CompTIA Security+ CertPrep (e-Learning)

CompTIA

- **Nível:** Avançado
- **Duração:** h

Sobre o curso

Prepara-te para a certificação CompTIA Security+ e desenvolve competências em cibersegurança.

O curso **CompTIA Security+ CertPrep** fornece os conhecimentos fundamentais para planear, implementar e manter práticas de segurança da informação, numa abordagem independente de fornecedor. A formação aborda temas essenciais como gestão de riscos, segurança de hosts e redes, autenticação, controlo de acessos, criptografia, segurança organizacional e resposta a incidentes. O curso está alinhado com os objetivos do exame de certificação **CompTIA Security+**.

A certificação **CompTIA Security+** é reconhecida como uma das certificações de referência para profissionais que pretendem iniciar ou consolidar uma carreira em segurança de TI. Representa um nível essencial de validação de competências para funções de segurança acima do nível inicial.

Ao longo deste curso, os participantes desenvolvem os conhecimentos necessários para se prepararem para o exame e adquirem competências práticas para evoluir para funções de segurança de nível intermédio.

O exame de certificação **CompTIA Security+** comprova que o candidato aprovado possui os conhecimentos e competências necessários para avaliar a postura de segurança de um ambiente empresarial, recomendar e implementar soluções de segurança adequadas, monitorizar e proteger ambientes híbridos, incluindo cloud, dispositivos móveis e IoT, atuar de acordo com leis e políticas aplicáveis, incluindo princípios de governance, risco e conformidade, e identificar, analisar e responder a eventos e incidentes de segurança.

Este curso e-learning inclui:

- **Conteúdos formativos estruturados em e-learning:** Aprende e desenvolve competências de forma eficiente e autónoma, com conteúdos estruturados através de um modelo de progressão da aprendizagem. Este modelo ajuda-te a compreender conceitos e a desenvolver competências alinhadas com os objetivos do curso.
- **Vídeos e conteúdos interativos integrados:** Acede a explicações, demonstrações e exemplos no momento em que são mais relevantes para a tua aprendizagem.
- **Atividades em laboratório:** Realiza exercícios práticos em ambientes simulados e reais, com cenários

próximos do contexto profissional e tarefas de nível básico e avançado.
- **Assessments e testes de preparação:** Valida os teus conhecimentos ao longo do curso através de avaliações e testes práticos.
- **Voucher de exame e retake:** Inclui voucher de exame de certificação e a possibilidade de repetição em caso de reprovação.

Diagnóstico de Conhecimentos

- Faça a nossa avaliação gratuita para verificar se detém os os conhecimentos base para garantir uma boa aprendizagem neste curso.

Destinatários

- Administradores de Redes
- Cybersecurity Associates
- Profissionais da área das TI interessados em iniciar uma carreira em cibersegurança

---

Objetivos

- Possuir conhecimentos e competências para avaliar a postura de segurança de um ambiente empresarial e recomendar e implementar soluções de segurança adequadas
- Monitorizar e proteger ambientes híbridos, incluindo cloud, dispositivos móveis e IoT
- Atuar com consciência e de acordo com os regulamentos e políticas aplicáveis, incluindo princípios de governança, risco e conformidade
- Identificar, analisar e responder a eventos e incidentes de segurança, preparando os candidatos para o exame de certificação CompTIA Security+.

Condições

Notas

Após a formação, é possível adquirir, na Rumos, o exame de certificação do parceiro oficial com 10% de desconto.
Oferta válida até 6 meses após a conclusão do curso nas modalidades live training ou presencial.

Para particulares
• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes

do início do curso.
• Possibilidade de pagamento faseado.
• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).
• Isenção de IVA para particulares.

Para empresas

• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).
• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

- Este curso pressupõe conhecimentos de nível básico na utilização e manutenção de workstations individuais.
- Os participantes deverão possuir as certificações CompTIA A+ (ou ter experiência equivalente) e CompTIA Network+ (ou ter experiência equivalente) e 2-3 anos de experiência em redes.

Metodologia

e-learning

Programa

- Síntese dos Conceitos Fundamentais de Segurança
- Comparação entre Tipos de Ameaças
- Explicação de Soluções Criptográficas
- Implementação de Gestão de Identidade e de Acesso
- Proteção da Arquitetura de Redes Empresariais
- Proteção da Arquitetura de Redes na Cloud
- Explicação de Conceitos de Resiliência e de Segurança de Sítios
- Explicação da Gestão de Vulnerabilidades
- Avaliação das Capacidades de Segurança de Redes
- Avaliação das Capacidades de Segurança de Endpoints
- Melhoria das Capacidades de Segurança de Aplicações
- Explicação de Conceitos de Resposta a Incidentes e Monitorização
- Análise dos Indicadores de Atividade Maliciosa
- Síntese dos Conceitos de Governança de Segurança
- Explicação dos Processos de Gestão de Riscos
- Síntese dos Conceitos de Proteção de Dados e Conformidade

Síntese dos Conceitos Fundamentais de Segurança

- Conceitos de Segurança
- Controlos de Segurança

Comparação entre Tipos de Ameaças

- Atores de Ameaça
- Superfícies de Ataque
- Engenharia Social

Explicação de Soluções Criptográficas

- Algoritmos Criptográficos
- Infraestrutura de Chave Pública (PKI)
- Soluções Criptográficas

Implementação de Gestão de Identidade e de Acesso

- Autenticação
- Autorização
- Gestão de Identidade

Proteção da Arquitetura de Redes Empresariais

- Arquitetura de Redes Empresariais
- Dispositivos de Segurança de Rede
- Comunicações Seguras

Proteção da Arquitetura de Redes na Cloud

- Infraestrutura da Cloud
- Sistemas Embebidos e Arquitetura Zero Trust

Explicação de Conceitos de Resiliência e de Segurança de Sítios

- Gestão de Ativos
- Estratégias de Redundância
- Segurança Física

Explicação da Gestão de Vulnerabilidades

- Vulnerabilidades de Dispositivos e Sistemas Operativos
- Vulnerabilidades de Aplicações e Cloud
- Métodos de Identificação de Vulnerabilidades
- Análise e Remediação de Vulnerabilidades

Avaliação das Capacidades de Segurança de Redes

- Padrões de Segurança de Redes
- Melhoria das Capacidades de Segurança de Redes

Avaliação das Capacidades de Segurança de Endpoints

- Implementar Segurança de Endpoints

- Fortalecimento de Dispositivos Móveis

Melhoria das Capacidades de Segurança de Aplicações

- Padrões de Segurança de Protocolos de Aplicações
- Conceitos de Segurança de Aplicações Cloud e Web

Explicação de Conceitos de Resposta a Incidentes e Monitorização

- Resposta a Incidentes
- Forense Digital
- Fontes de Dados
- Ferramentas de Alerta e Monitorização

Análise dos Indicadores de Atividade Maliciosa

- Indicadores de Ataque de Malware
- Indicadores de Ataque Físico e de Rede
- Indicadores de Ataque a Aplicações

Síntese dos Conceitos de Governança de Segurança

- Políticas, Normas e Procedimentos
- Gestão de Alterações
- Automação e Orquestração

Explicação dos Processos de Gestão de Riscos

- Processos e Conceitos de Gestão de Riscos
- Conceitos de Gestão de Fornecedores
- Auditorias e Avaliações

Síntese dos Conceitos de Proteção de Dados e Conformidade

- Classificação de Dados e Conformidade
- Políticas de Pessoal