Ano Lectivo	2016/17
Curso	Engenharia Informática
Unidade Curricular	Segurança
Língua de ensino	Português

ECTS/tempo de trabalho (horas)

ECTS	Total	Horas de contacto semestral						
		T	TP	PL	S	TC	O	OT
2.5	65	15	15					

T - Teóricas; TP - Teórico-práticas; PL - Prática-laboratorial; S - Seminário; OT - Orientação tutorial; TC - Trabalho de campo; E - Estágio; O* - Outras horas caraterizadas como Ensino Clínico ao abrigo da Diretiva nº 77/453/CEE de 27 Junho adaptada pela Diretiva 2005/36/CE;

Docente Responsável/Carga letiva [nome completo e e-mail]	Secundino Domingos Marques Lopes / secundino.lopes@estgp.pt
Outros Docentes e respetivas cargas letivas [nome completo e e-mail]	Secundino Domingos Marques Lopes / secundino.lopes@estgp.pt
Pré-requisitos [competências à entrada; pré-requisitos; precedências]	Não
Objetivos da aprendizagem (conhecimentos, aptidões e competências) a desenvolver pelos estudantes, operacionalização dos objetivos e medição do seu grau de cumprimento)	Na sociedade atual em que a informação e o conhecimento, em que esta se baseia, constituem o principal ativo de uma instituição, torna-se imperioso que a respetiva segurança e proteção sejam endereçadas a todos os níveis da organização e que se utilizem as melhores práticas para garantir a fiabilidade e a disponibilidade deste ativo. Atualmente são muitos os fatores a ter em consideração relativamente à segurança da informação e dos sistemas Pretende-se que neste domínio o aluno seja capaz de: (a) Identificar os conceitos fundamentais da segurança em Sistemas de Informação e definir as principais tarefas associadas à definição e implementação de uma política de segurança; (b) Desenhar e gerir o ciclo de vida da segurança de um sistema; (c) Explicar os objetivos fundamentais da criptografia; (d) Instalar e configurar tecnologias de Firewall, assim como sistemas de deteção e prevenção de ataques (IPS, IDS); (e) Instalar e configurar as várias topologias de acesso remoto (VPN).
Conteúdos Programáticos [estrutura de conteúdos a desenvolver para o total de horas previsto]	(1) Modern Network Security Threats (Fundamental Principles of a Secure Network, Attack Methodologies) (2) Securing Network Devices (Privilege Levels and Role-Based, Monitoring Devices, Using Automated Features) (3) Authentication, Authorization and Accounting (Configure Server-Based AAA) (4) Implementing Firewall Technologies (Context-Based Access Control, Zone-Based Policy Firewall) (5) Implementing Intrusion Prevention (IPS Technologies, Implementing IPS) (6) Securing the Local Area Network: (Endpoint Security Considerations, Layer 2 Security Considerations, Wireless, VoIP and SAN Security Considerations) (7) Cryptography (Cryptographic Services, Hashes and Digital Signatures, Symmetric and Asymmetric Encryption) (8) Implementing Virtual Private Networks (VPNs, IPSec VPN Components and Operation, Site-to-Site IPSec VPNs, Remote Access VPN, SSL VPNs) (9) Managing a Secure Network (Secure Network Lifecycle, Self-Defending Network, Building a Comprehensive Security Policy)
Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular	As competências associadas à Unidade Curricular constituem uma especialização das competências e conhecimentos desenvolvidos em Unidades Curriculares como Redes de Computadores I e II, e Administração de Sistemas. Os conteúdos programáticos apresentados permitem por um lado que o aluno obtenha o máximo de conhecimentos teóricos para o desenho, gestão e monitorização da segurança de um sistema, e por outro consiga por em prática estes mesmos conhecimentos através da configuração de vários equipamentos como routers, switchs, firewall, IPS/IDS, e da aplicação de técnicas de encriptação e controlo de acessos.

Metodologias de ensino (avaliação incluída) [indicar os produtos, critérios e pesos de avaliação] (máx1000 carateres)	**1 - Metodologias de ensino** Todos os conteúdos a lecionar estarão disponíveis na Intranet da Escola. Os conteúdos serão apresentados aos alunos com recurso a apresentações dinâmicas em PowerPoint. Para desenvolvimento dos conteúdos lecionados serão disponibilizados laboratórios ou fichas práticas para implementação individual ou em grupo. Os momentos de avaliação apresentam sempre a avaliação da componente teórica e da componente prática. Esta ultima, é realizada nas estações de trabalho disponíveis. No domínio da avaliação, o aluno pode optar por um dos dois regimes apresentados na secção de avaliação. **2 - Avaliação por frequência** (1) Avaliação continua/por frequência: um teste teórico (30%) e um teste prático (70%). Considera-se aprovado se a média final da avaliação obtida, de acordo com as ponderações apresentadas, for superior ou igual a 10 valores; **3 - Avaliação por Exame** (2) Avaliação por Exame Final: componente teórica (30%) componente prática (70%).
Demonstração da coerência das metodologias de ensino com os objectivos da aprendizagem da unidade curricular	Considerando que a Unidade Curricular é essencialmente de prática laboratorial, a metodologia de ensino proposta é a mais adequada para motivar o aluno a envolver-se de forma ativa no seu próprio processo de aprendizagem. Toda a componente laboratorial é o mais próximo possível da exigência que o mercado de trabalho apresenta a profissionais no domínio do networking.
Bibliografia Principal	1. Edmundo Monteiro, Fernando Boavida; “Engenharia de Redes Informáticas”; 10ª Edição; FCA; 2011. 004.7 MNT (outra edição) 2. Série de normas ISO/EIC 27000; Information Technology — Security Techniques; 2009 (disponíveis em suporte papel na Biblioteca da Escola). 3. CCNA Security 1.0 Student Lab Manual; 2010. 4. Cisco Internetworking Technology Handbook (Disponível na Internet) http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook 5. Todos os conteúdos lecionados encontram-se disponíveis no espaço de eLearnig da CISCO em http://cisco.netacad.net/ ou na página de apoio à Unidade Curricular na Intranet da Escola.
Bibliografia Complementar	
Situações especiais [estudantes com estatuto especial]	**1 - Avaliação por frequência** **2 - Avaliação por Exame**