Ficha de Unidade Curricular – (Versão A3ES 2018-2023)

1. Caracterização da Unidade Curricular.

1.1. Designação da unidade curricular ***(1.000 carateres).***
Cibersegurança / Cibersecurity

1.2. Sigla da área científica em que se insere ***(100 carateres).***
INF

1.3. Duração[1] ***(100 carateres).***
Semestral

1.4. Horas de trabalho[2] ***(100 carateres).***
162

1.5. Horas de contacto[3] ***(100 carateres).***
67,5H (T:43,5H TP:12H; PL: 12H)

1.6. ECTS ***(100 carateres).***
6

1.7. Observações[4] ***(1.000 carateres).***
Optativa

1.7. Remarks ***(1.000 carateres).***
Optional

2. Docente responsável e respetiva carga letiva na Unidade Curricular ***(preencher o nome completo) (1.000 carateres).***
José Manuel de Campos Lages Garcia Simão (18h)

3. Outros docentes e respetivas cargas letivas na unidade curricular ***(1.000 carateres).***
Lucía Fernández Suárez (18h)
Nuno Miguel Machado Cruz (15h)
Tiago Miguel Braga da Silva Dias (16,5h)

4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes). ***(1.000 carateres).***

Os estudantes que terminam com sucesso esta unidade curricular deverão ser 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, encriptação 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.
7. Proceder a uma análise de risco e definição de ameaças.

4. Intended learning outcomes (knowledge, skills and competences to be developed by the students). ***(1.000 characters).***

Students who successfully complete this course unit should be able to:

1. List the different mechanisms for information protection and main objectives (confidentiality, data integrity) and problems (key space size, key generation) of modern cryptography.
2. Describe some of the key application areas of number theory, such as public key encryption, block ciphers and hash functions, and *blockchain* infrastructures.

3. Identify existing vulnerabilities in the software and use techniques appropriate to their mitigation or correction
4. Explain the cryptographic mechanisms available on modern hardware platforms.
5. Identify different systems for detecting and preventing security breaches.
6. Identify the different existing regulatory frameworks.
7. Conduct a risk analysis and definition of threats.

5. Conteúdos programáticos ***(1.000 carateres).***

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. Blockchains.
- 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
- Sistemas de deteção de intrusão (IDS) e prevenção de intrusão (IPS).
- Resposta a incidentes.
- Políticas de segurança.

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

5. Syllabus ***(1.000 characters).***

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.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular ***(1.000 carateres).***

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 o objetivo de aprendizagem de (1) a (2). A aplicação dos conceitos matemáticos apresentados nos pontos (I) para a definição dos diferentes métodos criptográficos e usos apresentados nos pontos II, III, IV, V, e VI, possibilitará o aluno atingir os objetivos de aprendizagem de (3) a (7).
A realização de séries de exercícios permite aferir o cumprimento dos objetivos de aprendizagem (1) a (9).

6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes ***(1.000 characters).***

For each learning objective there is at least one topic that is presented theoretically and evaluated in a practical component. The mathematical training in numbers theory, on which modern cryptographic techniques are based, is considered in point (I), allowing students to reach the learning objective from (1) to (2). The application of the mathematical concepts presented in points (I) for the definition of the different cryptographic methods and applications presented in points II, III, IV, V and VI will enable the student to achieve the learning objectives from (3) to (7) .
The practice with series of exercises allows to verify the fulfillment of the learning objectives (1) to (9).

7. Metodologias de ensino (avaliação incluída) ***(1000 carateres).***

A metodologia de ensino é maioritariamente teórica, com o recurso a séries de exercícios para consolidação de cada um dos temas. Pretende-se privilegiar a autonomia do estudante no desenvolvimento de soluções para problemas complexos, adequados ao seu nível cognitivo.
Os objetivos de aprendizagem de (1) a (9) são avaliados através de duas componentes: a teórica, constituída por avaliação presencial (e.g. teste escrito, apresentação e/ou teste oral), e a prática, que consiste na realização de séries de exercícios por cada tema.
A classificação final resulta de uma média aritmética ponderada das duas componentes de avaliação, em que a componente teórica tem um peso de 50% e a componente prática tem um peso de 50%.
Para ambas as componentes teórica e prática, o aluno deverá obter classificação mínima de 10 valores, para obter aprovação à UC.

7. Teaching methodologies (including assessment) ***(1.000 characters).***

The teaching methodology is mostly theoretical, with the use of series of exercises to consolidate each of the themes. It is intended to privilege student autonomy in the development of solutions to complex problems, appropriate to their cognitive level.
The learning objectives of (1) to (9) are evaluated through two components: theoretical, consisting of face-to-face assessment (e.g. written test, presentation and / or oral test), and practice, exercises for each theme.
The final classification results from a weighted arithmetic mean of the two assessment components, where the theoretical component has a weight of 50% and the practical component has a weight of 50%.
For both theoretical and practical components, the student must obtain a minimum grade of 10 values, to obtain approval to the CU.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular ***(3.000 carateres).***

As aulas teóricas destinam-se à apresentação das bases teóricas dos conteúdos programáticos, enquanto nas aulas teórico-práticas são desenhados e desenvolvidos pequenos projetos e analisados casos de estudo. Privilegia-se uma forma de apresentação interativa, dando espaço ao aluno para expor as suas dúvidas. A componente laboratorial serve para aplicar, num ambiente controlado, as técnicas apresentadas nas aulas teóricas e teórico-práticas.
O trabalho autónomo (extra aula) é guiado pelas séries de exercícios, desenhadas 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.

8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes ***(3.000 characters).***

Theoretical classes are designed to present the theoretical bases of the programmatic contents, while in theoretical-practical classes small projects are designed and developed along with the analysis of case studies. An interactive form of presentation is favored, giving space for the student to expose his doubts. The laboratory component is used to apply, in a controlled environment, the techniques presented in the theoretical and theoretical-practical classes.

Autonomous work (extra class) is guided by the series of exercises, designed to consolidate the skills of design and development of programmatic contents. The learning objectives are identified in the scripts presented to the students, allowing to clarify the competences that are necessary to acquire in the practical classes and in the accomplishment of the series of exercises.

9. Bibliografia de consulta/existência obrigatória ***(1.000 carateres).***

Menezes A.J., Oorschot P.C. van, Vanstone S.A., "Handbook on applied cryptography", 5ª edição, CRC Press, 2001 (ISBN 0-8493-8523-7)
Miguel Correia, Paulo Jorge Sousa, "Segurança no Software", 2ª Edição, FCA, 2017 (ISBN 978-972-722-858-4)
Yuri Diogenes, Erdal Ozkaya, "Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics", Packt, 2018 (ISBN 9781788475297)

Bibliografia Complementar:

Matt Bishop, "Introduction to Computer Security", Addsion Wesley, 2004 (ISBN 978-0321247445)
Wenliang Du, "Computer Security: A Hands-on Approach", CreateSpace Independent Publishing Platform, 2017 (ISBN 978-1548367947)
Hoffstein J., Pipher J., Silverman J.H, "An Introduction to Mathematical Criptography", Springer-Verlag 2008 (ISBN 978-0-387-77994-2)

---

[1] Anual, semestral, trimestral, …
[2] Número total de horas de trabalho.
[3] Discriminadas por tipo de metodologia adotado (T - Ensino teórico; TP - Ensino teórico-prático; PL - Ensino prático e laboratorial; TC - Trabalho de campo; S - Seminário; E - Estágio; OT - Orientação tutorial; O - Outro).
[4] Assinalar sempre que a unidade curricular seja optativa.