2015). "Los delitos informáticos", *Práctica Penal: cuaderno jurídico* (núm.81) pp. 14 a 28.

On-line resources:

ENISA (Agencia Europea para la ciberseguridad) - https://www.enisa.europa.eu/

Instituto Nacional de Ciberseguridad - www.incibe.es

Agencia Española de Protección de Datos www.agpd.es

SIC - Revista de Ciberseguridad, Seguridad de la Información y Privacidad - www.revistasic.es

Wired - www.wired.com

CIBER Elcano http://www.realinstitutoelcano.org/wps/portal/rielcano_es/publicaciones/ciber-elcano/

Software

The subject doesn't use software.

Language list

Name	Group	Language	Semester	Turn
(TE) Theory	1	Spanish	second semester	afternoon