

## Academia Técnico de Segurança

Possibilidade de pagamento faseado, sem juros, até 6 vezes.

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Lisboa
- **Com certificação:** CompTIA Security+
- **Data:** 23 Nov. 2020 a 13 Mar. 2021
- **Preço:** 2050€
- **Horário:** Pós-laboral - 2ª a 6ª, das 18h45 às 22h15
- **Duração:** 126 horas

Este percurso, visa criar profissionais de TI com as competências e experiência necessária para identificar ameaças e vulnerabilidades de segurança, configurar soluções que permitam reduzir a superfície de ataque de servidores, clientes, dispositivos de rede, sistemas industriais e dispositivos móveis, bem como a implementação diferentes tipos de metodologias de hardening.

### Condições Financeiras

- Taxa de inscrição: 220€, dedutível no valor total.
- Possibilidade de pagamento faseado para particulares, **até 6 prestações, sem juros.**
- Estudantes não residentes no território nacional, terão de efetuar um pagamento de 50% do valor total da propina no momento da inscrição.
- Os valores apresentados não incluem IVA. Isenção do valor do IVA a particulares.
- Para informações completas sobre os requisitos, descontos e condições financeiras disponíveis, contacte-nos através do [formacao@rumos.pt](mailto:formacao@rumos.pt) ou do botão Saber Mais.

### Porque quero frequentar esta Academia?

- 2 Certificações reconhecidas Internacionalmente.
- Os melhores profissionais certificados do mercado como formadores.
- Formação qualificada, através da Rumos. Uma das empresas líderes na área da formação.

### Que Certificações vou obter?

- Microsoft Technology Associate (MTA): Security Fundamentals
- CompTIA Security+

## Que profissões me esperam?

- Técnico de Segurança da Informação
  - Information Assurance Junior Assessor
  - Consultor de Segurança da Informação Júnior
- 

## Destinatários

- Destina-se a todos os interessados em aprofundar conhecimentos e desenvolver competências na área de Segurança de Redes e Sistemas, para consolidar uma carreira especializada em Segurança de Informação.
  - Profissionais que pretendam investir ou mudar de carreira.
- 

## Pré-requisitos

- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa
  - Privilegiam-se conhecimentos técnicos de informática e redes, ao nível dos conhecimentos que se adquirem na Academia [Técnico de Informática](#)
  - A Academia não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional
- 

## Metodologia

Constituído por 5 módulos de formação, integrados numa ótica de sessões mistas de teoria e prática. Cada módulo é constituído por um período de formação presencial e acompanhamento permanente e personalizado por parte de um formador. Serão elaborados exercícios e simulações de situações práticas com resolução individualizada garantindo uma aprendizagem mais eficaz. Os conteúdos ministrados durante o percurso foram desenvolvidos pela Rumos e Organizações parceiras, e são devidamente acompanhados por manuais, distribuídos aos Participantes.

### **Composição:**

- 126 Horas de Formação
  - 4 Ações de Formação TI
  - 1 Seminário Técnico
  - 2 Modulos e-Learning
  - 1 Ação de Formação Complementar
  - 2 Ações de Preparação para Exame
  - 2 Exames de Certificação
-

# Programa

## **Fundamentos de Segurança e Informática**

Tem como objetivo preparar os formandos com os conhecimentos fundamentais nas principais áreas da informática, em particular no que toca à instalação de sistemas operativos e segurança de sistemas de informação.

Conteúdo:

- Introdução à temática da segurança
- Evolução e antecedentes históricos
- Panorâmica geral sobre a situação atual
- Hardware
- Sistemas Operativos
- Virtualização e Cloud Computing
- Criação de máquinas virtuais em Hyper-V e VBox
- Utilização prática dos dois hipervisores
- Criptografia
- Redes de computadores

## **Security Fundamentals (e-Learning)**

Tem como objetivo preparar os formandos na consolidação de conhecimentos elementares e essenciais na área de Cyber segurança por forma a melhor preparar os formandos para o exame da Microsoft 98-367.

Conteúdo:

- Understanding Security Layers
- Authentication, Authorization, and Accounting
- Understanding Security Policies
- Understanding Network Security
- Protecting the Server and Client

## **Seminário: Powershell and Scripting**

Dotar os formandos com os conceitos básicos e essenciais em Powershell e em Scripting

## **CompTIA Security+**

Este modulo destina-se a dar uma panorâmica geral de segurança de redes e da sua relação com outras áreas das TI ao mesmo tempo que prepara os formandos com os conhecimentos necessários para fazerem o exame de certificação CompTIA.

Conteúdo:

- Comparing and Contrasting Attacks
- Comparing and Contrasting Security Controls
- Using Security Assessment Tools

- Comparing and Contrasting Basic Concepts of Cryptography
- Implementing Public Key Infrastructure
- Implementing Identity and Access Management Controls
- Managing Access Services and Accounts
- Implementing Secure Network Architecture Concepts
- Installing and Configuring Security Appliances
- Installing and Configuring Wireless and Physical Access Security
- Deploying Secure Host, Embedded, and Mobile Systems
- Implementing Secure Network Access Protocols
- Implementing Secure Network Applications
- Explaining Risk Management and Disaster Recovery Concepts
- Summarizing Secure Application Development Concepts
- Explaining Organizational Security Concepts

### **Ação de Preparação para Exame MTA**

Tem como objetivo preparar os formandos o exame 98-367 da Microsoft que permitirá alcançar a certificação MTA Security Fundamentals.

### **Hardening de Sistemas**

Trabalhar competências com vista a melhorar a segurança das infraestruturas de servidor, rede e demais dispositivos através de uma variedade de listas de verificação, guias, benchmarks e testes que resultam em um ambiente muito mais seguro.

Conteúdos:

- Introduction to Hardening
- Standards and Frameworks
- Vulnerability Assessment and tools
- Network Infrastructure hardening
- Windows Client hardening
- Windows Server hardening
- Linux hardening
- Testing System's Hardening

### **Introduction to Python: Fundamentals (e-Learning)**

Dotar os formandos com os conceitos essenciais em programação orientada a objetos, utilizando a linguagem Python, de forma a ficarem com as bases de uma linguagem de programação para posterior análise de vulnerabilidades:

Conteúdos:

- Python 3 fundamentals
- Strings and List manipulation
- Methods to Iterate through strings, lists and ranges
- Creating, reading and writing to files

## **Segurança no desenvolvimento de Software**

Dotar os formandos com os conceitos essenciais para analisar, identificar e mitigar vulnerabilidades no desenvolvimento de software

Conteúdos:

- Conhecer conceitos-chave de segurança e tipos de ameaças mais frequentes
- Identificar técnicas de defesa e mitigação de riscos em contexto de desenvolvimento de software
- Compreender o ciclo de vida de desenvolvimento de software e neste contexto
- Identificar problemas na criação de aplicativos seguros

## **Noções básicas de direito + Lei do Cibercrime**

- Noções básicas de direito
- Lei do Cibercrime

## **Ação de Preparação para Exame CompTIA S+**

Tem como objetivo preparar os formandos o exame SY0-501 que permitirá alcançar a certificação CompTIA Security+