Ficha de Unidade Curricular A3ES
Cibersegurança
Mestrado em Engenharia Informática e de Computadores
2025-26

1. Designação da unidade curricular

[4112] Cibersegurança / Cybersecurity

2. Sigla da área científica em que se insere	IC, n/d
3. Duração	Unidade Curricular Semestral
4. Horas de trabalho	162h 00m
5. Horas de contacto	Total: 60h 00m, h 00m das quais T: 46h 00m, h 00m | TP: 14h 00m, h 00m
6. % Horas de contacto a distância	Sem horas de contacto à distância
7. ECTS	6
8. Docente responsável e respetiva carga letiva na Unidade Curricular	[1551] José Manuel de Campos Lages Garcia Simão | Horas Previstas: 120 horas
9. Outros docentes e respetivas cargas letivas na unidade curricular	[1521] Nuno Miguel Machado Cruz | Horas Previstas: 120 horas [1743] Tiago Miguel Braga da Silva Dias | Horas Previstas: 120 horas [1917] Lucía Fernández Suárez | Horas Previstas: 120 horas

10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes).

Os estudantes que terminam com sucesso esta unidade curricular serão capazes de:
1. Enumerar os diferentes mecanismos para proteção de informação e principais objetivos (confidencialidade, integridade dos dados) e problemas (tamanho do espaço de chaves, geração de chaves) da criptografia moderna.
2. Descrever algumas das principais áreas de aplicação da teoria de números, tais como, criptografia de chave pública, cifra por blocos, funções de hash e infraestruturas de blockchain.
3. Identificar vulnerabilidades existentes no software e usar técnicas adequadas à sua mitigação ou correção
4. Explicar os mecanismos criptográficos disponíveis nas plataformas de hardware modernas.
5. Identificar os diferentes sistemas de deteção e prevenção de quebras de segurança.
6. Identificar os diferentes quadros normativos existentes.

10. Intended Learning objectives and their compatibility with the teaching method (knowledge, skills and competences by the students).

Students who successfully complete this course will be able to:
1. List the different mechanisms for information protection and the main objectives (confidentiality, data integrity) and problems (size of the key space, key generation) of modern cryptography.
2. Describe some of the main areas of application of number theory, such as public key cryptography, block encryption, hash functions and blockchain infrastructures.
3. Identify existing vulnerabilities in software and use appropriate techniques to mitigate or correct them
4. Explain the cryptographic mechanisms available on modern hardware platforms.
5. Identify the different systems for detecting and preventing security breaches.
6. Identify the different existing regulatory frameworks.

11. Conteúdos programáticos

I. Mecanismos para proteção da informação

- Introdução à criptografia e à cripto-análise.
- Conceitos de aritmética modular, corpos finitos e curvas elípticas.
- Cifras de bloco.
- Funcões de Hash criptográficas (sem e com chave). A construção de Merkle-Damgard.
- Aplicação: assinaturas digitais e cifra autenticada

II. Segurança no software

- Vulnerabilidades em aplicações web e aplicações móveis.
- Cópia e modificação de software.
- Injeção de ataques.
- Análise estática de código e mecanismos de proteção dinâmica.

III. Segurança no hardware

- Vulnerabilidades do *hardware* e técnicas de ataque e de defesa.
- Trusted Platform Module (TPM) e Trusted Execution Environments (TEEs).
- ARM TrustZone e Intel Software Guard Extensions (SGX).

IV. Segurança das comunicações

- Perímetros de segurança e ameaças
- Segurança em redes sem fios.
- Túneis seguros.
- Sistemas de deteção de intrusão (IDS) e prevenção de intrusão (IPS).

V. Quadros normativos tais como GDPR, ISO27000, ITIL, NIST, e gestão de risco.

11. Syllabus

I. Mechanisms for protection of information

- Introduction to cryptography and crypto-analysis.
- Concepts of modular arithmetic, finite bodies and elliptic curves.
- Block numbers.
- Cryptographic Hash Functions (without and with key). The construction of Merkle-Damgard. Blockchains.
- Application: digital signatures and authenticated cipher

II. Software security

- Vulnerabilities in web applications and mobile applications.
- Modification and copy of software.
- Injection of attacks.
- Static code analysis and dynamic protection mechanisms.

III. Hardware security

- Hardware vulnerabilities and attack and defense techniques.
- Trusted Platform Module (TPM) and Trusted Execution Environments (TEEs).
- ARM TrustZone and Intel Software Guard Extensions (SGX).

IV. Communication security

- Security perimeters and threats
- Intrusion Detection (IDS) and intrusion prevention (IPS) systems.
- Incident response.
- Security policies.

V. Regulatory frameworks such as GDPR, ISO27000, ITIL, NIST, and risk management.

12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular

Para cada objetivo de aprendizagem existe pelo menos um tópico que é apresentado de forma teórica e avaliado numa componente prática. A formação matemática em teoria dos números em que assentam as técnicas criptográficas modernas está contemplada no ponto (I), permitindo aos alunos atingir os objetivos de aprendizagem de (1) e (2), contribuindo ainda para o objetivo de aprendizagem (3). O ponto (II) contribui para os objetivos de aprendizagem (3) e (5). O ponto (III) contribui para o objetivo de aprendizagem (4) e os pontos (IV) e (V) contribuem para os objetivos de aprendizagem (5) e (6).

12. Evidence of the syllabus coherence with the curricular unit´s intended learning outcomes

For each learning objective there is at least one topic that is presented in a theoretical way and evaluated in a practical component. The mathematical training in number theory on which modern cryptographic techniques are based is included in point (I), allowing students to achieve the learning objectives of (1) and (2), also contributing to the learning objective (3). Point (II) contributes to the learning objectives (3) and (5). Point (III) contributes to the learning objective (4) and points (IV) and (V) contribute to learning objectives (5) and (6).

13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico

Adota-se uma metodologia baseada em exposição interativa e interrogação. Para a apresentação dos temas são utilizados slides que guiam o andamento da aula, mas são também apresentados exemplos reais de aplicação dos assuntos discutidos. Durante as aulas de exposição os alunos são convidados a interagir sendo questionados informalmente sobre os assuntos em análise. Os tópicos principais são explorados através de trabalhos práticos para cada um dos principais conteúdos programáticos (I, II, III e IV-V) onde os alunos realizam experiências para consolidação dos conceitos apresentados em aula teórica, usando horas de trabalho autónomo e horas de contacto com o docente, dentro de uma lógica simples de aprendizagem baseada em projetos. As aulas práticas servem para acompanhar a realização dos trabalhos assegurando o correto desenvolvimento das competências dos estudantes.

13. Teaching and learning methodologies specific to the curricular unit articulated with the pedagogical model

A methodology based on interactive exposition and questioning is adopted. Slides are used to present the topics, guiding the progress of the lesson, but real examples of the application of the subjects discussed are also presented. During the lectures, students are invited to interact by being asked informal questions about the subjects being analysed. The main topics are explored through practical work for each of the main syllabuses (I, II, III and IV-V) where students carry out experiments to consolidate the concepts presented in lectures, using hours of autonomous work and hours of contact with the teacher, within a simple logic of project-based learning. Practical classes are used to accompany the realisation of the work, ensuring the correct development of the students' skills.

14. Avaliação

A classificação final, que no mínimo terá de ser maior ou igual a 9,5 valores, resulta de uma média aritmética ponderada das duas componentes de avaliação, o exame (E) e os trabalhos práticos (P), em que E tem um peso de 50% (com nota superior ou igual a 9,5 valores) e P (média aritmética simples dos trabalhos, com nota mínima de 8 valores por trabalho) tem um peso de 50%. Todos os elementos de avaliação são pedagogicamente fundamentais.

14. Assessment

The final grade, which must be at least greater than or equal to 9.5 points, results from a ordinary arithmetic mean of two main evaluation components, exam (E) and assignments (A), in which E has a weight of 50% (with a grade greater than or equal to 9.5 points) and A (simple arithmetic average of the assignments, with a minimum grade of 8 values per assignment) has a weight of 50%. All the elements of evaluation are pedagogically fundamental.

15. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

As aulas teóricas destinam-se à apresentação das bases teóricas dos conteúdos programáticos, enquanto nas aulas práticas são acompanhados os projetos em curso por parte de cada grupo de alunos. Privilegia-se uma forma de apresentação interativa, dando espaço ao aluno para expor as suas dúvidas. O trabalho autónomo (extra-aula) é guiado pelos trabalhos práticos propostos no contexto de cada módulo (I, II, III e IV-V), desenhados para consolidar as competências de conceção e desenvolvimento dos conteúdos programáticos. Os objetivos de aprendizagem são identificados nos guiões apresentados aos alunos, permitindo clarificar as competências que são necessárias adquirir nas aulas práticas e na realização das séries de exercícios.

15. Evidence of the teaching methodologies coherence with the curricular unit´s intended learning outcomes

The theoretical classes are intended to present the theoretical bases of the syllabus, while in the practical classes the ongoing projects are monitored by each group of students. A form of interactive presentation is privileged, giving the student space to expose their doubts. The autonomous work (outside the classroom) is guided by the practical work proposed in the context of each module (I, II, III and IV-V), designed to consolidate the skills of design and development of the syllabus. The learning objectives are identified in the scripts presented to the students, allowing to clarify the skills that are necessary to acquire in practical classes and in the realization of the series of exercises.

16. Bibliografia de consulta/existência obrigatória

1-Menezes A.J., Oorschot P.C. van, Vanstone S.A. (2001), Handbook on applied cryptography, 5ª edição, CRC Press, ISBN: 0-8493-8523-7
2-Miguel Correia, Paulo Jorge Sousa (2017), Segurança no Software, 2ª Edição, FCA, ISBN:978-972-722-858-4
3-Yuri Diogenes, Erdal Ozkaya (2018), Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics, Packt, ISBN: 9781788475297
4-Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey (2006), Inside Network Perimeter Security, Second Edition, Sams, ISBN: 9780672327377.

17. Observações

Unidade Curricular Obrigatória, Unidade Curricular Opcional

Data de aprovação em CTC:

Data de aprovação em CP: