

Ficha Técnica - CompTIA Security+

Designação

CompTIA Security+ – Segurança Informática, Defesa de Redes, Gestão de Riscos e Protecção de Sistemas [Exame Incluído].

Área

Tecnologias de Informação e Comunicação (TIC).

Subárea

Cibersegurança | Segurança de Redes | Segurança de Sistemas | Gestão de Riscos | Protecção de Dados | Resposta a Incidentes.

Nível

Intermédio.

Carga Horária

60 horas.

Modalidade

Presencial, online ou híbrida.

Regime

Pós-laboral ou adaptável à disponibilidade dos formandos.

Objectivo Geral

Capacitar os formandos para compreender, implementar e avaliar medidas fundamentais de cibersegurança, desenvolvendo competências em protecção de redes e sistemas, gestão de identidades, criptografia, análise de riscos, monitorização e resposta a incidentes, em alinhamento com os objectivos da certificação CompTIA Security+.

Objectivos Específicos

No final da formação, os formandos deverão ser capazes de:

1. Explicar os princípios fundamentais de confidencialidade, integridade e disponibilidade da informação.
2. Identificar ameaças, vulnerabilidades e riscos que afectam sistemas e redes.
3. Aplicar conceitos básicos de segurança de redes e protecção de infra-estruturas.
4. Compreender mecanismos de autenticação, autorização e gestão de identidades.
5. Aplicar conceitos de criptografia, certificados digitais e protecção de dados.
6. Identificar medidas de segurança para sistemas operativos, aplicações e ambientes cloud.
7. Compreender processos de avaliação de vulnerabilidades e gestão de riscos.
8. Interpretar registos e alertas para reconhecer potenciais incidentes de segurança.
9. Aplicar procedimentos básicos de resposta a incidentes e recuperação de sistemas.
10. Resolver exercícios e cenários de preparação para o exame oficial CompTIA Security+.

Módulos da Formação

Nº	Módulo	Carga Horária
1	Conceitos Fundamentais de Cibersegurança	10 horas
2	Segurança de Redes e Infra-estruturas	10 horas
3	Gestão de Identidades, Acessos e Criptografia	10 horas
4	Segurança de Sistemas, Aplicações e Cloud	10 horas
5	Gestão de Riscos, Monitorização e Resposta a Incidentes	10 horas
6	Laboratórios Integrados e Preparação para o Exame	10 horas
	Total	60 horas

Público-Alvo

- Técnicos de informática e suporte técnico.
- Técnicos de redes e administradores de sistemas.
- Profissionais de segurança informática.
- Técnicos de suporte a infra-estruturas cloud.
- Estudantes e recém-formados em Informática e Telecomunicações.
- Profissionais que pretendam iniciar uma carreira em cibersegurança.
- Técnicos que pretendam aprofundar conhecimentos de segurança de redes e sistemas.

Pré-Requisitos

- Conhecimentos básicos de informática e sistemas operativos.
- Noções de redes informáticas, endereçamento IP e protocolos.
- Familiaridade com conceitos de hardware e software.
- Conhecimentos básicos de administração de sistemas recomendados.
- Computador com acesso à Internet para a realização de laboratórios.

Recomenda-se experiência prévia em redes ou suporte técnico. A formação é mais proveitosa quando os participantes já compreendem os fundamentos de sistemas operativos e conectividade.

Metodologia

Serão utilizadas as seguintes metodologias:

- Aulas expositivas e demonstrações orientadas.
- Laboratórios de configuração segura de sistemas.
- Exercícios de análise de ameaças e vulnerabilidades.
- Estudos de caso de incidentes de segurança.
- Interpretação de registos e alertas.
- Simulações de gestão de riscos e resposta a incidentes.
- Questionários e simulados de preparação para o exame.
- Projecto prático final de avaliação da segurança de um ambiente simulado.

CrITÉrios de Avaliação

- Participação e assiduidade — 20%
- Exercícios e actividades práticas — 30%
- Projecto prático final — 50%
- Total — 100%

Certificação

Certificado de Aproveitamento mediante:

- Frequência mínima de **75%**.
- Aproveitamento mínimo de **70%**.