

## Academia Cyber Security

Possibilidade de pagamento faseado, sem juros, até 18 vezes.

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Porto
- **Data:** 23 Nov. 2020 a 15 Nov. 2021
- **Preço:** 6200€
- **Horário:** Pós-laboral - 2ª a 6ª, das 18h45 às 22h15
- **Duração:** 350 horas

A Academia de Cyber Security dá-lhe as competências técnicas necessárias para construir uma carreira sustentada na área da Segurança de Informação.

Ao longo do percurso as matérias, e respetivo nível, vão evoluindo. O percurso inicia com as temáticas da identificação de ameaças e vulnerabilidades de segurança, configuração de soluções que permitam reduzir a superfície de ataque de variados tipos de sistemas informáticos, bem como a implementação de diferentes tipos de metodologias de hardening. Aborda a importância da análise a Incidentes e alguns métodos para prevenção dos mesmos. Culmina de forma a proporcionar a experiência e credibilidade para projetar, implementar e gerir um programa de segurança da informação para proteger as organizações de crescentes ataques sofisticados.

### Condições Financeiras

- Taxa de inscrição: 290€, dedutível no valor total.
- Possibilidade de pagamento faseado para particulares, **até 18 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?

- Possibilidade de Estágio no final da formação.
- 6 Certificações reconhecidas Internacionalmente.
- Formação qualificada, através da Rumos. Uma das empresas líderes na área da formação.

## Que Certificações vou obter?

- MTA Security Fundamentals
- CompTIA Security+
- Certified Ethical Hacker
- CompTIA Cybersecurity Analyst+
- ISO/IEC 27001
- M\_o\_R (Management of Risk) Certification
- Certificação Rumos Expert (CRE): Auditor de Segurança

## Que profissões me esperam?

- Técnico de Segurança da Informação
- Information Assurance Junior Assessor
- Consultor de Segurança da Informação
- Administrador de Segurança da Informação
- Cyber Security Analyst
- Penetration Test Engineer
- Auditor de Segurança da Informação
- Information Security Officer
- Chief Information Security Officer

## Estágio

Esta academia inclui a possibilidade de estágio curricular de 3 meses, após a conclusão da formação mediante a realização dos exames de Certificação com aproveitamento.

## Coordenadores Técnicos

---

### Rui Natário

Trainer Cyber Security @ Rumos

---

### Hugo Rodrigues

Trainer CISCO, Microsoft & Security

---

### Pedro Machado

DPO @ Grupo Ageas Portugal

---

## 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.

---

## Pré-requisitos

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

---

## Objectivos

- Munir os participantes com os conhecimentos e experiência em configuração de equipamentos de networking e segurança (Switches, Firewalls, VPNs, IPS e Load Balancers) bem como a implementação soluções que permitam reduzir a superfície de ataque de servidores, clientes, dispositivos de rede, sistemas industriais e dispositivos moveis (AV, HIDS, SIEM, Threat Analytics, ...).
- Preparar Analistas de Segurança para desenhar e implementar soluções de monitorização, análise, prevenção de intrusões, firewalls, controle de acesso e alarmística. Lidar com sistemas críticos e criar planos de resposta a incidentes e recuperação de desastres. Desenvolver competências na resposta a novas ameaças. Realizar análise de vulnerabilidades e testes de intrusão de forma a testar as soluções implementadas.
- Preparar auditores para realização de testes de intrusão a ambientes com elevado nível de segurança, adotando a perspectiva de um adversário avançado como modo de operação, permitindo uma melhor identificação, quantificação e gestão do risco, melhorando os conhecimentos necessários para conduzir auditorias de acordo com os requisitos e normas existentes.

---

## Metodologia

- Constituído por 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 garantindo uma aprendizagem mais eficaz.
- Os conteúdos ministrados durante o percurso foram desenvolvidos pela Rumos, em consulta a Organizações parceiras, e são devidamente acompanhados por material didático, distribuídos aos Participantes.

## **Composição:**

- 10 Ações de Formação TI
- 1 Seminário Técnico
- 4 cursos e-Learning
- 2 ações de Formação Complementares
- 6 Ações de Preparação para Exame
- 6 Exames de Certificação
- 1 CFT
- 1 Projeto Prático

## **Exames de Certificação**

- 6 exames de certificação;
- Os exames de certificação deverão ser realizados no final dos respetivos módulos de formação;
- As datas são sugeridas pela Rumos, no entanto, a marcação é feita pelo formando no momento em que se sentir preparado para tal;
- A marcação deve ser efetuada com 4 dias úteis de antecedência à data pretendida;
- Os exames têm de ser realizados até 6 meses após a data de fim da formação.

## **Certificação Rumos**

Baseada em casos práticos da vida real dos profissionais, esta certificação permite demonstrar a detenção de conhecimentos e competências autênticos. Para isso, o formando é sujeito à realização de um projeto que é espelho das tarefas realizadas pelos profissionais no seu dia-a-dia.

O formando é presente a um exame prático sobre as matérias lecionadas e com avaliação presencial. Após avaliação positiva, este obterá um Certificado Rumos que atesta as competências na respetiva área.

---

## **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+

### **Fundamentos Kali Linux (e-Learning)**

Dotar os formandos de conhecimentos essencial em Kali Linux e utiliza-lo como ferramenta em testes de intrusão e de defesa a eventuais ataques.

Conteúdos:

- About Kali Linux
- Getting Started with Kali Linux
- Linux Fundamental
- Installing Kali Linux
- Configuring Kali Linux
- Helping Yourself and Getting Help
- Securing and Monitoring Kali Linux
- Debian Package Management
- Advanced Usage
- Kali Linux in the Enterprise
- Introduction to Security Assessments

### **Ethical Hacking and Countermeasures**

Dotar os formandos com os conceitos e técnicas de Ethical Hacking para poder defender de futuros possíveis ataques, aprendendo a verificar, testar Hackar e proteger os seus próprios sistemas. Aprenderá ainda a cinco fases do Ethical Hacking (Gaining Access, Enumeration, Maintaining Access, and covering your tracks).

Conteúdos:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection

- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

### **Offensive Penetration Testing Services**

Num curso completamente prático, irá ser permitido aos formandos com acompanhamento do formador, explorar e utilizar algumas das ferramentas mais utilizadas em Ethical Hacking por forma a terem um pleno conhecimento ao nível do que é feito em Red Teams.

Conteúdos:

- Using the Metasploit Framework
- Information Gathering
- Finding Vulnerabilities
- Capturing Traffic
- Exploitation
  - Password Attacks
  - Client-Side Exploitation
  - Social Engineering
- Post Exploitation
- Web Application Testing
- Wireless Attacks
  - Lab: Packet capture
  - Lab: Packet Injection
  - Lab: Rogue Access Point

### **Ação de Preparação para Exame CEH**

Tem como objetivo preparar os formandos o exame CEH da Ec-Council que permitirá alcançar a certificação de Ethical Hacking (CEH).

### **Case Event Analyst**

Capacitar os formandos para deteção, monitorização e resposta de anomalias que possam indicar comportamentos anómalos e de como uma análise pró-ativa através de uma contante monitorização, análise e prevenção poderá prever e evitar o ataque informático por completo.

Conteúdos

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment



## **Capture the Flag - CTF**

Desafio prático de grupo que servirá para testar os conhecimentos e raciocínio lógico dos formandos, ao mesmo tempo que permite que os mesmos apliquem Técnicas e Conceitos adquiridos nos módulos anteriores, tanto a nível de Red Team como a nível de Blue Team.

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

Tem como objetivo preparar os formandos o exame que permitirá alcançar a certificação CompTIA Cybersecurity Analyst (CySA+).

## **Information Security Management ISO/IEC 27001/27002**

Boas práticas para gestão de segurança da informação seguindo as normas internacionais ISO/IEC 27001/2, de forma a dotar os formandos com as competências necessárias para conseguirem implementar, manter e melhorar a gestão de segurança da informação numa organização.

Conteúdos:

- Introduction to the ISO 27000 standards family Introduction to management systems and the process approach
- General requirements of ISO/IEC 27002
- Implementation phases of the ISO/IEC 27002 framework
- Introduction to risk management according to ISO 27005
- Continual improvement of information security
- Conducting an ISO/IEC 27002 certification audit

## **Ação de Preparação para Exame EXIN ISO/IEC 27001**

Tem como objetivo preparar os formandos o exame da EXIN que permitirá alcançar a certificação ISO/IEC 27001.

## **Risk Management**

Através de uma estruturação da Gestão de Risco transversal numa organização, seja a nível estratégico, de programa, de projeto ou de nível operacional dotamos os formandos de ferramentas e técnicas capazes de fazerem uma eficaz gestão de riscos, através de abordagens recomendadas, listas de verificação e indicadores.

Conteúdos:

- Explain the terminology that is used within M\_o\_R
- Understand the principles for the development of good risk management practices
- Design an approach to risk management to improve performance
- Identify and assess risks, then plan and implement risk responses
- Establish current practices using M\_o\_R healthcheck and maturity model
- Identify opportunities and ways to improve Risk management
- Understand the importance of Risk Specialisms

## **Ação de Preparação para Exame MoR**

Tem como objetivo preparar os formandos o exame que permitirá alcançar a certificação M\_o\_R (Management of Risk)

### **Proteção de Dados - RGPD**

A importância no novo Regulamento Geral de Proteção de Dados (RGPD) e o impacto que o mesmo poderá ter nas organizações no contexto da privacidade da informação.

### **Information Systems Security - Domains of knowledge - Part 1 (e-Learning)**

Neste curso poderá abordar os procedimentos e processos mais eficientes, para detetar adversários com conhecimentos que podem ser diretamente aplicados no dia a dia. Conhece as especificidades que permitam maximizar a segurança de uma organização.

Conteúdos:

- Segurança e Gestão de Riscos;
- Segurança de Ativos;
- Engenharia de Segurança;
- Comunicações e Segurança de Redes;
- Gestão de Identidades e Acessos;
- Avaliação de Segurança e Testes;
- Operações de Segurança;
- Segurança em Desenvolvimento de Software

### **Information Systems Security - Domains of knowledge - Part 2**

Neste curso poderá explorar a aplicabilidade das técnicas mais eficazes, para detetar adversários por forma a permitir e melhorar a segurança de uma organização.

Conteúdos:

- Segurança e Gestão de Riscos;
- Segurança de Ativos;
- Engenharia de Segurança;
- Comunicações e Segurança de Redes;
- Gestão de Identidades e Acessos;
- Avaliação de Segurança e Testes;
- Operações de Segurança;
- Segurança em Desenvolvimento de Software

### **Certificação Rumos Expert (CRE): Auditor de Segurança**

O formando é presente a um exame prático sobre as matérias lecionadas e com avaliação presencial. Após avaliação positiva, este obterá um Certificado Rumos que atesta as competências como auditor de Segurança, provando dessa forma serem profissionais altamente especializados e preparados para enfrentar desafios reais do dia-a-dia.