CompTIA Security+ CertPrep (CSeg+)

- **Formato do curso:** Presencial
- **Com certificação:** CompTIA Security+
- **Preço:** 1250€
- **Nível:** Intermédio
- **Duração:** 30 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.

Este curso vai ajudar na preparação dos formandos para o exame de certificação CompTIA Security+ SY0-501. 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.

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 quanstões 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

---

Programa

Mitigating threats

- Core system maintenance
- Virus and spyware management
- Browser security
- Social engineering threats

Cryptography

- Symmetric cryptography
- Public key cryptography

Authentication systems

- Authentication
- Hashing
- Authentication systems

Messaging security

- E-mail security
- Messaging and peer-to-peer security

User and role based security

- Security policies
- Securing file and print resources

Public key infrastructure

- Key management and life cycle
- Setting up a certificate server
- Web server security with PKI

Access security

- Biometric systems
- Physical access security
- Peripheral and component security

- Storage device security

Ports and protocols

- TCP/IP review
- Protocol-based attacks

Network security

- Common network devices
- Secure network topologies
- Browser-related network security
- Virtualization

Wireless security

- Wi-Fi network security
- Non-PC wireless devices

Remote access security

- Remote access
- Virtual private networks

Auditing, logging, and monitoring

- System logging
- Server monitoring

Vulnerability testing

- Risk and vulnerability assessment
- IDS and IPS
- Forensics

Organizational security

- Organizational policies
- Education and training
- Disposal and destruction

Business continuity

- Redundancy planning
- Backups
- Environmental controls