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

1. Caracterização da Unidade Curricular.

1.1. Designação da unidade curricular ***(1.000 carateres).***
Segurança em Redes de Computadores (SRC) / *Computer Networks Security*

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

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

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

1.5. Horas de contacto[3] ***(100 carateres).***
Total: 67,5 h; T: 45.5 h, TP: 10 h, PL: 12 h

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

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).***
Vítor Jesus Sousa de Almeida; 67,5 horas de contacto

3. Outros docentes e respetivas cargas letivas na unidade curricular ***(1.000 carateres).***

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

Os estudantes ao terminarem com sucesso esta unidade curricular serão capazes de:

1. Perceber claramente os conceitos de confidencialidade, integridade e autenticação e os protocolos usados para os garantir.
2. Identificar, quer do ponto de vista dos atacantes, quer dos defensores, os pontos críticos em termos de segurança.
3. Definir soluções possíveis para o incremento da segurança através da análise das vulnerabilidades, ameaças e tipos de ataques a sistemas de comunicação.
4. Usar e configurar os equipamentos de rede com os diferentes protocolos usados para incrementar a segurança.
5. Efetuar a escolha consciente da política de segurança mais adequada a cada situação.

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

Students to successfully finish this course you will:

1. *Clearly perceive the concepts of confidentiality, integrity and authentication and protocols used to ensure them.*
2. *Identify, either from the standpoint of the attackers or defenders, the critical points in terms of security.*
3. *Define possible solutions to increase the security by analyzing the vulnerabilities, threats and attacks of communication systems.*
4. *Use and configure network equipment with different protocols used to increase safety.*
5. *Make the conscious choice of the security policy most appropriate for each situation.*

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

Factos sobre segurança.
Ameaças, vulnerabilidades e ataques.
Noções de confidencialidade, integridade e autenticação.
Criptografia (algoritmos de *hash*, MAC e HMAC, números aleatórios, distribuição de chaves, Introdução à teoria dos números/matemática modular, cifras simétricas (substituição e transposição, algoritmos de César ao AES) e assimétricas (RSA), certificados digitais x.509 e autoridades de certificação, assinaturas digitais (DSA e Schnorr)).

Segurança em camadas OSI de baixo nível (MACSEC - 802.1ae, controlo de acessos - 802.1x, RADIUS, suporte de VPNs – PPP, EAP, GRE, PPTP, L2TP).
Segurança em redes sem fios (WLAN – do WEP ao WPA 3).
Segurança das comunicações ao nível das camadas OSI de rede e transporte (IPsec, IKEv2).
Segurança na Web (SSH, SSL/TLS, HTTPS).
Segurança nos serviços de *email* (segurança em SMTP, POP, IMAP, MIME; Sender Policy Framework (SPF), Domain keys).
Conceitos de segurança aplicados em Blockchain e Smart Contracts.
Segurança no IoT.
Políticas de segurança.
Práticas de segurança: *routers*, *firewalls*, IDS e armadilhas.
Segurança na gestão de redes.

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

Facts about safety.
Threats, vulnerabilities and attacks.
Cryptography (hash algorithms, key distribution, symmetric (substitution and transposition, algorithms from Cesar to AES) and asymmetric ciphers (introduction to number theory/modular mathematics, elliptical curves, RSA), digital certificates x.509 and certification authorities, digital signatures (DSA, Schnorr)).
Security for dial-in access (access control - 802.1x, RADIUS, support for VPN - PPTP, L2TP).
Security in wireless networks (WLAN – from WEP to WPA 3).
Communications security at the various layers of the OSI model (IPsec, IKEv2).
Security in Web (SSH, SSL / TLS, HTTPS)
Security services in email (security in SMTP, POP, IMAP, MIME; Sender Policy Framework (SPF), Domain keys)
Security concepts applied in Blockchain e Smart Contracts.
Security in IoT.
Security policies.
Security in network management.
Security practices: routers, firewalls, IDS and traps.

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

A segurança em redes é cada vez mais uma área do conhecimento incontornável para aqueles que se pretendem dedicar às redes de computadores. Nesta unidade curricular os estudantes ficam a conhecer os principais conceitos referentes à segurança aplicada às redes, assim como os protocolos usados ao nível das diversas camadas do modelo de referência OSI, desde os de suporte ao controlo de acessos, passando pelas VPN, pela segurança nas redes sem fios e em diversas aplicações mais comuns como *browsers* e *email*. Aprendem a usar os equipamentos de rede (*switches* e *routers*) como auxiliares dos *firewalls* para minimizarem eventuais ataques já descritos anteriormente. Aprendem o que é política de segurança e a sua importância para a segurança das empresas, isto respeitando a legislação em vigor.

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

The network security is increasingly an area of knowledge essential for those who intend to devote to computer networks. In this course students get to know the main concepts related to security applied to networks, as well as the protocols used across the various layers of the OSI reference model, since the support for access control, through the VPN, to the security at wireless networks and in many applications such as browsers and email. They learn to use the network equipment (switches and routers) as auxiliaries of firewalls to minimize any attack, previously described. Learn what is the security policy and its importance to the safety of enterprises, that respecting the law.

7. Metodologias de ensino (avaliação incluída) ***(1.000 carateres).***

Ensino teórico-prático, estando previstas 30 aulas a que correspondem 67,5 horas de contacto. O tempo total de trabalho estimado para o estudante é de cerca de 162 horas. As aulas de caracter teórico destinam-se à exposição e discussão dos principais conteúdos programáticos, incentivando a interatividade e colocação de questões.
Os tópicos principais são ainda explorados através da realização de fichas teórico/práticas em que as fichas teóricas são realizadas individualmente extra-aula e as fichas práticas/trabalhos são realizadas em grupo. Os resultados de aprendizagem são avaliados individualmente através de 2 testes escritos e/ou de exame final, das fichas teóricas individuais de resolução extra-aula e da discussão da componente prática.
A classificação final é obtida através de 60% da classificação da componente teórica mais 40% da classificação da componente prática.
As avaliações seguem as regras indicadas nas "Normas de Avaliação de Conhecimentos" em vigor no ISEL.

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

Theoretical and practical teaching along 30 lectures that correspond to 67.5 contact hours. The total time for student work is around 162 hours. The theoretical lectures serve to discuss the topics of the main syllabus, encouraging interactivity and asking questions. The main topics are further explored by performing computer-based projects and the design and implementation of physical networks using routers (problem-based learning).
The learning outcomes are individually assessed through written tests and/or final exam, and the discussion of the practical components.
The final grade is obtained with the percentages of 60% from the theory evaluation plus 40% from the practical evaluation.
The evaluation of the students follows the rules expressed in “Normas de Avaliação de Conhecimentos” from ISEL.

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

Os objetivos da unidade curricular são obtidos através de aulas teóricas e respetivos elementos de apoio (slides) e bibliografia, da realização de exercícios práticos e de casos de estudo selecionados pelo docente. O objetivo do ponto de vista prático é alcançado através de trabalhos laboratoriais, em que os alunos desenvolvem e estudam o funcionamento de mecanismos de segurança em redes usando os equipamentos de redes. A realização dos trabalhos de laboratório é acompanhada pelo docente durante as horas de contacto para assegurar o correto desenvolvimento dos conhecimentos e das competências dos estudantes.

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

The objectives of the course are achieved through lectures and respective supporting elements (slides) and bibliography, conducting practical exercises and case studies selected by the teacher. The goal of a practical standpoint is achieved through laboratory work, in which students develop and study the functioning of security mechanisms in networks using network equipment. The completion of the laboratory work is accompanied by the teacher during the contact hours to ensure the correct development of knowledge and skills of students.

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

- Folhas da disciplina
- “Segurança em Redes Informáticas, 5ª edição”, André Zúquete, FCA, 2018
- “Cryptography and Network Security - Principles and Practice, Seventh edition”, William Stallings, Prentice-Hall, 2017

---

[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.