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, 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 Reconhecida como uma das normas mais importantes na segurança da informação, a certificação ISO/IEC 27001 da PECB valida competências para implementar, gerir e melhorar um Sistema de Gestão da Segurança da Informação (SGSI). Baseada numa abordagem de gestão de risco, permite assegurar a confidencialidade, integridade e disponibilidade da informação,

promovendo a melhoria contínua dos processos organizacionais.

:: **Certificação Rumos Expert (CRE): CyberSecurity Engineer** Através da realização de um projeto prático baseado em cenários reais e tarefas do dia-a-dia, esta certificação prática valida a aplicação das competências técnicas e o desempenho no terreno de um CyberSecurity Engineer.

Que profissões me esperam?

:: Auditor de Segurança da Informação

:: Information Security Officer

:: Chief Information Security Officer (CISO)

Objectivos

- 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 para gestão eficaz da segurança da informação
- Obter certificação reconhecida internacionalmente através do Exame de Certificação PECB 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
- 5 Ações de Formação
- 1 Hands-on Lab

- 1 Seminário
- 1 Ação de Preparação para Exame
- 1 Exame de Certificação Internacional: PECB ISO/IEC 27001
- 1 Exame Rumos CRE: Cyber Security Engineer

Exame de Certificação ISO 27001

- O exame de certificação 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.

Pré-requisitos

- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa;
- Conhecimentos técnicos em informática, cibersegurança ou administração de sistemas de informação, equivalentes às que se adquirem na Academia Técnico de Informática ou formação equiparada
- O percurso 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 (7h)

Este módulo aborda o impacto crescente da Inteligência Artificial na cibersegurança, explorando tanto o seu potencial defensivo como os riscos associados à sua utilização maliciosa. Os formandos irão analisar o papel da IA na deteção e resposta a ameaças, as ferramentas e técnicas baseadas em modelos de machine learning e linguagem natural, e as implicações legais e éticas do seu uso. O módulo inclui ainda um conjunto de casos práticos e ferramentas aplicadas em contextos reais de segurança.

Competências desenvolvidas:

- Identificação de aplicações práticas e riscos da utilização de IA em cibersegurança
- Utilização de ferramentas e modelos de IA para apoio à análise e resposta a ameaças

- Interpretação de regulamentações e desafios éticos associados à IA

Programa:

- Fundamentos e Cenário de Ameaças
- Introdução Estratégica à IA na Cibersegurança
    - Desmistificar a IA: Diferenças práticas entre IA, Machine Learning e Deep Learning, com analogias para públicos não técnicos.
    - A natureza dual da IA: Introdução ao paradigma “IA para Defesa vs. IA para Ataque” desde o início.
- O Ecossistema de Risco da IA
    - Categoria de Risco 1: IA como Arma
    - Categoria de Risco 2: Ataques à IA (IA Adversária)
    - Categoria de Risco 3: Riscos Operacionais e de Governance
- Governança, Ferramentas e Conformidade
- Panorama de Ferramentas e Aplicações Práticas
    - Aplicação da IA em SIEM, SOAR, EDR/XDR, Segurança de Rede, UEBA, e Threat Intelligence
    - Como avaliar uma ferramenta com “IA”
- Ética, Legislação e Conformidade
    - Desafios Éticos enquanto Risco Empresarial: Responsabilização, transparência e equidade
    - EU AI Act
    - Modelos de Governance
    - O papel das autoridades
    - Passos para a conformidade

DevSecOps Foundation (17,5h)

Este módulo fornece uma visão abrangente das práticas DevSecOps, destacando a importância da segurança desde o início do desenvolvimento até à operação. Serão abordadas ferramentas e processos como threat modeling, secure code review, integração contínua (CI/CD) e análise de vulnerabilidades. Os formandos irão ainda compreender como promover a colaboração entre equipas de desenvolvimento, operações e segurança.

Competências desenvolvidas:

- Aplicação de práticas seguras em pipelines CI/CD
- Identificação e mitigação de vulnerabilidades desde o desenvolvimento
- Promoção da cultura DevSecOps nas organizações

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
- Introdution Threat Modeling
- Introdution
- Why Threat Model?
- Process overview

- Models
- Deep dive of threats (STRIDE)
- Tools
- Introdution Secure Code Review
- Code Review
- Phylosophy
- Methodology
- Perform Secure Code Review
- Tools
- CI-CD integration life-cycle
- Introdution 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.

ISO/IEC 27001 Foundation – PECB (14h)

Os formandos irão conhecer os elementos essenciais para a implementação e gestão de um SGSI, com base na norma ISO/IEC 27001. Serão explorados temas como políticas de segurança, controlos, auditoria interna e melhoria contínua. O módulo prepara também os participantes para o exame de certificação ISO/IEC 27001 Foundation.

Competências desenvolvidas:

- Compreensão dos requisitos da norma ISO/IEC 27001
- Conhecimento de controlos e objetivos de segurança da informação
- Preparação para a certificação ISO/IEC 27001 Foundation

Programa:

- Introdução, contexto e definições
- Principais publicações
- Liderança e suporte ao SGSI
- Planeamento e operação do SGSI
- Objetivos de controlo e controlos de segurança da informação (Parte 1)
- Objetivos de controlo e controlos de segurança da informação (Parte 2)
- Obtenção da Certificação ISO/IEC 27001

Ação de Preparação para Exame PECB ISO/IEC 27001:2022 Foundation (7h)

Durante esta ação de preparação, serão abordados os conteúdos mais relevantes da norma ISO/IEC 27001, com esclarecimento de dúvidas, simulação de questões e estratégias práticas para maximizar o sucesso no exame.

Competências desenvolvidas:

- Consolidação dos principais tópicos da norma
- Prática de resolução de questões de exame
- Planeamento estratégico para a obtenção da certificação

Fundamentos de Proteção de Dados – RGPD (7h)

Neste módulo serão analisadas as bases legais do RGPD, os direitos dos titulares dos dados, o papel do Encarregado de Proteção de Dados (DPO), as obrigações das organizações e as consequências de incumprimento. O objetivo é dotar os formandos de conhecimento prático para aplicar o regulamento em ambientes reais.

Competências desenvolvidas:

- Interpretação dos princípios do RGPD
- Identificação de responsabilidades e obrigações legais
- Aplicação prática de medidas de conformidade

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

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

Este módulo aborda a estrutura e os requisitos da diretiva NIS2, com foco nos operadores de serviços essenciais e prestadores de serviços digitais. Serão exploradas políticas, gestão de riscos, continuidade de negócio, tratamento de incidentes e aspetos éticos e legais relacionados com a segurança das redes e da informação.

Competências desenvolvidas:

- Interpretação dos requisitos da NIS2
- Planeamento de medidas de conformidade
- Aplicação de boas práticas em cibersegurança organizacional

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

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

Neste seminário serão apresentados os objetivos e pilares do DORA, a sua articulação com outras regulamentações da UE, os desafios da sua implementação e as entidades afetadas. Os formandos terão uma visão clara sobre as exigências de gestão de incidentes, governança e terceiros prestadores de serviços.

Competências desenvolvidas:

- Compreensão dos principais elementos do DORA
- Identificação de entidades abrangidas e obrigações
- Avaliação dos desafios de 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

Cyber Resilience Act – CRA (7h)

Os formandos irão analisar o enquadramento legal do CRA, os requisitos de segurança, as obrigações de notificação e as melhores práticas para assegurar a conformidade. O módulo permite compreender o impacto transversal desta legislação na cadeia de fornecimento digital e na proteção do consumidor.

Competências desenvolvidas:

- Compreensão das exigências legais do CRA
- Aplicação de práticas de conformidade em produtos digitais
- Interpretação de implicações para fabricantes e utilizadores

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

Try to Hack Me – Security Engineer (Hands-on Lab) (14h)

Neste laboratório prático, os formandos irão trabalhar em cenários avançados de defesa de infraestruturas, com foco na identificação de vulnerabilidades, aplicação de medidas corretivas e monitorização de sistemas. Utilizando a plataforma "Try to Hack Me", terão contacto com tarefas típicas do dia a dia de um Security Engineer.

Competências desenvolvidas:

- Implementação de medidas de proteção de sistemas e redes
- Monitorização de infraestruturas e resposta a ameaças
- Prática de defesa em ambientes simulados

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

A Certificação Rumos Expert (CRE) consiste na resolução de um caso prático inspirado em desafios reais do setor. Os formandos aplicam os conhecimentos desenvolvidos em contextos técnicos e normativos, sendo avaliados por um júri. Esta certificação atesta o domínio técnico e a preparação para funções como Cyber Security Engineer.

Competências desenvolvidas:

- Integração de conhecimentos técnicos e normativos
- Capacidade de resolver desafios práticos de segurança
- Validação final das competências profissionais

Sessão de Encerramento

Esta sessão marca o final do percurso formativo, promovendo a partilha de experiências entre formandos e equipa pedagógica. São apresentados os principais destaques da Academia, feedback recolhido, resultados obtidos e oportunidades de progressão profissional no setor da cibersegurança.

Objetivos:

- Reflexão sobre a aprendizagem e evolução individual
- Reforço da rede de contactos profissionais
- Planeamento de próximos passos na carreira em cibersegurança