



Escola Superior de Tecnologia e Gestão

Designação	Cibersegurança
------------	----------------

Área de Formação (CNAEF)	ECTS	Nível EQF
481 – Ciências Informáticas	3	6

	Presenciais	Online - síncronas	Online - assíncronas	TOTAL
Horas de contacto	8	24		32
Horas de trabalho autónomo				52
Horas TOTAIS				84

Público a que se destina	- Jovens e adultos com formação de base em áreas não CTEAM
Vagas (se aplicável)	

1. Equipa docente/ Equipa de Formação

	nome	email	Science ID
Responsável científico IPVC	Silvestre Malta	smalta@estg.ipvpc.pt	5D1C-FC16-564D
Docentes; Formadores/as	Paulo Vaz Pedro Carneiro	vazpaulo@estg.ipvpc.pt pedrocarneiro@estg.ipvpc.pt	

2. Resumo

Esta microcredencial explora os princípios fundamentais da cibersegurança e o seu impacto no mundo digital, proporcionando aos estudantes um entendimento essencial sobre como manter a segurança online. Os participantes irão identificar e descrever as vulnerabilidades e ameaças digitais mais comuns, bem como aprender estratégias e boas práticas para proteger dados e sistemas. Além disso, será analisado como as organizações podem reforçar a sua defesa contra ciberataques. Por fim, os estudantes terão acesso a recursos informativos para explorar diferentes percursos profissionais na área da cibersegurança.

3. Objetivos de aprendizagem

1. Explorar os princípios fundamentais para manter a segurança online, incluindo o conceito de cibersegurança e o seu impacto potencial.
2. Identificar e descrever os tipos mais comuns de vulnerabilidades e ameaças digitais.
3. Explicar estratégias e boas práticas para garantir a segurança num ambiente online.
4. Analisar como as organizações podem proteger as suas operações contra ciberataques.



5. Aceder e utilizar diversos recursos informativos para explorar diferentes percursos profissionais na área da cibersegurança.

4. Conteúdos

Introdução à Cibersegurança; Ataques, Técnicas e Conceitos; Proteção de Dados e Privacidade; Proteção da Organização; Carreira em Cibersegurança

5. Metodologias de ensino e aprendizagem

Apresentação teórica dos conceitos, complementada com demonstrações e resolução de exercícios práticos.

Período não presencial: Realização de atividades práticas, estudo individual e em grupo sobre os conteúdos abordados.

6. Avaliação

- Trabalhos Práticos - 40%
- Prova Escrita - 60%

7. **Bibliografia** (Deve optar apenas por uma norma de referência bibliográfica: ex. APA 6ª edição, Vancouver ou NP 405)

Cisco Networking Academy, Introduction to Cybersecurity; Cisco Networking Academy, Cybersecurity Essentials; A. Zúquete, "Segurança em Redes Informáticas - 6 ed", FCA, 2021

Aprovação em CTC (data):

(parecer)