Universitat Autònoma de Barcelona

2021/2022

Cybersecurity

Code: 105779
ECTS Credits: 6

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

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

Contact

Name: Josep Cañabate Pérez
Email: Josep.Canabate@uab.cat

Use of Languages

Principal working language: catalan (cat)
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 l

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

Taking into account that the modality of the class is Online, with the aim of achieving the learning objectives described in this Guide, we will develop a methodology that combines the individual study from the Manual, and the readings that will be presented in each topic, in addition of some documentaries.

Each topic will have a forum of doubts, and a Forum of "Contributions" will be established where the students can introduce readings, articles, webs, documentaries, and all kinds 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 in an autonomous way (documents, readings, videos, etc.) and the forums and Online sessions will be devoted to deepening on the topics discussed as well as solving possible doubts

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.

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Videoconference with the active participation of the students	12	0.48	2, 1, 7
Type: Supervised			
RESOLUTION OF DOUBTS ON SUBJECT AND PRACTICES	6	0.24	2, 1, 7
Type: Autonomous			
PRACTICAL CASES PREPARATION	60	2.4	2, 1, 7

RISC SCENARIOS STUDY AND RESOLUTION	60	2.4	2, 1, 7	

Assessment

The evaluation of the subject will be done through: Continuous evaluation (30% of the overall score): To pass this section each student must make a quality participation, in each discussion forum (there will be 5 forums, divided by thematic areas). Therefore, each student expects a minimum of 5 quality interventions (that is, providing notions and comments that go beyond what is included in the manuals including bibliography and references) At the same time, each student must enter a minimum of 4 contributions in the section dedicated to these effects of the subject. Each intervention in the forum and each contribution represent 10% of the evaluation of this section, the rating will be established based on criteria of quality, originality, coherence and interaction, if possible. The interventions or extra contributions will be evaluated positively, but we remember that you can never exceed the 3 points that this section has in relation to the overall score. Individual work consisting of the analysis of a technological risk scenario (15% of the overall score) The student will be presented with a risk scenario for IT (Information Technologies) in which the impact for the security of the information will have to be analyzed (integrity, confidentiality and availability) Individual work consisting in the elaboration of good IT usage practices in a complex organization (15% of the overall score) The student must perform good IT practices for an organization that has a complex structure, which can compromise the security of information. Final examination of the subject (40% of the overall grade) The exam will consist of test-type questions and to develop and will be based on the contents of the manual's agenda plus the mandatory readings.

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 thereassessment 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, 7, 8, 11, 6
PARTICIPATE IN FORUMS AND CLASS	30%	5	0.2	2, 1, 7
PRACTICAL EVALUATION ACTIVITIES	30%	5	0.2	2, 1, 3, 4, 9, 5, 10, 7, 8, 11, 6

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.