Universitat Autònoma de Barcelona

Cybersecurity

2019/2020

Code: 105746
ECTS Credits: 6

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

Contact

Name: Josep Cañabate Pérez

Email: Josep.Canabate@uab.cat

Use of Languages

Principal working language:	spanish (spa)
Some groups entirely in English:	No
Some groups entirely in Catalan:	Yes
Some groups entirely in Spanish:	No

Teachers

Xavier Rubiralta Costa

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 I

Competences

- Apply specific software tools to solve problems specific to security.
- Assume the social, ethical and professional responsibility that derives from professional practice.
- 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.

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. Assume the social, ethical and professional responsibility that derives from professional practice.
4. Be able to communicate efficiently in English, both orally and in writing.
5. Carry out scientific thinking and critical reasoning in matters of preventions and security.
6. Evaluate the technical, social and legal impact of new scientific discoveries and new technological developments.
7. Formulate strategies of company management.
8. Generate innovative and competitive proposals in research and in professional activity developing curiosity and creativity.
9. Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
10. Make efficient use of ITC in the communication and transmission of results.
11. Show respect for diversity and the plurality of ideas, people and situations.

Content

SYLLABUS

BLOCK 1

Lesson 1. Introduction to the subject and definition of basic concepts.

Lesson 2. Physical components of a computer system or computer and networks.

Lesson 3. Program of a computer system or computer (operating system, applications, licenses).

Lesson 4. Acquisition, development and implementation of information systems.

Lesson 5. Government and IT Management / COBIT (Control Objectives for Information and Related Technology).

BLOCK 2

Lesson 6. Audit process of information systems.

Lesson 7. Technological delinquency.

Lesson 8. Electronic test.

Lesson 9. Forensic Readiness and Digital Forensic Investigation.

BLOCK 3

Lesson 10. Protection of the assets of information systems.

Lesson 11. Information security management and compliance

Lesson 12. Development of the information security program.

BLOCK 4

Topic 13. Information security incident management.

Topic 14. Analysis of ISO 27000 (Information Security Management System) and NIST 800_53.

Topic 15. Critical Infrastructures and Business Continuity Plan.

BLOCK 5

Lesson 16. Trends: Cloud Computing, BYOD, Big Data, mobility, social networks, Internet of Things, etc.

Lesson 17. Differences and scope of cybersecurity and information security. National Cybersecurity Plans.

Lesson 18. Recommendations and good practices in the management of security in the business and private sphere

Methodology

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

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
PROFESSORS EXPLAINATION	44	1.76	2, 1, 5, 7
Type: Supervised			
SUPPORT TUTORIES FOR FOLLOW-UP OF TEACHING UNITS	2	0.08	2, 1, 7
Type: Autonomous			
PRACTICAL CASES PREPARATION	47	1.88	2, 1, 9, 5, 7
RISC SCENARIOS STUDY AND RESOLUTION	47	1.88	2, 1, 7

Assessment

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.

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 40%. 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).

B) PRACTICAL WORK (20% 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).

C) PRESENTATION OF RISK SCENARIOS RELATED TO THE INFORMATION SYSTEM (20% OF THE FINAL NOTE) During the semester will be proposed problems in class that must be solved individually and present the solution in writing. The delivery of the corresponding reports will mean their evaluation and the average of both will represent 10% of the final grade. These tasks can also be individual reflections, exercises, case presentations, etc. Given their nature, they are not susceptible to recovery at the end of the semester D) PARTICIPATION IN THE FORUMS AND IN CLASS (10% OF THE FINAL NOTE) During the semester debate / opinion topics will be proposed both in class and in the fora provided on the web of the subject (MOODLE). The objective is for students to discuss among themselves in a public and moderate way with the teachers about these issues. The evaluation will represent 10% of the final grade. Given their nature, they are not susceptible to recovery at the end of the semester

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 an evaluation 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.

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes

FINAL EXAM	40%	2	0.08	2, 1, 9, 5, 10, 7, 8, 11, 6
PARTICIPATE IN FORUMS AND CLASS	10%	2	0.08	2, 1, 9, 5, 10, 7, 8, 11, 6
PRACTICAL EVALUATION ACTIVITIES	30%	3	0.12	2, 3, 4, 9, 5, 10, 8, 11, 6
PRESENTATION OF RISK SCENARIOS RELATED WITH INFORMATION SYSTEMS	20%	3	0.12	2, 1, 3, 9, 5, 6

Bibliography

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.

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.