POLI ESCOLA SUPERIOR TECNOLOGIA GESTÃO TÉCNICO GUARDA	**GUIA DE FUNCIONAMENTO DA UNIDADE CURRICULAR** (GFUC)	**MODELO** PED.008.03

Curso	**Tesp Cibersegurança**						
Unidade curricular (UC)	**Segurança em Redes e Sistemas Informáticos**						
Ano letivo	2023/2024	*Ano*	2.º	*Período*	1.º semestre	*ECTS*	4.5
Regime	Obrigatório	*Tempo de trabalho (horas)*			Total: 112.5	Contacto: 45	
Docente(s)	**Pedro Manuel Pinto Teixeira**						
☐ *Responsável* ☒ *Coordenador(a)* ☐ *Regente*	*da UC ou Área/Grupo Disciplinar* *(cf. situação de cada Escola)*	**Fernando Melo Rodrigues**					

GFUC PREVISTO

1. OBJETIVOS DE APRENDIZAGEM

Pretende-se que o aluno adquira conhecimentos e competências no domínio da Engenharia de Redes comunicações. No fim da disciplina o aluno deve:

O1. Capacidade de definição e implementação de Políticas de Segurança;
O2. Conhecimento dos principais mecanismos e tecnologias de segurança;
O3. Conhecimento dos aspetos relacionados com a segurança de Sistemas Informáticos;
O4. Capacidade de conceber e instalar soluções de segurança em Redes Informáticas;
O5. Saber projetar sistemas de gestão e de segurança de redes, adequados aos cenários e
O6. Capacidade de realizar tarefas de monitorização e auditoria de segurança

2. CONTEÚDOS PROGRAMÁTICOS

C1. Introdução à segurança
- a. Importância da Segurança Informática
- b. Conceitos fundamentais
- c. Segurança Física e Segurança Lógica
- d. Políticas de Segurança Informática

C2. Ameaças à Segurança Informática
- a. Tipos de Ameaças
- b. Reconhecimento de Sistemas, Serviços e Vulnerabilidades
- c. Escuta de Pacotes
- d. Usurpação de Endereço IP
- e. Sequestro de Sessão TCP
- f. Negação de Serviço
- g. Engenharia Social
- h. Vírus, Vermes e Cavalos de Troia
- i. Lista de Vulnerabilidades

C3. Conceitos fundamentais sobre *firewalls*
- a. Filtro de Pacotes
- b. Tradução de endereços e Portos
- c. Deteção e prevenção de Intrusão
- d. Proxies
- e. Redes Privadas Virtuais

C4. Criptografia
- a. Criptografia e criptanálise
- b. Encriptação Simétrica e Encriptação assimétrica
- c. Hashing
- d. Cifras de bloco e stream
- e. Algoritmos
- f. Módulos de encriptação por hardware
- g. Evolução de criptografia
- h. Assinaturas digitais

C5. Filtros de pacotes em routers Cisco
- a. Arquitetura de Filtragem de Pacotes em Routers Cisco
- b. Configuração e Aplicação de Listas de Controlo de Acesso
- c. Exemplos práticos
- d. Listas de Acesso Sensíveis ao Contexto (CBAC)
- e. Tradução de endereços (NAT)

C6. Autenticação
- a. Técnicas de autenticação
- b. Protocolos
- c. Autenticadores de mensagens

3. DEMONSTRAÇÃO DA COERÊNCIA DOS CONTEÚDOS PROGRAMÁTICOS COM OS OBJETIVOS DA UC

Os Conteúdos 1, 2, estão coerentes com o Objetivo 1, pois focam as características das redes, as aplicações telemáticas e as arquiteturas de comunicação.
O Conteúdo 3 é coerente com o Objetivo 2, pois são lecionados os conteúdos referentes às cablagens.
O Conteúdo 4 é coerente com o Objetivo 3, pois são lecionadas as tecnologias de comunicação existentes nos diferentes ambientes.
O Conteúdo 5 e 6 são coerentes com o Objetivo 4, pois são lecionados conteúdos de gestão e segurança, e explicada a forma de os implementar num projeto.
Os conteúdos 7, 8, 9, e 10 são coerentes com o objetivo 5 e 6, pois são lecionados os conteúdos que permitem ao aluno ficar apto a planear, projetar e fiscalizar a implementação de uma rede de comunicação.

4. BIBLIOGRAFIA PRINCIPAL

Obrigatória:

B1. Omar Santos, John Stuppi, " CCNA Security 210-260 Official Cert Guide Premium Edition eBook and Practice Test", Cisco Press 2015

B2. CISCO, "White Paper - The Science of Intrusion Detection System Attack Identification", http://www.Cisco.com/en/US/products/sw/secursw/ps2113/products_white_paper09186a0080092334.shtml, (Julho 2013)

Recomendada:

B4. Kazienko, P., Dorosz, P., "Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture)",

http://www.windowsecurity.com/articles/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html, (Abril 2013)

5. METODOLOGIAS DE ENSINO (REGRAS DE AVALIAÇÃO)

Metodologias de ensino:

1. *Lição expositiva*
2. *Pesquisa individual*
3. *Demonstração experimental*

Regras de avaliação:

Avaliação contínua: *A aprovação obtém-se quando a média ponderada dos fatores de avaliação frequência/exame e componente prática, for igual ou superior a 10 valores, sendo dispensados de exame. Esta consiste:*

Testes escritos (40%). Trabalho práticos de laboratório (60%)

Avaliação final*: para o estudante que não tenha obtido aproveitamento na avaliação contínua ou não a tenha realizado. Exame e Exame de Recurso:*

Teste escrito (40%). Trabalho práticos de laboratório (60%)

6. DEMONSTRAÇÃO DA COERÊNCIA DAS METODOLOGIAS DE ENSINO COM OS OBJETIVOS DA UC

Lição expositiva *é transversal aos objetivos O1, O3, O4 em virtude da necessidade da introdução dos conteúdos teóricos.*

Complementarmente, tal como se infere pelos O4 e O5, será introduzida uma componente com um cariz prático pelo que será adotado o método de ***demonstração experimental*** *na elaboração de configurações de equipamentos.*

Trabalho de projeto está coerente com os objetivos visto que o trabalho consiste no planeamento e projeto de uma rede de comunicação, passando por todas as fases de aprendizagem, desde a análise dos requisitos, passando pela escolha das tecnologias, dos equipamentos e dos sistemas de gestão e segurança. Pelo que obriga à aplicação prática de todos os conceitos abordados ao longo do semestre

7. REGIME DE ASSIDUIDADE

Não tem regime de assiduidade.

8. CONTACTOS E HORÁRIO DE ATENDIMENTO

Nome	Email	Telefone	Gabinete
Pedro Pinto	ppinto@ipg.pt	1020	CI-ESTG

9. OUTROS

-

DATA

19 de Setembro de 2023

ASSINATURAS

Assinatura dos Docentes, Responsável/Coordenador(a)/Regente da UC ou Área/Grupo Disciplinar

O(A) Docente

(assinatura)

O(A) Coordenador(a) da Área/Grupo Disciplinar

(assinatura)