



## CompTIA Security+ CertPrep (Cseg+)

CompTIA

- **Nível:** Avançado
  - **Duração:** 35h
- 

### Sobre o curso

**Prepare for the CompTIA Security+ certification while building your cybersecurity knowledge, skills, and abilities.**

The Security+ Certification Prep Course provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security. This course maps to the CompTIA Security+ certification exam (SY0-701).

#### **What is Security+ Certification?**

The Security+ certification is considered to be the minimum level of certification for all IT security positions beyond entry-level. This course delivers the core knowledge required to pass the exam and the skills necessary to advance to an intermediate-level security job.

The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents.

---

### Destinatários

- Network Administrators
  - Cybersecurity Associates
  - IT personnel interested in pursuing a career in cybersecurity
-

## Condições

Após a formação, é possível adquirir, o exame de certificação do parceiro oficial com 10% de desconto. Oferta válida até 6 meses após a conclusão do curso.

---

## Pré-requisitos

- Network Administrators
- Cybersecurity Associates
- IT personnel interested in pursuing a career in cybersecurity

### Diagnóstico de Conhecimentos:

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

## Programa

- Summarize Fundamental Security Concepts
- Compare Threat Types
- Explain Cryptographic Solutions
- Implement Identity and Access Management
- Secure Enterprise Network Architecture
- Secure Cloud Network Architecture
- Explain Resiliency and Site Security Concepts
- Explain Vulnerability Management
- Evaluate Network Security Capabilities
- Assess Endpoint Security Capabilities
- Enhance Application Security Capabilities
- Explain Incident Response and Monitoring Concepts
- Analyze Indicators of Malicious Activity
- Summarize Security Governance Concepts
- Explain Risk Management Processes
- Summarize Data Protection and Compliance Concepts

### Summarize Fundamental Security Concepts

- Security Concepts
- Security Controls

### Compare Threat Types

- Threat Actors
- Attack Surfaces

- Social Engineering

### **Explain Cryptographic Solutions**

- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

### **Implement Identity and Access Management**

- Authentication
- Authorization
- Identity Management

### **Secure Enterprise Network Architecture**

- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications

### **Secure Cloud Network Architecture**

- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture

### **Explain Resiliency and Site Security Concepts**

- Asset Management
- Redundancy Strategies
- Physical Security

### **Explain Vulnerability Management**

- Device and OS Vulnerabilities
- Application and Cloud Vulnerabilities
- Vulnerability Identification Methods
- Vulnerability Analysis and Remediation

### **Evaluate Network Security Capabilities**

- Network Security Baselines
- Network Security Capability Enhancement

### **Assess Endpoint Security Capabilities**

- Implement Endpoint Security
- Mobile Device Hardening

### **Enhance Application Security Capabilities**

- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

### **Explain Incident Response and Monitoring Concepts**

- Incident Response
- Digital Forensics
- Data Sources
- Alerting and Monitoring Tools

### **Analyze Indicators of Malicious Activity**

- Malware Attack Indicators
- Physical and Network Attack Indicators
- Application Attack Indicators

### **Summarize Security Governance Concepts**

- Policies, Standards, and Procedures
- Change Management
- Automation and Orchestration

### **Explain Risk Management Processes**

- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments

### **Summarize Data Protection and Compliance Concepts**

- Data Classification and Compliance
- Personnel Policies