

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-requirments.

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 the latter with special attention to learning men and women with respect and equality without prejudice to gender, installed and deployed in a facility to protect people and property before the different risks that can affect them.

Knowing the regulatory framework that regulates security technologies, and their relationship with the sectors of public security and private security.

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

On the other hand, to know the existing physical security systems and how they are combined with electronic security systems to minimize the different risks to which the installation we wish to protect may be exposed.

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.

The 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 used by private detectives.

- Technologies applicable to private investigation.
- Private detectives and security audits.
- Transmissions, 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. Continuous tests, and final test.	24	0.96	
Classes with TIC support	12	0.48	
Individual and group work (search for material, discussion, preparation and presentation).	110	4.4	
Evaluation	4	0.16	

- Classes with TIC support. Resolution of doubts and questions. Job tracking
- Resolution of exercises and practices: individual realization of works and practical cases, with ICT support.
- Personal study: Consolidation of theoretical and practical knowledge.
- The tutorials with the faculty will be arranged by email.

The language in which classes are taught is: Spanish.

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
Final exam.	50%	0	0	1, 5, 6, 7, 9, 13, 14, 15, 23
PEC 3	16.6%	0	0	2, 3, 4, 6, 9, 10, 11, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24
PEC 2	16.6%	0	0	2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 19, 21, 23, 24
PEC 1	16.6%	0	0	2, 3, 4, 6, 8, 9, 12, 13, 17, 18, 19, 20, 21, 23, 24

The continuous assessment tests will be theoretical/practical in nature or multiple-choice (PEC 1, PEC 2 and PEC 3) and will be completed individually.

For continuous assessment to be valid, the student must complete all PECs. If any PEC is not submitted, the continuous assessment will be cancelled and the student will move directly to the resit examination.

All assignments must be cited in accordance with the corresponding regulations. No assignment will be accepted without proper citation.

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

Cheating in exams or plagiarism.

If, during an examination, students are found to be cheating, they will automatically fail and will not be allowed to access the resit examination.

In the event of plagiarism in the drafting of assignments (PECs), each case will be assessed individually and, in extreme cases, the option of direct failure without the possibility of resit may be considered.

If the student does not pass the subject in accordance with the criteria mentioned above, a resit examination may be taken on the date scheduled in the timetable. This examination will cover the entire content of the programme.

In order to take part in the resit examination, students must have previously been assessed in a set of activities whose weighting 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, "in the event that a student commits any irregularity that may lead to a significant variation in the grade of an assessment activity, this assessment activity will be graded with a 0, regardless of any disciplinary proceedings that may be initiated. If several irregularities occur in assessment activities within the same subject, the final grade for that subject will be 0."

If the student is repeating the subject, they must complete all the tests specified in this teaching guide without exception. Assignments previously submitted by the student in earlier academic years will not be accepted.

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

PLAGIARISM:

If, during the correction process, there are indications that an activity or assignment has been completed using answers assisted by artificial intelligence, the lecturer may supplement the activity with a personal interview in order to verify authorship of the text.

Single Assessment

Students who opt for single assessment will take a final synthesis test covering all the subject content (50%) and will submit the subject assignment (50%).

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

The same resit system as for continuous assessment will apply.

Resit Examination

Students who do not pass the subject, that is, who do 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 they have been assessed in a set of activities whose weighting is equivalent to at least two thirds of the total grade for the subject.

If the student has not been assessed in these two thirds because they did not attend the tests, they will receive a grade of Not Presented, without the possibility of sitting the final resit examination.

In this examination, the full content 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.

The final grade will be published at least 72 hours before the resit exam.

Change of Date for 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.

Not assessed

Students will obtain a not assessed/not submitted course grade unless they have submitted more than 30 % of the assessment items.

Review

To request a review of an assessment activity, the student must send an email to the lecturer, who will indicate

the review procedure.

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

If unforeseen circumstances arise that prevent the normal development of the subject, the teaching staff may modify both the methodology and the assessment system of the subject.

USE OF AI

In this subject, the use of Artificial Intelligence (AI) techniques is permitted as an integral part of the development of the assignment, provided that the final results reflect a significant contribution by the student in the analysis and personal reflection on the topics addressed.

The student must identify which part of the assignment has been completed using AI and which part has not, as well as the name of the AI application used.

A lack of transparency in the use of AI will be considered a breach of academic honesty and may result in a penalty in the grade for the activity, or more serious sanctions in cases of greater severity.

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.

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

Calero, L.M. (2005). *La seguridad privada en España: actores, especificaciones y su planificación*. Madrid: Editorial Universitas Internacional. S.L.

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.

Ferro, J.M. (2015). *Manual operativo del director y jefe de seguridad*. Madrid: Editorial Auto-Editor.

Foucault, M. (2012). *Vigilar y Castigar*. Madrid: Editorial Biblioteca Nueva, S.L.

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. S.L.

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, S.A.
- 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 campañas de Marruecos, 1909-1927*. Madrid.
- Perales, T. (2014). *Instalaciones de sonido, imagen y seguridad electrónica*. Madrid: Editorial Marcombo.
- Poveda, M.A., 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.

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