



Técnico de Segurança

Infrastructure - Cibersegurança

Com certificação

- **Nível:** Entrada
 - **Duração:** 126h
-

Sobre o curso

Esta Carreira Profissional pretende 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*.

Este é o primeiro percurso de um conjunto de três, que formam a [Carreira Profissional Cyber Security](#).

Inclui as Certificações:

- CompTIA Security+
-

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.

Saídas Profissionais:

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

Condições

- 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 e condições financeiras disponíveis, contacte-nos através de info@galileu.pt ou do botão Saber +

Desconto – Profissionais em situação de desemprego

- **10% de desconto** válido **para inscrições a título particular de pessoas que se encontrem em situação de desemprego**, para o efeito, será solicitado **documento comprovativo da situação atual** – Não acumulável com outras campanhas em vigor.

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 [Carreira Profissional Técnico de Informática](#)
- A Carreira Profissional 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 GALILEU 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
- 1 Exame de Certificação

Exame:

Conheça os [prazos limite para realização do exame de certificação](#).

[Contacte-nos](#), caso tenha alguma específica sobre os exames.

Programa

- Fundamentos de Segurança e Informática
- Security Fundamentals (e-Learning)
- Seminário: Powershell and Scripting
- CompTIA Security+ Certification Prep
- Ação de Preparação para Exame CompTIA S+ (SY0-601) – Parte I
- Hardening de Sistemas
- Introduction to Python: Fundamentals
- Segurança no desenvolvimento de Software
- Noções básicas de direito + Lei do Cibercrime
- Ação de Preparação para Exame CompTIA S+ (SY0-601) – Parte II

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 Ciber Segurança.

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 CompTIA S+

Tem como objetivo preparar os formandos o exame SY0-601 que permitirá alcançar a certificação CompTIA Security+

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 SY0-601 que permitirá alcançar a certificação CompTIA Security+