Politécnico de Viseu
Tecnologia e Gestão Viseu

FICHA ECTS
Segurança Informática
2021-22

Caraterização da Unidade Curricular / Characterisation of the Curricular Unit

Designação da Unidade Curricular / Curricular Unit:	[31821484] Segurança Informática [31821484] ICT Security
Plano / Plan:	Licenciatura em Engenharia Informática V2
Curso / Course:	Licenciatura em Engenharia Informática Computer Sciences Engineering
Grau / Diploma:	Licenciado
Departamento / Department:	Departamento de Informática
Unidade Orgânica / Organic Unit:	Escola Superior de Tecnologia e Gestão de Viseu
Área Científica / Scientific Area:	Ciências Informáticas
Ano Curricular / Curricular Year:	3
Período / Term:	S1
ECTS:	4.5
Horas de Trabalho / Work Hours:	0119:30

Horas de Contacto/Contact Hours:

(T) Teóricas/Theoretical:	0019:30	(TC) Trabalho de Campo/Fieldwork:	0000:00
(TP) Teórico-Práticas/Theoretical-Practical:	0000:00	(OT) Orientação Tutorial/Tutorial Orientation:	0000:00
(P) Práticas/Practical:	0026:00	(E) Estágio/Internship:	0000:00
(PL) Práticas Laboratoriais/Pratical Labs:	0000:00	(O) Outras/Others:	0000:00
(S) Seminário/Seminar:	0000:00		

Inválido para efeito de certificação

Docente Responsável / Responsible Teaching

[3078] Filipe Manuel Simoes Caldeira

Docentes que lecionam / Teaching staff

[3078] FILIPE MANUEL SIMOES CALDEIRA

Objetivos de Aprendizagem

Reconhecer e discutir os principais aspetos relacionados com a segurança informática (técnicos, sociais, legais e éticos). Identificar os principais mecanismos, tecnologias e ferramentas de segurança. Definir e implementar políticas de segurança. Capacitar para o desenvolvimento de código mais seguro. Realizar tarefas de monitorização e auditoria. Instalar soluções de segurança em redes e sistemas informáticos.

Learning Outcomes of the Curricular Unit

To understand and discuss main aspects related to ICT security (technical, social, legal and ethical aspects). Identify key mechanisms, technologies and security tools. Define and implement security policies. Support the development of secure code. Perform monitoring and auditing tasks. Install security solutions in information systems and networks.

Conteudos Programáticos (Lim:1000)

- Introdução à Segurança Informática
- Criminalidade informática
- Vulnerabilidades de segurança
- Políticas de segurança
- Introdução à Criptografia (algoritmos simétricos e assimétricos)
- PGP e GPG (email seguro)
- Autoridades de Certificação
- O Cartão do Cidadão Português
- SSL e TLS
- Redes Privadas Virtuais (VPN)
- Sistemas de detecção de intrusão (IDS)
- Sistemas de autenticação (e.g. RADIUS)
- Segurança em redes sem fios 802.11 (WLAN)
- Sistemas de Firewall
- Segurança no desenvolvimento de software (vulnerabilidades, ataques e proteção de serviços Web)

Inválido para efeito de certificação

Syllabus (Lim:1000)

- Introduction to Computer Security
- Computer Crime
- Security Vulnerabilities
- Security Policies
- Introduction to Cryptography (symmetric and asymmetric algorithms)
- PGP and GPG (secure email)
- Certification Authorities
- The Portuguese Citizen Card
- SSL and TLS
- Virtual Private Networks (VPN)
- Intrusion Detection Systems (IDS)
- Authentication systems (e.g. RADIUS)
- Wireless networks Security 802.11 (WLAN)
- Firewall Systems
- Security in software development (vulnerabilities, attacks and Web services protection)

Inválido para efeito de certificação

Metodologias de Ensino (Avaliação incluída; Lim:1000)

Utilização do quadro e videoprojector; resolução de fichas de trabalho de carácter prático nas aulas práticas e laboratoriais (O desempenho do aluno nesses exercícios é tido em conta na classificação final); intervenção permanente dos participantes, na colocação de questões pertinentes relativas às matérias abordadas; apoio aos alunos, nomeadamente no horário tutorial; utilização da plataforma moodle para a disponibilização do material de apoio e para comunicação entre Professor ¿ Aluno.

Avaliação Continua e Época Normal: A avaliação consiste em avaliação prática (trabalhos práticos e assiduidade) - 40% e uma escrita, de carácter individual, que compreende toda a matéria lecionada - 60%. Restantes épocas: Aplicam-se as regras da época normal ou caso os alunos não sejam avaliados na componente prática, a avaliação consiste num teste escrito - 100% englobando toda a matéria. Cada componente de avaliação tem uma classificação mínima de 9,5 val.

Teaching Methodologies (Including evaluation; Lim:1000)

Pedagogical strategies employed in the course: Oral presentation in lectures using the video projector; solving proposed exercises in practical classes (The student's performance in the practical classes is taken into account in the final grade); permanent intervention of participants placing relevant questions relating the addressed subject; support students, particularly in the scheduled tutorial hours; use of the e-learning moodle platform in order to provide access to the course materials and also to improve communication teacher - student.

Continuous Assessment and "Época Normal": The evaluation consists of practical assessment (practical work and attendance) - 40% and a individual written exam that comprises all taught subjects - 60%.
Other evaluation moments: Previous rules apply or If students are not evaluated in the practical component, the evaluation consists of a written test - 100% encompassing all subjects. Each evaluation component has a minimum grade of 9.5 in 20.

Inválido para efeito de certificação

Bibliografia de Consulta (Lim:1000)

- Apontamentos disponibilizados pelos Docentes.

- Segurança em redes informáticas, André Zúquete, A., (4a Edição), FCA, 2010, ISBN: 978-972-722-767-9
- RFC 2196, The Site Security Handbook, IETF, 1997.
- Engenharia de redes informáticas, Edmundo Monteiro, Fernando Boavida, (10ª edição), FCA, 2011, ISBN 978-972-722-694-8
- Gestão de sistemas e redes em Linux, Jorge Granjal, (2ª edição), FCA, , 2010 , ISBN 978-972-722-645-0
- Computer and information security handbook, John R. Vacca, Elsevier, 2009, ISBN 978-0-12-374354-1
- Segurança no Software, Miguel Correia e Paulo Sousa, FCA, 2010 ISBN: 978-972-722-662-7
- Cryptography and Network Security: Principles and Practice, W. Stallings, (5a Edição), 2010, ISBN-13: 978-0136097044
- The history of information security: a comprehensive handbook, Karl de Leeuw, Jan Bergstra, Elsevier, 2007, ISBN 978-0-444-51608-4
- Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network, Anónimo; SAMS

Bibliography (Lim:1000)

- Apontamentos disponibilizados pelos Docentes.

- Segurança em redes informáticas, André Zúquete, A., (4a Edição), FCA, 2010, ISBN: 978-972-722-767-9
- RFC 2196, The Site Security Handbook, IETF, 1997.
- Engenharia de redes informáticas, Edmundo Monteiro, Fernando Boavida, (10ª edição), FCA, 2011, ISBN 978-972-722-694-8
- Gestão de sistemas e redes em Linux, Jorge Granjal, (2ª edição), FCA, , 2010 , ISBN 978-972-722-645-0
- Computer and information security handbook, John R. Vacca, Elsevier, 2009, ISBN 978-0-12-374354-1
- Segurança no Software, Miguel Correia e Paulo Sousa, FCA, 2010 ISBN: 978-972-722-662-7
- Cryptography and Network Security: Principles and Practice, W. Stallings, (5a Edição), 2010, ISBN-13: 978-0136097044
- The history of information security: a comprehensive handbook, Karl de Leeuw, Jan Bergstra, Elsevier, 2007, ISBN 978-0-444-51608-4
- Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network, Anónimo; SAM

Observações

«Observações»

Observations

«Observations»

Observações complementares

Inválido para efeito de certificação