Designação	Princípios Técnicos em Cibersegurança (C-Academy)	Área Científica	-
Classificação	Unidade/Projeto Extracurricular	Escola	Escola Superior de Tecnologia e de Gestão de Bragança
Ano Letivo	2023/2024	Ano Curricular	1
Nível	-	Créditos ECTS	2.0
Tipo	Modular	Semestre	-
Código	9929-949-1005-00-23		

Horas totais de trabalho	54	Horas de Contacto	T -	TP 35	PL -	TC -	S -	E -	OT -	O -

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutórica; O - Outra

Nome(s) do(s) docente(s)	Nuno Gonçalves Rodrigues

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Compreender o ciclo de desenvolvimento de software, incluindo a programação, depuração e testes.
2. Conhecer ferramentas e práticas de gestão e controlo de versões e de correções de software.
3. Compreender o modelo de comunicação cliente-servidor através de sockets e a sua interface programática.
4. Conhecer os fundamentos, conceitos, princípios, limitações e efeitos da cibersegurança.
5. Compreender os requisitos de confidencialidade, integridade e disponibilidade e conhecer as técnicas de criptografia atuais e emergentes.
6. Conhecer diferentes classes de ataques (passivo, ativo, interno, distribuído) e os riscos e vulnerabilidades de segurança emergentes.
7. Conhecer diferentes tipos de bases de dados, as suas vantagens e desvantagens comparativas.
8. Conhecer recursos criptográficos de segurança em bases de dados.

Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:
1. Demonstrar possuir um domínio de nível intermédio das tecnologias de informação e comunicação.
2. Demonstrar ter conhecimentos de sistemas operativos e as suas interfaces de linha de comando.
3. Demonstrar ter conhecimentos básicos de redes de comunicação, endereços IP e portos.

Conteúdo da unidade curricular

Introdução à programação.
Repositórios de código para versionamento e partilha.
Mecanismos criptográficos para proteção da informação.
Bibliotecas criptográficas para o desenvolvimento de software.
Autenticação e Autorização.
Bases de dados relacionais e não relacionais e técnicas para garantir confidencialidade, integridade e disponibilidade.
Análise de listas de vulnerabilidade típicas em software (CWE) e de listas de software com vulnerabilidades (CVE).
Relatórios de riscos de segurança emergentes.

Conteúdo da unidade curricular (versão detalhada)

1. Introdução à programação.
   - Variáveis, tipos, operações de controlo de fluxo, entrada e saída, funções, variáveis de ambiente.
   - Leitura e escrita de ficheiros.
   - Bibliotecas para comunicação com processos remotos.
2. Repositórios de código para versionamento e partilha.
3. Mecanismos criptográficos para proteção da informação.
   - Cifra simétrica e assimétrica, MAC e assinatura digital.
   - Certificados e infraestruturas de chave pública.
4. Bibliotecas criptográficas para o desenvolvimento de software.
5. Autenticação e Autorização.
   - Armazenamento de palavras-passe.
   - Modelos e políticas de segurança.
6. Bases de dados relacionais e não relacionais.
   - Introdução às bases de dados relacionais e não relacionais.
   - Técnicas para garantir confidencialidade, integridade e disponibilidade em bases de dados.
7. Vulnerabilidades em software.
   - Análise de listas de vulnerabilidade típicas em software (CWE).
   - Análise de listas de software com vulnerabilidades (CVE).
   - Relatórios de riscos de segurança emergentes (ENISA, OWASP Top 10).

Bibliografia recomendada

1. Slides da Unidade Curricular
2. “Computer Security: Principles and Practice”, William Stallings and Lawrie Brown, Pearson, 2021. ISBN 9781292220611
3. “Python Crash Course (2nd Edition): A Hands-On, Project-Based Introduction to Programming”, Eric Mattes, No Starch Press, 2019. ISBN 9781593279288

Métodos de ensino e de aprendizagem

Ensino teórico-prático, distribuído por 8 sessões a que correspondem 35 horas de contacto. O tempo total de trabalho do formando previsto é de 54 horas. As aulas de carácter teórico destinam-se à exposição e discussão dos principais conteúdos programáticos, incentivando a interatividade e colocação de questões.
Os tópicos são ainda explorados através da realização de laboratórios práticos.

Alternativas de avaliação

- Avaliação Final - (Ordinário, Trabalhador) (Final, Recurso)
  - Exame Final Escrito - 50%
  - Trabalhos Práticos - 50%

Língua em que é ministrada

Português

Este documento só tem validade académica depois de autenticado, em todas as suas folhas, com o selo a óleo da Instituição.

Validação Eletrónica

Nuno Gonçalves Rodrigues	José Luís Padrão Exposto	José Carlos Rufino Amaro
03-07-2024	04-07-2024	04-07-2024

Este documento só tem validade académica depois de autenticado, em todas as suas folhas, com o selo a óleo da Instituição.