

# Ficha Técnica - CompTIA Security+

---

**Designação:** CompTIA Security+ – Fundamentos e Práticas de Cibersegurança

**Área de Formação:** Tecnologias de Informação

**Subárea:** Cibersegurança | Segurança da Informação | Redes e Sistemas

**Nível:** Intermédio

**Regime:** Teórico-Prático

**Carga Horária:** 60 horas

**Modalidade:** Presencial / Online / Híbrida

## **Público-Alvo**

- Técnicos de Informática
- Técnicos de Redes
- Técnicos de Telecomunicações
- Técnicos de Suporte
- Administradores de Sistemas
- Administradores de Redes
- Técnicos de Segurança Informática
- Profissionais de TI
- Estudantes de Informática e Telecomunicações
- Profissionais que pretendam iniciar carreira em Cibersegurança
- Profissionais que pretendam preparar-se para a CompTIA Security+

## **Pré-Requisitos**

- Conhecimentos básicos de informática;
- Conhecimentos básicos de sistemas operativos;
- Conhecimentos básicos de redes TCP/IP são recomendados;
- Noções de administração de sistemas constituem uma vantagem;
- Não é obrigatório possuir experiência profissional em cibersegurança.

## **Objetivo Geral**

Capacitar os formandos para identificar ameaças e vulnerabilidades, implementar mecanismos de proteção, administrar controlos de segurança e responder a incidentes em redes, sistemas, dispositivos, aplicações e ambientes cloud.

## **Objetivos Específicos**

1. Identificar ameaças, vulnerabilidades, riscos e diferentes tipos de ataques cibernéticos.
2. Implementar mecanismos de segurança em redes, sistemas, dispositivos e ambientes cloud.
3. Aplicar técnicas de autenticação, controlo de acesso, criptografia e proteção de dados.
4. Monitorizar ambientes tecnológicos, identificar incidentes e aplicar procedimentos de resposta e recuperação.
5. Desenvolver e implementar medidas de segurança através de um projeto prático integrado.

## DISTRIBUIÇÃO DA CARGA HORÁRIA

| Módulo       | Tema                                             | Carga Horária |
|--------------|--------------------------------------------------|---------------|
| 1            | Fundamentos de Cibersegurança                    | 5h            |
| 2            | Ameaças, Vulnerabilidades e Ataques              | 6h            |
| 3            | Segurança de Redes e Infraestruturas             | 6h            |
| 4            | Arquitetura e Segurança de Sistemas              | 5h            |
| 5            | Identidade, Autenticação e Controlo de Acesso    | 5h            |
| 6            | Segurança de Dados e Criptografia                | 5h            |
| 7            | Segurança na Cloud e Ambientes Modernos          | 4h            |
| 8            | Segurança de Aplicações e Desenvolvimento Seguro | 4h            |
| 9            | Operações de Segurança e Monitorização           | 5h            |
| 10           | Resposta a Incidentes e Forense                  | 4h            |
| 11           | Gestão de Riscos, Governança e Conformidade      | 4h            |
| 12           | Segurança Física, Continuidade e Projeto Prático | 7h            |
| <b>Total</b> |                                                  | <b>60h</b>    |

## Certificação

- Frequência mínima de **75% da carga horária**;
- Aproveitamento mínimo de **70% na avaliação**