UAB
Universitat Autònoma de Barcelona

Cybersecurity

Code: 105746
ECTS Credits: 6

2024/2025

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

Contact

Name: Laura Casas Diaz

Email: laura.casas@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.

Objectives and Contextualisation

- Know the basic computer concepts and the functioning of an information system that can affect the security of c
- Know the physical components of a computer system or computer and
- Know the process of auditing information systems.
- Analyze the Government and the Management of Information Technolo
- 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 l

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

SYLLABUS

BLOCK 1

Lesson 1. Introduction and methodology of the subject.

Lesson 2. Basic concepts of information technologies.

Lesson 3. Basic concepts of information security and cybersecurity.

BLOCK 2

Lesson. Known cybersecurity events.

Lesson 5. Cyber threats: definition and types.

Lesson 6. Artificial intelligence and cybersecurity.

Lesson 7. Cyber defense aircraft and national cybersecurity.

BLOCK 3

Lesson 8. State and European regulations on cybersecurity.

Lesson 9. Technological crimes.

Lesson 10. Electronic evidence.

Lesson 11. Forensic Preparation and Digital Forensic Investigation.

BLOCK 4

Lesson 12. Protection of information systems assets.

Lesson 13. Analysis of the main cybersecurity standards.

Lesson 14. Critical infrastructures and Business Continuity Plan.

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
PROFESSORS EXPLAINATION	44	1.76	
Type: Supervised			
SUPPORT TUTORIES FOR FOLLOW-UP OF TEACHING UNITS	2	0.08	
Type: Autonomous			
PRACTICAL CASES PREPARATION	47	1.88	
RISC SCENARIOS STUDY AND RESOLUTION	47	1.88	

Teaching language: Catalan
Lectures in the classroom correspond to the master methodology in which the teacher exposes the subject matter of study, but also the debate and solve problems and situations, the rest corresponds to practical sessions where students work in groups, discussing materials reflective and solving concrete cases. The contents studied in the theoretical sessions (in addition to the compulsory basic bibliography) will be evaluated through written tests. On the other hand, the contents worked on in the practical sessions will also be evaluated through the delivery of the tasks carried out.
Likewise, the students, outside the classroom, contribute to the learning of the subject with the search of documentation of topics related to the subject matter of study. Each student, in addition to his / her attendance in the classroom and the individual study, must carry out a search for documentation and personal consolidation work on what is presented in class

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, 7, 8, 12, 14, 15, 16, 17, 18

GROUP WORK	25%	4	0.16	1, 4, 5, 6, 8, 13, 14, 15, 18
PRACTICAL EVALUATION ACTIVITIES	25%	4	0.16	3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18

The evaluation of the subject is based on gathering different evidence funds for the score on student participation that allows the student to continuously evaluate. We propose, then, a continuous evaluation, measured through the written comments on the works, problems and forums directed by the subject, the delivery of the work worked in group in the practice sessions and written exams.

In order to obtain a positive evaluation, at least all the sections (A, B and C) above 50% must be overcome.

Continuous assessment

a) PRACTICAL WORK (25% OF THE FINAL NOTE)

These practical works will be requested during the semester and will focus on specific aspects that will determine the teaching staff. Each of the works must be evaluated above 40% and must be delivered on the proposed date according to the schedule. The average of practical work will be 20% of the course grade.

The works will be recoverable (in the week dedicated for that purpose at the end of the semester). Students who have not submitted any of the works at the scheduled time will not be evaluated and will not be able to recover them, except forthose who provide a justification (written document).

b) GROUP WORK (25% of the final grade)

The practice will consist of the presentation of a team work related to the topic of the subject, with students having to develop a prevention program aimed at vulnerable groups. Obtain a minimum grade of 3 (out of a total of 10) to be able to add the activity to the continuous evaluation.

Final assessment

A) 2 FINAL EXAMINATION (50% OF THE FINAL NOTE)

The students, individually, will perform a final exam, this will be done on the official date of the calendar established by the EPSI. In this exam you must obtain a minimum qualification of 50%. This exam will consist of a test of thirty questions about the syllabus of the subject and the resolution of a practical case on the analyzed subjects. As for the test type test will consist of thirty questions with multiple choice (four answers only one correct), with a penalty for incorrect question of 0.25 / 30 (or four incorrect ones a correct one).The exams will be recoverable a week dedicated to that effect at the end of the semester. Students not presented will not be evaluated, except for those who provide a justification (written document).

Re-evaluation

In case of not passing the subject according to the aforementioned criteria (continuous evaluation), a recovery test may be done on the date scheduled in the schedule, and it will cover the entire contents of the program.

To participate in the reassessment the students must have been previously evaluated of a set of activities, the weight of which equals a minimum of two-thirds of the total grade of the subject. However, the qualification that will consist of the student's file is a maximum of 5-Approved.

Students who need to change an evaluation date must present the justified request by filling in the document that you will find in the moodle space of Tutorial EPSI.

Plagiarism

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, "in the event that the student makes any irregularity that could lead to a significant

variation in the grade of anevaluation act, it will be graded with a 0 This evaluation act, regardless of the disciplinary process that can be instructed In case of various irregularities occur in the evaluation acts of the same subject, the final grade of this subject will be 0 ".

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

Changing the date of a test or exam

Students who need to change an assessment date must submit the justified request by completing the document that they will find in the moodle space for EPSI Tutoring. Once the document is completed, it must be sent to the teaching staff of the subject and to the coordination of the Degree.

Revision

At the time of carrying out each evaluation activity, the teaching staff will inform the students of the mechanisms for reviewing the qualifications. For single assessment students, the review process will be the same.

Single Assessment

Students who opt for the single assessment will take a final synthesis test of all the content of the subject (50%) and will deliver the subject work (50%).The date for this test and the delivery of the course work will be the same scheduled in the schedule for the last continuous assessment exam.The same recovery system is applied as for the continuous evaluation. The tests/exams may be written and/or oral at the discretion of the faculty.

Evaluation of students in the second or more call

Students who repeat the subject must take the scheduled tests and exams and deliver the subject work on the dates indicated in the Moodle classroom.The tests/exams may be written and/or oral at the discretion of the faculty.

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 en 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

No es necesario programario para esta asignatura.

Language list

Name	Group	Language	Semester	Turn
(TE) Theory	1	Catalan	second semester	afternoon
(TE) Theory	2	Catalan	second semester	afternoon
(TE) Theory	3	Catalan	second semester	afternoon