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

Curso	TesP Cibersegurança						
Unidade curricular (UC)	Hacking de Aplicações						
Ano letivo	2022/2023	*Ano*	2	*Período*	1	*ECTS*	4,5
Regime	Obrigatório	*Tempo de trabalho (horas)*			Total: 112,5	Contacto: 45	
Docente(s)	Pedro Manuel Pinto Teixeira						
☐ *Responsável* ☒ *Coordenador(a)* ☐ *Regente*	*Área/Grupo Disciplinar* *(cf. situação de cada Escola)*	Fernando Melo Rodrigues					

GFUC Previsto

1. OBJETIVOS DE APRENDIZAGEM

Após a conclusão da UC, os alunos deverão ser capazes de:

1. Desenvolver software de acordo com a legislação nacional e normas internacionais para segurança do software
2. Saber usar um processo de desenvolvimento de software seguro
3. Identificar as ameaças, vulnerabilidades e ataques ao software mais comuns e saber aplicar as devidas medidas de mitigação
4. Usar os vários tipos de encriptação para aumentar a segurança do software

2. CONTEÚDOS PROGRAMÁTICOS

1. Segurança do software e segurança da informação
2. Ciclos de vida de desenvolvimento de software seguro
3. Legislação sobre segurança
4. Normas internacionais de certificação de segurança
    1. ISO/IEC 27001
    2. PCI-DSS
5. Ameaças, vulnerabilidades e ataques mais comuns
    3. XSS
    4. Buffer overflow
    5. SQL Injection
    6. Outros

6. Encriptação
    7. Simétrica
    8. Fluxo
    9. Troca segura de chaves de encriptação usando Diffie-Hellman
    10. Assimétrica
    11. Hashing
    12. Certificados digitais

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

1. Os Conteúdos 1, 3 e 4 estão coerentes com o Objetivo 1, pois focam aspetos fundamentais da segurança, a legislação portuguesa vigente e normas internacionais de segurança do software.
2. O Conteúdo 2 coerente com o Objetivo 2, pois foca os processos de desenvolvimento de software seguro mais usados na indústria.
3. O Conteúdo 5 coerente com o Objetivo 3, pois foca as ameaças, vulnerabilidades e ataques ao software mais comuns, como se manifestam e como podem ser minimizados.
4. O Conteúdo 6 coerente com o Objetivo 4, pois foca as técnicas e algoritmos de encriptação e a sua aplicação no desenvolvimento de software.

4. BIBLIOGRAFIA PRINCIPAL

Obrigatória:

1. Apontamentos fornecidos pelo docente
2. Whitman, M. e Mattord, H. (2011), Principles of Information Security, Cengage Learning
3. Gregory, P. (2010), CISSP Guide to Security Essentials, Cengage Learning
4. Dafydd Stuttard, Marcus Pinto, (2011), The Web Application Hacker's Handbook, 2nd edition, Wiley Publishing, Inc.
5. Michael Howard, David LeBlanc, (2003), Writing Secure Code, 2nd edition, Microsoft Press

Recomendada:

1. Miguel Correia, Paulo Sousa, (2017), Segurança no Software, FCA
2. Michael Howard, David LeBlanc, (2005), 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, McGraw-Hill/Osborne
3. William Stallings, (2011), Cryptography and Network Security Principles and Practices, 5th edition, Prentice Hall
4. Nuno Carvalho (2009) Organizações e Segurança Informática, Lugar da Palavra Editora
5. Zúquete, A. (2010), Segurança em Redes Informáticas, FCA Editora

5. METODOLOGIAS DE ENSINO (REGRAS DE AVALIAÇÃO)

Metodologias de ensino:

1. Lição expositiva
2. Lição interativa
3. Resolução de problemas
4. Trabalho de projeto

Regras de avaliação:

Avaliação contínua:

- Realização de 6 trabalhos práticos – 100%

Avaliação por exame final na Época Normal, Época de Recurso ou Época Especial:

- Realização de 6 trabalhos práticos – 100%

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

1. Lição expositiva está coerente com os objetivos devido à necessidade de apresentar os conteúdos teóricos aos alunos, nomeadamente os vários aspetos relacionados com a segurança, a legislação e normas aplicáveis.

2. Lição interativa está coerente com os objetivos pois a interação alunos/docentes ajuda a aprendizagem dos conceitos para além da introdução de novas ideias, perspetivas e soluções que podem ser aplicadas tanto na fase de análise como na de desenvolvimento de software seguro, tendo em conta os agentes externos e como minimizar os seus efeitos.

3. Resolução de problemas está coerente com os objetivos pois a aplicação de conteúdos teóricos a exercícios práticos de inspiração realista, relacionados com o estudo da segurança do software, a aplicação dos controlos adequados, incluindo a encriptação, perante as possíveis ameaças, vulnerabilidades e ataques, ajuda a consolidar a matéria, realçando o saber fazer.

4. Trabalho de projeto está coerente com os objetivos pois abrange o desenvolvimento de software seguro, passando por todas as fases desde a sua conceção até à sua utilização, pelo que obriga à aplicação prática de todos os conceitos abordados ao longo do semestre a uma situação realista nova.

7. CONTATOS

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

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)