Cyber Security

Segurança Informática

Com certificação

- **Nível:** Iniciado
- **Duração:** 357h

Sobre o curso

Esta Carreira Profissional fornecer-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.

Inclui as Certificações:

- MTA Security Fundamentals
- CompTIA Security+
- Ethical Hacking
- CompTIA Cybersecurity Analyst
- ISO/IEC 27001
- M_o_R (Management of Risk) Certification
- Certificação Rumos Expert (CRE): Auditor de Segurança

Objetivos:

- 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 perspetiva 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.

Estágio:

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

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.

Saídas Profissionais:

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

Pré-requisitos

- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa;
- Valorizam-se conhecimentos técnicos de informática ao nível de redes e sistemas;
- O percurso não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional.

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 GALILEU, em consulta a Organizações parceiras, e são devidamente acompanhados por material didático, distribuídos aos Participantes.

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 GALILEU, 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 a validade de 6 meses a contar da data de fim da formação.

Programa

- Fundamentos de Segurança e Informática
- Security Fundamentals (e-Learning)
- CompTIA Security+
- Ação de Preparação para Exame MTA
- Seminário: Powershell and Scripting
- Hardening de Sistemas
- Segurança no desenvolvimento de Software
- Ação de Preparação para Exame Comptia S+

- Marketing Pessoal e Comunicação
- Fundamentos Kali Linux (e-Learning)
- Ethical Hacking and Countermeasures
- Offensive Penetration Testing Services
- Ação de Preparação para Exame CEH
- Noções básicas de direito + Lei do Cibercrime
- Monitorização, Deteção e Prevenção de Intrusões
- Resposta a Incidentes com Técnicas Forenses
- Ação de Preparação para Exame CompTIA CySA+
- Information Security Management ISO/IEC 27001/27002
- Ação de Preparação para Exame EXIN ISO/IEC 27001
- Risk Management
- Ação de Preparação para Exame MoR
- Proteção de Dados – RGPD
- Information Systems Security – Domains of knowledge – Part 1 (e-Learning)
- Information Systems Security – Domains of knowledge – Part 2
- Certificação Rumos Expert (CRE): Auditor de Segurança

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:

- Cybersecurity Overview
- History & Hardware
- Operating Systems
- Virtualization & Cloud Computing
- Using Hypervisors
- Networking
- Cryptography
- Clients & Servers

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

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 formados com os conhecimentos necessários para fazerem o exame de certificação Comptia.

Conteúdo:

- Security Fundamentals
- Data Security
- Application Security
- Hosts and Devices Protection
- Internal Network Protection
- Perimeter Network Protection
- Physical Security
- Compliance and Operational Security
- Threats

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.

Seminário: Powershell and Scripting

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

Hardening de Sistemas

Trabalhar competências com vista a melhor 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
- Hardening
- Standards

- DISA STIGs
- Windows 7 Hardening
- Windows 10 Hardening
- Linux Hardening
- Windows Server 2012 Hardening
- Windows & Linux Hardening
- OpenVas

Segurança no desenvolvimento de Software

Dotar os formandos com os conceitos essenciais em programação Python para que possam utilizar os mesmos, em futuros testes de intrusão e prevenção de incidentes.

Conteúdos:

- Ciclo de vida de desenvolvimento de software
- Conceitos básicos da programação
- Desenho de código seguro
- Testes de segurança de software

Ação de Preparação para Exame Comptia S+

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

Marketing Pessoal e Comunicação

- Marketing Pessoal: definição e exploração do conceito
- Identificação da importância do Marketing Pessoal no crescimento pessoal e profissional
- A análise Swot aplicada aos objetivos pessoais e profissionais
- Abordagem ativa ao mercado de trabalho

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
- Bypassing Antivirus Applications
- Post Exploitation
- Web Application Testing
- Wireless Attacks

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).

Noções básicas de direito + Lei do Cibercrime

Monitorização, Deteção e Prevenção de Intrusões

Capacitar os formandos para deteção e monitorização 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:

- Policy and Compliance
- Evaluating Security Risks
- Defensible Security Architecture
- Defensible Endpoint Security Architecture
- Traditional Attack Techniques
- Network Security Monitoring (NSM)
- Identity and Access Management Security
- Designing a Vulnerability Management Program
- Analyzing Vulnerability Scans
- Monitoring Logs
- Monitoring Critical Events

Resposta a Incidentes com Técnicas Forenses

Dotar os formandos com os conhecimentos em ferramentas para que possam fazer uma eficaz a deteção, resolução e prevenção de incidentes de segurança.

Conteúdos:

- Preparação para o Incidente
- Deteção e caracterização de incidente
- Recolha de Evidências/Dados
- Análises de Dados
- Contenção e Remediação
- Erradicação
- Documentação e Conclusões

Ação de Preparação para Exame CompTIA CySA+

Tem como objetivo preparar os formandos o exame CS0-001 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 CS0-001 que permitirá alcançar a certificação EXIN ISO/IEC 27001.

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.