Curso: Academia Information Security Management

Duração: 105h
Área formativa: Cursos

Sobre o curso

Com o aumento da criminalidade cibernética e o surgimento constante de novas ameaças é um desafio gerir os riscos cibernéticos.

A **Academia Information Security Management** ajuda os profissionais e as organizações a se tornarem conscientes dos riscos e a identificarem e abordarem proativamente os pontos fracos.

A Academia Information Security Management foi projetada para desenvolver as competências dos profissionais na área de segurança da informação. O programa abrange as principais normas e regulamentos internacionais na área da segurança da informação. Desde a aplicação de inteligência artificial na cibersegurança aos principios do DevSecOps, os participantes irão adquirir conhecimentos baseado nas principais normas, como a ISO/IEC 27001/27002, Proteção de Dados – RGPD, Digital Operational Resilience Act – DORA, Network and Information Security Directive 2 – NIS2 e Cyber Resilience Act – CRA.

Porque quero frequentar esta Academia?

:: 1 Certificação reconhecida Internacionalmente

:: Os melhores profissionais certificados do mercado como formadores

:: Formação qualificada, através da Rumos, uma das empresas líderes na área da formação e distinguida “Marca n.º 1 na Escolha dos Profissionais 2024” pela ConsumerChoice

:: Acesso ao **Employability Hub**, um serviço dedicado a apoiar a integração e a progressão de carreira dos formandos das Academias da FLAG. Oferecemos um acompanhamento personalizado, focado na maximização do teu posicionamento no mercado de trabalho. Descobre mais sobre o Employability Hub aqui.

Que certificações vou obter?

:: ISO/IEC 27001

:: Certificação Rumos Expert (CRE): Cyber Security Engineer

Que profissões me esperam?

:: Auditor de Segurança da Informação

:: Information Security Officer

:: Chief Information Security Officer (CISO)

Objectivos

A **Academia Information Security Management** tem como objetivos:

:: Conhecer e desenvolver competências práticas e teóricas em áreas como análise de riscos, implementação de controles de segurança, auditoria e conformidade;

:: Compreender e aplicar as principais normas internacionais, como a ISO/IEC 27001/27002 para gestão eficaz da segurança da informação;

:: Obter certificação reconhecida internacionalmente através do Exame de Certificação EXIN ISO/IEC 27001.

Metodologia

:: Constituído por módulos de formação, integrados numa ótica de sessões mistas de teoria e prática.

:: 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 didáctico, distribuídos aos participantes.

:: Existem ainda, ao longo da Academia, momentos de autoestudo onde serão facultados guiões, ou materiais, que servirão como um roteiro valioso durante a jornada individual de aprendizagem do formando.

Composição

:: 105 Horas de Formação

:: 6 Ações de Formação

:: 1 Seminário

:: 1 Ação de Preparação para Exame

:: 1 Exame de Certificação Internacional: ISO 27001

:: 1 Exame CRE: Cyber Security Engineer

Exame de Certificação ISO 27001

:: O exame de certificação internacional deverá ser realizado no final do respetivo módulo de formação;

:: A data é sugerida 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 10 dias úteis de antecedência à data pretendida;

:: O exame tem de ser realizado até 6 meses após a data de fim da formação;

:: Exame para certificação Information Security Foundation based on ISO IEC 27001 (EXIN): apenas disponível em remoto.

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.

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 ou formação equiparada. A Academia não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional.

Destinatários

Profissionais TI, Auditores de Segurança, Consultores de Segurança, Gestores de Segurança, Analistas de Segurança, Arquitetos de Redes e Administradores de Redes e Sistemas.

Programa

AI in Cybersecurity (3,5h)

O objetivo deste módulo é proporcionar aos formandos uma visão abrangente das implicações da Inteligência Artificial (IA) na cibersegurança, explorar os riscos relacionados com a IA, conhecer o panorama das ferramentas com IA utilizadas em cibersegurança, analisar os desafios éticos da IA neste contexto e também conhecer a legislação global relacionada com a IA, bem como as autoridades relevantes.

Programa:

- Introduction to Artificial Intelligence in Cybersecurity
- Risks Related to AI
- AI Tools Landscape in Cybersecurity
- Ethical Challenges of AI in Cybersecurity
- Global AI Legislation and Relevant Authorities

DevSecOps Foundation (21h)

Neste módulo, os formandos vão explorar os fundamentos de DevSecOps e aprender como integrar práticas de segurança ao longo do ciclo de vida de desenvolvimento e operações de software.
O módulo aborda a evolução da segurança no desenvolvimento, práticas culturais do DevSecOps, modelação de ameaças, revisão de código seguro, integração CI/CD e implementação de segurança em pipelines de entrega contínua.

Programa:

- AppSec Fundamentals
    - The history behind software development practices and how they’ve evolved over the years
    - The importance of this field and the concepts of what makes DevSecOps
    - DevSecOps culture and as a discipline
- Introduction Threat Modeling
    - Introduction
    - Why Threat Model?
    - Process overview
    - Models
    - Deep dive of threats (STRIDE)
    - Tools
- Introduction Secure Code Review
    - Code Review
    - Phylosophy
    - Methodology
    - Perform Secure Code Review
    - Tools
- CI-CD Integration Life-Cycle
    - Introduction to GitHub Actions

    - Secret Scanning
    - SAST
    - SCA
    - IAC
    - DAST
    - How to perform hardening images
    - How to perform a gap analyses
    - Review Owasp top 10 CI-CD Attacks
- CI-CD Arquitecture Implementation
    - Create a Security Flow base in use cases

Information Security Management ISO/IEC 27001/27002 (31,5h)

Neste módulo iremos abordar as 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.

Programa:

- Information Security Management definitions
    - Difference between data and information
    - Value of data and information
    - Information Systems
    - Information architecture
- Management Systems
- PDCA model
- Security organization
    - Context of the organization
    - Policies
    - Hierarchy
        - Roles and responsibilities
        - Segregation of duties
    - Inventory and asset management
    - Access control
    - Supplier relationships
- Legislation, regulations, and standards
- Security Controls
    - Organizational
    - People
    - Physical
    - Technological
- Risk management
    - Threat vs. Vulnerability
    - Risk Exposure
    - Security measure
    - Quantitative and qualitative risk analysis

Ação de Preparação para Exame EXIN ISO/IEC 27001 (3,5h)

Esta sessão tem como objetivo preparar os formandos para o exame da EXIN que permitirá alcançar a certificação ISO/IEC 27001.

Fundamentos de Proteção de Dados – RGPD (7h)

Neste módulo os formandos irão compreender a importância do novo Regulamento Geral de Proteção de Dados (RGPD), qual o seu impacto nas organizações e qual o contexto da privacidade da informação e as suas implicações.

Programa:

- European Legislative Process
- Essential Definitions – Personal Data and Privacy concepts and principles
- Responsibilities
- Data Subject Rights
- Data Protection Officer (DPO) role
- Data Breach Management
- Sanctions, Fines, and Administrative Procedures
- Privacy by Design vs. Privacy by Default

Seminário: Digital Operational Resilience Act – DORA (3,5h)

Neste seminário, os formandos irão adquirir *insights* sobre o Digital Operational Resilience Act (DORA), compreender os seus objetivos, identificar as entidades afetadas, explorar os seus pilares fundamentais e abordar os desafios encontrados durante as fases de desenvolvimento e implementação.

Programa:

- DORA introduction
    - Main objectives and obligations
    - EU Context
    - Timeline and application
- Entities Affected by DORA
- DORA obligations
    - Key pillars
    - Incident Management
    - Governance
    - Third parties' management
- Challenges in DORA Implementation
    - Best practices
    - Deliverables
- Main Challenges

Network and Information Security Directive 2 – NIS2 (14h)

Pretende-se com este módulo que os formandos consigam adquirir uma compreensão sólida dos requisitos da Network and Information Security Directive 2 (NIS2), preparando-se assim, para implementar medidas de segurança eficazes em conformidade com essa regulamentação.

Programa:

- Introduction to the Network and Information Security Directive 2 (NIS2)
- Structure and requirements
- Essential Service Operators and Digital service Providers
- Policies
- Risk analysis and Incident handling
- Business continuity and crisis management
- Best practices in Cybersecurity
- Ethical and Legal Aspects of NIS2

Cyber Resilience Act – CRA (7h)

Neste módulo os formandos irão adquirir uma compreensão profunda do Cyber Resilience Act Europeu, qual o seu enquadramento legal, requisitos de cibersegurança e implicações práticas tanto para fabricantes quanto para utilizadores. Neste módulo trabalhar-se-á o conhecimento e as estratégias necessárias para navegar pelas complexidades do CRA e reforçar a postura geral de cyber segurança dos produtos digitais no mercado europeu.

Programa:

- Understanding the Cyber Resilience Act (CRA)
- Framework and regulatory landscape
- Requirements and main objectives
- Impacts on manufacturers and user
- Notification requirements
- Best practices for compliance and implementation
- Cross-Border perspectives
- Enhancing Consumer Protection

Certificação Rumos Expert (CRE): Cyber Security Engineer (14h)

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 Cyber Security Engineer, provando dessa forma serem profissionais altamente especializados e preparados para enfrentar desafios reais do dia-a-dia.

Sessão de Encerramento

Sessão de encerramento de fim de ciclo formativo com análise de resultados alcançados