

Degree programme	Type	Course
Prevention and Integral Safety and Security	OB	1

Contact lecturer

Name : Jose Martinez Martinez

Email : jose.martinez.martinez@uab.cat

Prerequisites

This subject doesn't have any pre-requirements.

Group languages

You can consult this information at the [end](#) of the document.

Objectives

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 equality 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 minimalizaci různých rizik k tomu, aby instalace byly upevněny, aby mohly být vystaveny.

Learning outcomes

1. Coordinate the resources of the three main subsystems of the prevention and integral security sector: people, technology and infrastructures.
2. Use the capacity for analysis and synthesis to solve problems.
3. Respond to problems applying knowledge to practice.
4. Work in institutional and interprofessional networks.
5. 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.
6. 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.
7. 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.
8. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
9. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
10. Propose new methods or well-founded alternative solutions.

11. Critically analyse the principles, values and procedures that govern professional practice.
12. Analyse the sex- or gender-based inequalities and the gender biases present in one's own area of knowledge.
13. Propose projects and actions that incorporate the gender perspective.
14. Propose viable projects and actions that promote social, economic and environmental benefits.
15. Draw up management proposals for prevention and security in an organisation.
16. Identify, develop or acquire and maintain the main resources necessary to respond to tactical and operational needs inherent in the prevention and security sector.
17. Analyse the preventative interventions in matters of security, environment, quality and social corporate responsibility and identify the inherent risk factors.
18. Analyse specific risks and understand the prevention mechanisms.
19. Take a preventative view in the area of security.
20. Diagnose the situation of integral security in companies and organisations.
21. Work and learn autonomously.
22. Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
23. Make efficient use of ITC in the communication and transmission of results.
24. Analyse the situation and identify the points that are best.

Contents

Basic framework of security technologies.

Physical security systems.

- Perimeter.
- Exterior.
- Interior.

Electronic security systems.

- Access control.
- Intrusion.

- Video surveillance. CCTV.
- Fire protection systems.

Security installations.

- Regulations.
- Technologies.
- Costs.

Future of security technologies.

- Drones: ground, aerial, and underwater.
- Robotics.
- Security technologies applicable to conflicts.

Weapons, explosives.

- Weapons regulations.
- Explosives regulations.

- Weapons and explosives trafficking.
- Armor.

Technology for private detectives.

- Technologies applicable to private investigation.
- Private detectives and security audits.
- Communications, image, and sound in private investigation.
- Open-source intelligence (OSINT).

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Work planning Readings, reflection on the subjects. Preparation of individual works. PEC, and final test.	30	1.2	3, 4, 5, 6, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
Theoretical and practical classes + 4 Evaluation	45	1.8	1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 18, 19, 20, 21, 22
Individual and group work (search for material, discussion, preparation and presentation).	75	3	3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 18, 19, 21

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

Continuous assessment activities

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

It will be based on criteria founded on continuous assessment, which makes attendance mandatory and will allow us to measure the degree to which the student has achieved the specific competencies of the programme.

Partial examination. Total value: 20%.

Examinations may be, at the teacher's discretion, either oral or written. Written examinations may consist of multiple-choice questions, short-answer questions, long-answer essay questions, or a combination of all the previously described types. The examination grade must be at least 3.5 in order to count towards the continuous assessment.

Continuous assessment activities. 3 continuous assessment tests. Each with a value of 16.6%. Total value: 50%.

The grade for each continuous assessment activity must exceed 3.5 in order to count towards the continuous assessment. In any continuous assessment activity where plagiarism, similarity, or incorrect citation is detected, the grade will be 0. Continuous assessment activities submitted after the deadline will be graded as "0". These activities may consist of an assignment or an examination based on the teaching materials, readings, etc., proposed for each of them.

Final examination. Total value: 30%.

Examinations may be, at the teacher's discretion, either oral or written. Written examinations may consist of multiple-choice questions, short-answer questions, long-answer essay questions, or a combination of all the previously described types. The examination grade must be at least 3.5 in order to count towards the continuous assessment. If the student does not achieve a minimum grade of 3.5, they will proceed directly to the resit examination.

For the continuous assessment to be counted, students must sit 3 of the 5 assessable activities: continuous assessment activities, partial examination, and final examination. In addition, the grades obtained in the examinations and continuous assessment activities must be at least 3.5 in order to count towards the continuous assessment. If the student does not sit all the assessment activities or does not achieve a minimum grade of 3.5 in each of them, they will proceed directly to the resit examination.

Continuous assessment activities and assignments must be cited in accordance with the applicable regulations. No assignment will be accepted without proper citation.

https://ddd.uab.cat/pub/recdoc/2016/145881/citrefapa_a2016.pdf

If the student does not pass the subject in accordance with the aforementioned criteria -continuous assessment-, they may take a resit examination on the date scheduled in the timetable. This examination will cover a summary of all the contents of the programme.

In order to participate in the resit examination, students must have previously been assessed in a set of activities whose weight is equivalent to at least two thirds of the total grade for the subject. However, the grade recorded in the student's academic transcript will be a maximum of 5 -pass-.

Students who need to change the date of an assessment activity must submit a request by completing the document available in the EPSI Tutoring Moodle space.

Without prejudice to any other disciplinary measures deemed appropriate, and in accordance with current academic regulations, "if a student commits any irregularity that may lead to a significant variation in the grade of an assessment act, that assessment act will be graded as 0, regardless of any disciplinary proceedings that may be initiated. If several irregularities occur in the assessment acts of the same subject, the final grade for that subject will be '0'."

Tests or examinations may be written and/or oral, at the discretion of the teaching staff.

PLAGIARISM:

If the student commits any type of irregularity that may lead to a significant variation in the grade of an assessment act, that act will be graded as 0, regardless of any disciplinary proceedings that may arise from it. If several irregularities are verified in the assessment acts of the same subject, the final grade for that subject will be 0. Activities in which fraud or misuse of AI has been detected cannot be recovered.

If, during correction, there are indications that an activity or assignment has been completed using AI-assisted responses, the teacher may complement the activity with a personal interview in order to verify authorship of the text.

Single assessment

Students who choose single assessment will complete 3 assessment activities:

1. A final synthesis examination covering all the contents of the subject, worth 50%.
2. Submission of the subject assignment, worth 40%.
3. Oral presentation of the subject assignment, worth 10%.

The date for this examination and for the submission of the subject assignment will be the same as the date scheduled in the timetable for the last continuous assessment examination.

The same resit system as for continuous assessment will apply.

In order to be eligible for the resit examination, the student must have submitted all the required assessment activities.

Attendance: choosing single assessment does not exempt the student from attending class.

Assessment of students in their second enrolment or subsequent enrolments

Students who are repeating the subject must complete all the scheduled tests and examinations and submit the subject assignments on the dates indicated in the Moodle classroom.

Not assessable

If the student commits any type of irregularity that may lead to a significant variation in the grade of an assessment act, that act will be graded as 0, regardless of any disciplinary proceedings that may arise from it. If several irregularities are verified in the assessment acts of the same subject, the final grade for that subject will be 0.

Activities in which fraud or misuse of AI has been detected cannot be recovered.

The student will receive a grade of "not assessable" whenever they have not submitted more than 30% of the assessment activities.

Resit examination

A student who does not pass the subject, that is, who does not achieve a total grade of 5 out of 10, in accordance with the criteria established in the two previous sections, may sit a final examination provided that the student has been assessed in a set of activities whose weight is equivalent to at least two thirds of the total grade for the subject.

If the student has not been assessed for these two thirds because they did not sit the assessment activities, they will receive a grade of "not presented", without the possibility of taking the final resit examination.

In this examination, all the contents of the subject will be assessed again. If the final examination is passed, the subject will be passed with a maximum grade of 5, regardless of the grade obtained in the examination.

In order to be eligible for the resit examination, the student must have been assessed for two thirds of the total assessment.

Change of date of a test or examination

Students who need to change the date of an assessment activity must submit a request by completing the document available in the EPSI Tutoring Moodle space.

Once the document has been completed, it must be sent to the teaching staff of the subject and to the degree coordination office.

Review

At the time each assessment activity is carried out, the teacher will inform students, via Moodle, of the procedure and the date for reviewing the grades.

The ordinary procedure will be as follows: in order to review the assessment activity, the student must send an email to the teacher, who will indicate the review mechanism.

For students under single assessment, the review process will be the same.

The grades for each test will be communicated within a maximum of 10 calendar days from the date of the test, except where unforeseen circumstances prevent the normal development of the subject. In such cases, the teaching staff may modify both the methodology and the assessment of the subject, as well as the deadlines for publishing grades.

USE OF AI

Restricted use:

"For this subject, the use of Artificial Intelligence (AI) technologies is permitted exclusively for support tasks, such as bibliographic or information searches, text correction, or translations [... others? ...], [activities *xxx] [other specific situations where deemed appropriate]. The student must clearly identify which parts have been generated using this technology, specify the tools used, and include a critical reflection on how these tools have influenced the process and the final outcome of the activity. Lack of transparency regarding the use of AI in this assessable activity will be considered a breach of academic honesty and may result in a partial or total penalty in the grade for the activity, or more serious sanctions in severe cases."

Puedo prepararlo también en una versión más formal para guía docente universitaria en inglés académico.

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 ejércitos 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 and the CAD program, in the free version nanoCAD v.5.

Course groups and languages

The information provided is provisional until November 30. After this

date, you will be able to consult the language of each group through this [link](#). To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(TE) Theory	1	Spanish	second semester	afternoon
(TE) Theory	2	Spanish	second semester	afternoon