UAB Universitat Autònoma de Barcelona

Cybersecurity

Code: 107929
ECTS Credits: 6

2025/2026

Degree	Type	Year
Criminology	OP	4

Contact

Name: Jose Cañabate Perez

Email: josep.canabate@uab.cat

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

- Understand the essential principles of cybersecurity, including confidentiality, integrity, availability, authentication, and information traceability.
- Identify the main attack vectors and cyber threats, such as malware, ransomware, denial-of-service attacks (DDoS), phishing, identity theft, and vulnerability exploitation.
- Learn the most common technical and organizational protection measures, including firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus software, encryption, multi-factor authentication, network segmentation, and patch management.
- Understand the cybersecurity risk management cycle, including the identification of critical assets, threat and vulnerability analysis, impact assessment, and control definition.
- Explore the applicable regulatory and legal framework in cybersecurity, such as the Spanish National Security Scheme (ENS), the GDPR (in its information security dimension), and the NIS2 Directive, with practical implications for criminological. investigations.
- Analyze cybersecurity incidents from a criminological perspective, understanding how incidents are planned, executed, and responded to, and the role criminologists can play in such scenarios.
- Become familiar with basic concepts of digital forensics, with attention to the chain of custody, collection of digital evidence, and the initial use of forensic tools.
- Promote a culture of cybersecurity within organizations, understanding human factors, security policies, user training, and the design of prevention strategies.

- Develop a critical view of emerging cybersecurity challenges, such as protection against advanced persistent threats (APT), cyber intelligence, protection of critical infrastructures, or the use of artificial intelligence in attack and defense contexts.

Learning Outcomes

1. CM34 (Competence) Accurately apply prevention models in specific crime situations.
2. CM37 (Competence) To intervene professionally in preventive actions, in conflict resolution or in attention to victims on the basis of scientific evidence and in accordance with the values of pacification and the prevention of new conflicts.
3. CM38 (Competence) Intervene professionally with a gender perspective.
4. KM30 (Knowledge) Identify the legal framework that regulates primary, secondary, and tertiary prevention for the different forms of crime.
5. SM42 (Skill) Apply the most effective forms of prevention to address the specific problem of crime.
6. SM43 (Skill) Identify risk and protective factors in reference to different forms of crime.

Content

The course syllabus covers a broad range of essential concepts and practices in the field of cybersecurity and information technologies. It begins with an introduction to the course methodology, providing students with a solid foundation in core IT and information security concepts. As the course progresses, it explores well-known cybersecurity incidents, various types of cyber threats, and the role of artificial intelligence in detecting and responding to such incidents. Cyber defence strategies and national plans aimed at protecting critical infrastructures are also addressed.

The course also covers national and European regulations related to cybersecurity, as well as cybercrime and the importance of electronic evidence in investigating digital offenses. Furthermore, 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 infrastructure, and the development of business continuity plans to ensure that an organization can continue operating during and after disruptive events. This comprehensive approach equips students to face cybersecurity challenges effectively and competently.

BLOCK 1 - INTRODUCTION AND FUNDAMENTALS

Topic 1. Security fundamentals.
Topic 2. Basic concepts of information security and cybersecurity.
Topic 3. Governance, risk management and regulatory compliance.

BLOCK 2 - THREAT LANDSCAPE

Topic 4. Cyber risk and threats.
Topic 5. Main cyberattacks.
Topic 6. Risk assessment.

BLOCK 3 - ASSET PROTECTION, SECURITY OPERATIONS AND RESPONSE

Topic 7. Asset protection.
Topic 8. Architectures, models and frameworks.
Topic 9. Security controls.
Topic 10. Security operations and response.

BLOCK 4 - CYBERSECURITY REGULATIONS

Topic 11. National and European cybersecurity regulations.

Topic 12. Technological crime.

Topic 13. Forensic readiness and digital forensic investigation.

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Lectures	19.5	0.78	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Seminar	19.5	0.78	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Type: Supervised			
External work for the preparation of activities	5	0.2	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Type: Autonomous			
Reseach on resources and prepare assessable activities.	30	1.2	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Preparing cybersecurity scenarios for classroom-based learning.	35	1.4	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Study	36	1.44	CM34, CM37, CM38, KM30, SM42, SM43, CM34

The course combines theoretical instruction with active collaborative learning methodologies. It is primarily based on three complementary teaching strategies: lecture-based classes, the Jigsaw technique, and problem-based learning (PBL).

First, lecture sessions will introduce the basic principles of each topic, provide structure to the content, and offer a solid theoretical framework. The lecturer will deliver clear and guided explanations of fundamental cybersecurity concepts (confidentiality, integrity, availability, attack vectors, protection systems, risk management, etc.), supported by visual materials and current real-world examples.

Each unit will then be expanded and consolidated through the Jigsaw methodology. This cooperative learning technique involves students working autonomously and collaboratively in small groups. The process is organized in two phases:

- Expert phase: Each group member is assigned a specific subtopic within the broader theme (e.g., one student focuses on phishing, another on ransomware, another on firewalls, etc.). Students with the same subtopic gather in an "expert group" to study it in depth and prepare a clear explanation for their peers.
- Base group phase (puzzle reconstruction): Each student returns to their original group and teaches the others what they have learned. In this way, the group reconstructs the full content through peer-to-peer exchange, promoting shared responsibility, active learning, and critical consolidation of knowledge.

This methodology fosters deep comprehension, development of communication skills, and teamwork, which are essential competencies for the multidisciplinary approach to cybersecurity within criminology.

In addition, the course will incorporate Problem-Based Learning (PBL) as part of its assessment strategy. PBL is an educational methodology that uses real-world problems as a starting point for acquiring and integrating new knowledge. In the context of cybersecurity, this approach is particularly effective due to the dynamic and multifaceted nature of cyber risks.

Students will be presented with a cybersecurity risk scenario, which might involve a ransomware attack on a company, a data breach in a financial institution, or a targeted phishing campaign. The problem must be complex and open-ended, allowing for multiple perspectives and possible solutions.

Students will be organized into small collaborative groups that will work independently to analyze and understand the problem. Collaboration will encourage the exchange of ideas, discussion, and confrontation of different viewpoints, enriching the learning experience.

They will identify what they already know and what they need to learn in order to address the problem. This requires active research, where students gather relevant information on cybersecurity, including attack and defense techniques, applicable regulations, and best practices. Research may involve reviewing academic literature, analyzing previous case studies, and consulting experts in the field.

With the gathered information, students will analyze the problem in depth, identify exploited vulnerabilities and possible consequences, and develop strategies and action plans to mitigate risks and prevent future incidents.

This process requires critical thinking and the application of both technical and practical 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
Advanced and Persistent Threat (APT) analysis activity	30%	1.5	0.06	CM34, CM37, CM38, KM30, SM42, SM43
Class presentation of a risk scenario related to cibersecurity	20%	1.5	0.06	CM34, CM37, CM38, KM30, SM42, SM43
Prova final	50%	2	0.08	CM34, CM37, CM38, KM30, SM42, SM43

Assessment activities can be carried out throughout the course, partly individually and partly in groups. Assessment is continuous and organised according to the training activities described above. The continuous assessment system combines attendance at theoretical/lecture classes, active participation in seminars, completion of assessable activities (with a global weight of 50%) and passing the final exam (with a global weight of 50%). Given that the final exam involves the assessment of knowledge acquired cumulatively through continuous assessment activities, it is an essential requirement to pass the final exam with a 5/10. Evaluation

1. Evaluation model

The evaluation model is continuous and has the educational objective that students and teachers can know the degree of achievement of the competencies in order to guide their training process. Value of each assessment item: individual work (20%); group work (30%); final test (50%).

Attendance at 80% of theoretical classes and seminars is mandatory in order to pass the subject.

2. Assessment items

a. Presentation in class of a risk scenario and written submission of the work (20%).

This activity consists of choosing a risk scenario from those proposed by the teacher, or from those proposed by the students and validated. A risk analysis must be carried out and recommendations proposed. The results of the risk analysis and the proposed recommendations will be discussed in the seminar. Depending on the complexity of the proposed scenario, it will be authorized to be carried out in pairs.

b. Seminar work. Each seminar will be scheduled to analyze a scenario related to a threat. In this sense, each seminar will be dedicated to one of the main current cybersecurity threats (Ramsonware, DDoS, Social Engineering, ATPs, etc.). To prepare for this activity, students will be provided with materials relatedto the subject in advance. At the end of the session, a questionnaire or written test will be given, depending on the activity, to evaluate the acquisition of knowledge. Each activity will be evaluated out of 10, the average of all the notes will have a weighting of 30% on the final note.

c. Questionnaire on the syllabus of 30 questions, 4 options, only one correct, penalty of 0.25 out of 30.

3. Conditions for being evaluated

Students will be assessable provided that they have completed a set of activities whose weight 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 threshold, the subject teacher may consider the student as non-assessable,

4. Requirements to pass the subject and retakes

A minimum grade of 5 is required for all items that make up the assessment. If a student does not pass the assessment part corresponding to individual work, group work or the final exam, they will have the possibility of making up the day established for re -assessment. Individual work and group work are made up through one or more theoretical questions on the contents and subjects worked on in the respective activities. To pass the subject for re-evaluation, it is necessary to have a 5 in all items. If this minimum grade is not obtained in each item, even if the arithmetic mean of the four evaluation items exceeds 5, the final grade in the report will be 4.5.

Considering that this is a second opportunity, the maximum grade for tests and recovered work is 5.

5. Late submissions

They are not accepted, except in cases of force majeure. The student will obtain a 0 for the practice not submitted.

6. Excuses

Excuses to fulfill obligations due to illness or force majeure may be accepted provided that an official certificate is provided. Absences for academic reasons must be previously accepted by the teaching staff.

7. Fraudulent conduct

A student who copies or attempts to copy an exam will receive a 0 on that exam. A student who presents a practice in which there are signs of plagiarism or who cannot justify the arguments for their practice will receive a 0 and will receive a warning.

8. Punctuality

Classes start on time. Entry to class once it has started, or exit before it has ended, is not permitted, except with reasonable justification.

9. Honors Degrees

Students who obtain a grade of 9 or higher in the final grade may obtain the Honors Degree for the course. For this purpose, an evaluation committee will be formed among all the teaching staff of the group, which will evaluate with objective criteria whether any student meets the requirements of excellence required to obtain this qualification. In any case, by academic regulations, only a maximum of 5% of honors degrees can be awarded out of the total number of students enrolled in a course. The evaluation committee with objective criteria may decide not to award any honors degrees.

10. Single assessment

Those students who take part in the single assessment system, after being approved by the faculty, will take the following final tests.
1. Final multiple-choice exam worth 50%. This exam will be conducted on the mandatory course manual " ISACA, (2021), Fundamentals of Cybersecurity, Study Guide, 3rd edition."
2. Completion of a coursework on the risk and threat scenarios that will be proposed on the virtual campus at the beginning of the course with a value of 30%.
3. Oral presentation (lecture) before the teacher on a topic on the subjects that will be proposed at the beginning of the course with a value of 20%.
Not assessable: The same non-assessable criterionwill be applied as for continuous assessment.

11. Use of Artificial Intelligence

Restricted use: "For this subject, the use of Artificial Intelligence (AI) technologies is allowed exclusively in [support tasks, such as bibliographic or information searches, text correction or translations. The student must clearly identify which parts have been generated with this technology, specify the tools used and include a critical reflection on how these have influenced the process and the final result of the activity. The lack of transparency of the use of AI in this assessable activity will be considered a lack of academic honesty and may lead to a partial or total penalty in the grade of the activity, or greater sanctions in serious cases.

Bibliography

Mandatory handbook

ISACA (2021). *Fundamentos de Ciberseguridad. Guía de estudio (3ª ed.). Isaca.*

Othre recommended references

Alonso Lecuit, J. (2021). Directiva NIS2: valoraciones y posiciones desde el sector privado (Documento de trabajo DT6/2021). [Directiva NIS2 at http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_

Communications-Electronics Security Group. (2009). Good Practice Guide18: Forensic Readiness, The National Archives - CESG.

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

Fojón, E., Coz, J.R., & Miralles, R. (2011). *La ciberseguridad nacional, un compromiso de todos: de una cultura reactiva a una de prevención y resiliencia*. ISMS Forum.

Gómez-Vieites, A. (2018). *Enciclopedia de la seguridad informática* (2ª ed.). RA-Ma Editorial.

ISACA. (2017). *CSX Cybersecurity Fundamentals Study Guide* (rev. ed.). Isaca.

ISACA. (2019). COBIT2019: Framework - Governance and Management Objectives. ISACA. Sucesor de COBIT5 (2012), incorpora mejoras para integración y adaptación.

ISACA. (2024). CISM Study Guide 2024-2025: CISM exam prep. Kevin Sirius. ISACA Store.

ISACA. (2024). *Guía actualizada para la certificación CSX Fundamentals*. Isaca.

Ortiz Plaza, R., & Núñez Baroja, A. (2021). De la concienciación al riesgo humano en la ciberseguridad. *Revista SIC: Ciberseguridad, seguridad de la información y privacidad,* 30(143), 72-73.

Piattini, M., del Peso, E., & del Peso, M. (2011). *Auditoría de tecnologías y sistemas de información.* RA-Ma Editorial.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence,* 2(3), 1-28.

Velasco Núñez, E. (2013). Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica. *Diario La Ley*, (8183), 1-9.

Velasco Núñez, E. (2015). Los delitos informáticos. *Práctica Penal: Cuaderno Jurídico*, (81), 14-28.

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

This subject does not require software.

Groups and Languages

Please note that this information is provisional until 30 November 2025. You can check it through this link. To consult the language you will need to enter the CODE of the subject.

Name	Group	Language	Semester	Turn
(SEM30) Seminaris (30 estudiants per grup)	1	Spanish	first semester	afternoon
(TE) Theory	1	Spanish	first semester	afternoon