Security Technology

Code: 101867
ECTS Credits: 6

2025/2026

Degree	Type	Year
Prevention and Integral Safety and Security	OB	1

Contact

Name: Jose Martinez Martinez

Email: jose.martinez.martinez@uab.cat

Teaching groups languages

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

Prerequisites

This subject doesn´t have año pre-requierments.

Objectives and Contextualisation

Differentiate and define security systems, such as electronic, physical and human elements, in latter with special attention to learning men and women with respect and ecuality without prejudice to gender, installed and deployed in facility to protect people and property before that can affect them.

Knowing the regulatory framework, que regula las tecnologías de seguridad, y sus relaciones con los sectores de seguridad pública y privada.

Know the different electronic security devices that are marketed, installed, and maintained for the design of comprehensive security plans.

Na jiné straně, know existují zdravotnické systémy systémů a jak jsou kombinovány s elektronickými systémy zabezpečení k minimizaci různých rizik k tomu, aby instalace byly upevněny, aby mohly být vystaveny.

Competences

- Act with ethical responsibility and respect for fundamental rights and duties, diversity and democratic values.
- Carry out analyses of preventative measures in the area of security.
- Have a general understanding of basic knowledge in the area of prevention and integral safety and security.
- Identify the resources necessary to respond to management needs for prevention and integral security.
- Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
- Make changes to methods and processes in the area of knowledge in order to provide innovative responses to society's needs and demands.
- Make efficient use of ITC in the communication and transmission of results.

- Plan and coordinate the resources of the three large subsystems that interact in questions of security: people, technology and infrastructures.
- Respond to problems applying knowledge to practice.
- 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.
- Take account of social, economic and environmental impacts when operating within one's own area of knowledge.
- Take sex- or gender-based inequalities into consideration when operating within one's own area of knowledge.
- Use the capacity for analysis and synthesis to solve problems.
- Work and learn autonomously.
- Work in institutional and interprofessional networks.

Learning Outcomes

1. Analyse specific risks and understand the prevention mechanisms.
2. Analyse the preventative interventions in matters of security, environment, quality and social corporate responsibility and identify the inherent risk factors.
3. Analyse the sex- or gender-based inequalities and the gender biases present in one's own area of knowledge.
4. Analyse the situation and identify the points that are best.
5. Coordinate the resources of the three main subsystems of the prevention and integral security sector: people, technology and infrastructures.
6. Critically analyse the principles, values and procedures that govern professional practice.
7. Diagnose the situation of integral security in companies and organisations.
8. Draw up management proposals for prevention and security in an organisation.
9. Identify, develop or acquire and maintain the main resources necessary to respond to tactical and operational needs inherent in the prevention and security sector.
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 new methods or well-founded alternative solutions.
13. Propose projects and actions that incorporate the gender perspective.
14. Propose viable projects and actions that promote social, economic and environmental benefits.
15. Respond to problems applying knowledge to practice.
16. 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.
17. 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.
18. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
19. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
20. 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.
21. Take a preventative view in the area of security.
22. Use the capacity for analysis and synthesis to solve problems.
23. Work and learn autonomously.

24. Work in institutional and interprofessional networks.

Content

Basic framework of security technologies.

- Physical security systems.
  - Perimeter.
  - Exteriores.
  - Interiores.
- Electronic security systems.
  - Acceso control.
  - Intrusión.
  - Video sobrevivencia.
  - CCTV.
- Security facilities.
  - Regulaciones.
  - Tecnologías.
  - Costas.
- Fire protection system.
  - Detección.
  - Extinción.
  - Alert and evacuation.
- Future of security technologies.
  - Drones
  - Robóticos.
  - Cybersecurity.
  - Artificial Intelligence
- Weapons, explosivas and armor.
  - Weapons Regulations.
  - Explosivas Regulations.
  - Shielding Technology.
  - Technologies applicable in conflicts.
- Technology of private detectives.
  - Technologies applicable to private investigation.
  - Security audits.
  - Transmisiones, image and sound.

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
40 h Theoretical and practical classes + 4 Evaluation	44	1.76	
Type: Supervised			
Work planning Readings, reflection on the subjects. Preparation of individual works. PEC, and final test.	12	0.48	
Type: Autonomous			
Individual and group work (search for material, discussion, preparation and presentation).	94	3.76	

Teaching language: Spanish

Theoretical classes.

- The theoretical classes will consist of exposing the subjects of the subject (magisterial exhibition with audiovisual support or Power Poit), resolution of the exercises and resolution of doubts, as well as cooperative learning and the case method.

• Practical classes and resolution of practical cases.

- The practical classes are destined to the accomplishment or resolution of the exercises, exhibition of works and presentations, individual or in group. They can also be used for the visualization of audiovisual materials.

• Reading and seminars:

- The readings will be accompanied by audiovisual media.
- The seminars will be based on the presentation of real cases and discussion of the technological and human resources deployed for the implementation of prevention and security plans.

• Debates and discussion forums.
• Oral presentation of work in the classroom.
• Completion of works / projects / reports.
• Study for the exam. Final test (one first part type test, and the second one case to be developed).

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
Examination of the topic	20%	0	0	1, 4, 21, 5, 7, 8, 2, 9, 12, 14, 20, 19, 18, 16, 17
Final exam	30%	0	0	6, 3, 1, 4, 21, 5, 7, 8, 2, 9, 12, 14, 20, 19, 18, 16, 17, 23, 22
PEC	50%	0	0	1, 4, 21, 10, 7, 15, 8, 2, 11, 12, 13, 14, 20, 19, 18, 16, 17, 24

The assessment will be based on continuous evaluation criteria, which makes attendance mandatory and allows us to measure the degree of specific competencies of the program achieved by the student.

The values of each item for evaluation are listed in the following table. All items must be passed with a minimum grade of 3.5 in order to be counted toward the evaluation.

Midterm Exam. Total value: 20%.
Exams may be, at the professor's discretion, either oral or written. Written exams may include multiple choice questions, short-answer questions, essay questions, or a combination of these formats. The exam must be passed with a minimum grade of 3.5 to count toward the continuous evaluation.

PEC (Continuous Evaluation Tests). Five PECs, each worth 10% (0.6% for the written work, 0.4% for the oral presentation). Total value: 50%.
Each PEC must be passed with a minimum grade of 3.5 to count toward the continuous evaluation. Any PEC found to contain plagiarism, excessive similarity, or improper citation will receive a grade of 0. PECs submitted after the deadline will be graded as "0". PECs may consist of a written assignment or a test on the teaching materials, readings, etc., as specified for each.

Final Exam. Total value: 30%.
Exams may be, at the professor's discretion, either oral or written. Written exams may include multiple choice questions, short-answer questions, essay questions, or a combination of these formats. The exam must be passed with a minimum grade of 3.5 to count toward the continuous evaluation. If the student does not achieve a 3.5, they will proceed directly to the resit exam.

To be eligible for continuous evaluation, students must take all the assessable tests (PECs, midterm exam, and final exam).
Each of these must be passed with a minimum grade of 3.5 to be included in the continuous evaluation. Failure to take all the assessments or to achieveat least a 3.5 in each will result in the student going directly to the resit exam.

PECs and assignments must be properly cited in accordance with the relevant guidelines.
No work will be accepted without proper citation. Citation Guide

If the student does not pass the course according to the criteria outlined above (continuous evaluation), a resit exam may be taken on the scheduled date.
This exam will cover a summary of the entire course content.

To be eligible for the resit exam, the student must have been previously assessed in a set of activities that together constitute at least two-thirds of the total course grade.
However, the maximum grade that can be recorded in the student's transcript for the resit exam is 5 (pass).

Students who need to reschedule an assessment date must submit a request using the form available in the EPSI Tutoring Moodle space.

Without prejudice to other appropriate disciplinary actions, and in accordance with current academic regulations:
"In the event that a student commits any irregularity that may significantly affect the grading of an assessment, the act will be graded with a 0, regardless of any disciplinary process that may be initiated. If multiple irregularities occur in assessments for the same subject, the final grade for that subject will be 0."

Tests and exams may be written and/or oral, at the discretion of the instructor.

PLAGIARISM:
If there are indications during grading that an activity or assignment contains responses generated with the help of artificial intelligence, the instructor may request a personal interview to verify authorship of the text.

Single Assessment:
Students opting for the single assessment will complete a final synthesis test covering all course content (50%) and submit the course assignment (50%).
The date for this test and the assignment submission will coincide with the last scheduled exam for continuous evaluation.
The same resit system as for continuous evaluation will apply.

Evaluation of students in a second or subsequent attempt:
Students repeating the course must complete all scheduled tests and exams and submit all required assignments by the indicated Moodle deadlines.

Not Assessable (No Show):
If the student has not been assessed on at least two-thirds of the course due to not participating in assessments or submitting assignments, they will receive the grade "Not Assessable" according to EPSI Evaluation Regulations.
This means the student may not take the final resit exam.

Resit Exam:
A student who does not pass the course (fails to reach a total of 5 out of 10), according to the criteria described above, may take a final resit exam only if they have been assessed in a set of activities equivalent to at least two-thirds of the total course grade.
If not, they will receive a "Not Presented" grade and will not be eligible for the resit exam.
This exam will re-evaluate the entire course content.
If the exam is passed, the final grade for the course will be a maximum of 5, regardless of the score obtained.

Change of Assessment or Exam Date:
Students who need to change the date of an assessment must submit a request using the form found in the EPSI Tutoring Moodle space.
Once completed, the form must be sent to the course instructor and the Degree Coordinator.

Review:
To request a review of an assessment, students must email the instructor, who will provide the procedure for review.
The review process will be the same for single-assessment students.

USE OF AI
In this course, the use of Artificial Intelligence (AI) tools is allowed as an integral part of the development of the assignment, provided that the final results reflect a significant contribution from the student in terms of personal analysis and reflection on the topics covered. The student must identify which parts of the work have been completed using AI and which have not, as well as the name of the AI tool used. Lack of transparency in the use of AI is considered a breach of academic integrity and may result in a penalty in the activity grade, or more serious sanctions in severe cases.

Bibliography

Aguado, V. (2007). Derecho de la Seguridad Pública y Privada. Navarra: Editorial Aranzadi.

Arzoz, X. (2010) Videovigilancia, seguridad ciudadana y derechos fundamentales. Navarra: Editorial Thomson Reuters.

Bentham, J. (1989). El Panóptico. Madrid: Editorial Endymion.

BUBL, M. (2017) La ciencia secreta de la cerrajería. Austria: BUBL.

Calero, LM (2005). La seguridad privada en España: actores, especificaciones y sume Planificación. Madrid: Editorial Universitas Internacional. SL

Desdentado, A., Muñoz, B. (2012). Control informático, videovigilancia y protección de datos en el trabajo. Valladolid: Editorial Lex Nova.

Díaz, F. (2013). Diccionario LID. Inteligencia y Seguridad. Madrid: Editorial Empresarial.

Hierro, JM (2015). Manual operativo del director y jefe de seguridad. Madrid: Editorial Auto-Editor.

Foucault, M. (2012). Vigilar y Castigar. Madrid: Editorial Biblioteca Nueva,SL

Freedman, L. (2019). La Guerra del Futuro. Barcelona: Editorial Crítica.

Gómez, R. (2014). Diccionario terminológico para la seguridad privada. Madrid: Editorial Tecnos.

Gómez, R. (2014). Diccionario terminológico de la seguridad privada. Madrid: Editorial Tecnos. SL

González, J. (2012) Inteligencia. Valencia: Tirant lo Blanch

González, M. (2011). Guía visual para falsear Cerraduras(3.ed.). Illinois: Standard Publicaciones, Inc.

Innerarity, D., Solana, J. (2011). La humanidad amenazada: gobernar los Riesgos globales. Barcelona: Editorial Paidós.

Lamas, L. (2019) Apertura de puertas, técnicas y trucos. (4.ed.). Madrid: Nivel Medio.

Lyon, D. (1995). El ojo electrónico. El auge de la sociedad de vigilancia. Madrid: Editorial Alianza.

Macías Fernández. D. (2014). David contra Goliat. Guerra y Asimetría en la edad contemporánea. Madrid. Editorial Instituto Universitario Gutiérrez Mellado.

Martínez, R. (2002). Armas: ¿Libertad americana o Prevención europea? Barcelona: Editorial Ariel.

Martínez, R., Rodríguez, J. (2018). Inteligencia artificial y armas letales Autónomas. Gijón: Ediciones Trea.

Martínez. E. (2008). Los soldados del Rey. Madrid. Editorial Andújar.

McLaughlin, E., Muncie, J. (2014). Diccionario de criminología. Barcelona: Editorial Gedisa, SA

Miró, F. (2012). El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Barcelona: Editorial Marcial Pons.

Montoya, R. (2014). Drones. La muerte por control remoto. Madrid: Editorial Akal.

Muñoz Bolaños. R. (2001). La campaña de 1909. Las campanas de Marruecos, 1909-1927. Madrid.

Perales, T. (2014). Instalaciones de sonido, imagen y seguridad electrónica. Madrid: Editorial Marcombo.

Poveda, MA, Torres, B. (2015). Dirección y gestión de la seguridad privada. Madrid: Editorial Fragua.

Puell de la Villa. F. (2007). La guerra con armas de fuego. M. Artola (ed.). Historia de Europa. Madrid. Editorial Espasa Calpe. Vol. II.

Quedada. F. (2007). La Guerra con arma blanca . M. Artola (ed.) Historia de Europa. Madrid. Editorial. Espasa Calpe. Vol. I.

Ridaura, M.ª J. (2015). Seguridad Privada y Derechos Fundamentales (La nueva Ley 5/2014, de abril, de Seguridad Privada). Valencia: Editorial Tirant lo Blanch.

Rodríguez, A (2005). 250 modelos de cerrajería. Barcelona: Ediciones CEAC.

Rodríguez, F. (2018). Circuito cerrado de televisión y seguridad electrónica. (ed.2) Madrid. Editorial Paraninfos.

Somoza, O. (2004). La muerte violenta. Inspección ocular y cuerpo del delito. Madrid: Editorial la Ley.

Teijeiro de la Rosa. JM. (2016). Dinero y ejercitos en España. De la Antigüedad al siglo XXI. Madrid.

Torrente, D. (2015). Análisis de la seguridad privada. Barcelona: Editorial UOC.

Software

This subject will use the basic software of the office 365 package.

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
(TE) Theory	1	Spanish	second semester	afternoon
(TE) Theory	2	Spanish	second semester	afternoon