Rumos valorizamos profissionais!

# CompTIA Security+ CertPrep (CSeg+)

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Live Training
- **Com certificação:** CompTIA Security+
- **Data:** 22 Fev. 2021 a 26 Fev. 2021
- **Preço:** 2150€
- **Horário:** Laboral - das 09h30 às 16h30
- **Nível:** Intermédio
- **Duração:** 35 horas

Este curso destina-se a dar uma panorâmica geral de segurança de redes e da sua relação com outras áreas das TI. Serve como introdução genérica a este tema ou como estágio inicial para estudos mais especializados em segurança. Ao longo do curso será possível distinguir mais claramente as áreas funcionais associadas às funções de segurança da informação.

Logo nos primeiros módulos, aos alunos terão oportunidade de realizar atividades práticas com ferramentas e software de segurança cibernética, antes de prosseguir com os conceitos de gestão de identidade e acesso à infraestrutura, e design do sistema de segurança. O curso termina com conceitos de gestão de risco, desenvolvimento seguro de software e políticas organizacionais de segurança.

Este curso vai ajudar na preparação dos formandos para o exame de certificação CompTIA Security+ SY0-601. De salientar que a frequência do curso não é suficiente para preparar um formando para qualquer exame CompTIA.

***O curso inclui o respetivo exame de certificação.***

Este curso também está disponível no formato E-learning. Para mais informações aceda ao link: CompTIA Security+

## Destinatários

- Administradores de Redes e Sistemas
- Profissionais de TI interessados em seguir uma carreira na área de Cibersegurança

## Pré-requisitos

- Certificação CompTIA A+
- Certificação CompTIA Network+
- Experiência de Windows 7/8

É importante que os formandos tenham o nível recomendado de experiência de trabalho em TI antes de fazerem o exame. Para a certificação CompTIA Security+ é recomendado ter pelo menos 2 anos de experiência de administração de sistemas focados na segurança.

---

## Objectivos

No final da ação de formação os participantes deverão estar aptos a:

- Identificar conceitos fundamentais de segurança informática.
- Identificar ameaças e vulnerabilidades de segurança em:
    - redes
    - aplicações, dados e máquinas
    - controlo de acessos, autenticação e gestão de contas
    - gestão de certificados
- Lidar com questões de cumprimento de regras e normas de operação
- Identificar problemas de gestão do risco
- Gerir incidentes de segurança
- Contribuir para o planeamento da continuação do negócio da recuperação de desastres

---

## Metodologia

Este curso está disponível na modalidade:

- Presencial
- Live Training
- E-Learning

---

## Programa

**Comparing and Contrasting Attacks**

- Compare and Contrast Information Security Roles
- Explain Threat Actor Types
- Compare and Contrast Social Engineering Attack Types
- Determine Malware Types

**Comparing and Contrasting Security Controls**

- Compare and Contrast Security Control and Framework Types
- Follow Incident Response Procedures

**Using Security Assessment Tools**

- Explain Penetration Testing Concepts
- Use Topology Discovery Software Tools
- Use Fingerprinting and Sniffing Software Tools
- Use Vulnerability Scanning Software Tools

**Comparing and Contrasting Basic Concepts of Cryptography**

- Compare and Contrast Basic Concepts of Cryptography
- Compare and Contrast Cryptographic Attack Types
- Explain Hashing and Symmetric Cryptographic Algorithms
- Explain Asymmetric Cryptographic Algorithms

**Implementing Public Key Infrastructure**

- Implement Certificates and Certificate Authorities
- Implement PKI Management

**Implementing Identity and Access Management Controls**

- Compare and Contrast Identity and Authentication Concepts
- Install and Configure Authentication Protocols
- Implement Multifactor Authentication

**Managing Access Services and Accounts**

- Install and Configure Authorization and Directory Services
- Implement Access Management Controls
- Differentiate Account Management Practices
- Implement Account Auditing and Recertification

**Implementing Secure Network Architecture Concepts**

- Implement Secure Network Architecture Concepts
- Install and Configure Secure Switching Infrastructure
- Install and Configure Network Access Control
- Install and Configure Secure Routing and NAT Infrastructure

**Installing and Configuring Security Appliances**

- Install and Configure Firewalls and Proxies
- Install and Configure Load Balancers
- Install and Configure Intrusion Detection/Prevention Systems

- Install and Configure Logging and SIEM Systems

**Installing and Configuring Wireless and Physical Access Security**

- Install and Configure Wireless Infrastructure
- Install and Configure Wireless Security Settings
- Explain the Importance of Physical Security Controls

**Deploying Secure Host, Embedded, and Mobile Systems**

- Implement Secure Hardware Systems Design
- Implement Secure Host Systems Design
- Implement Secure Embedded Systems Design
- Implement Secure Mobile Device Systems Design

**Implementing Secure Network Access Protocols**

- Implement Secure Network Operations Protocols
- Implement Secure Remote Access Protocols
- Implement Secure Remote Administration Protocols

**Implementing Secure Network Applications**

- Implement Secure Web Services
- Implement Secure Communications Services
- Implement Secure Virtualization Infrastructure
- Implement Secure Cloud Services

**Explaining Risk Management and Disaster Recovery Concepts**

- Explain Risk Management Processes and Concepts
- Explain Disaster Recovery Planning Concepts
- Explain Resiliency and Continuity of Operations Strategies
- Summarize Basic Concepts of Forensics

**Summarizing Secure Application Development Concepts**

- Explain the Impact of Vulnerability Types
- Summarize Secure Application Development Concepts

**Explaining Organizational Security Concepts**

- Explain the Importance of Security Policies
- Implement Data Security and Privacy Practices
- Explain the Importance of Personnel Management