



Cyber Security

Infrastructure - Cibersegurança

Promoção: EARLY BIRD: 5% de desconto até 18 de maio. Garante já a tua vaga!

Live Training (também disponível em presencial)

Com certificação

- **Localidade:** Imprimir Curso
- **Data:** 18 Jun 2024
- **Preço:** 6200 € (POSSIBILIDADE DE PAGAMENTO FASEADO ATÉ 18 MENSALIDADES
Os valores apresentados não incluem IVA. Oferta de IVA a particulares.)
- **Horário:** Pós-laboral e Sábados das 3ª e 5ª feiras 18h45 às 22h15 e sábados das 9h30 às 13h00
- **Nível:** Intermédio
- **Duração:** 350h

Sobre o curso

A Academia Cybersecurity está desenhada para desenvolver competências técnicas avançadas em cibersegurança, ao formar e certificar os formandos numa das áreas mais críticas e maior crescimento a nível mundial.

Com uma abordagem imersiva e uma forte componente prática nos principais domínios de ataque e defesa em cibersegurança, o programa deste percurso de formação é constituído por vários módulos que vão explorar diferentes especializações e verticalidades da área da segurança informática aplicadas à realidade do mercado profissional.

Os formandos vão poder consolidar as principais frameworks de segurança informática e evoluírem passo a passo aplicando diferentes técnicas avançadas e abordagens tais como: Ethical hacking, testes de penetração e vulnerabilidade, análise e auditoria da conformidade dos sistemas de informação, entre muitos outros desafios.

Através de laboratórios *hands-on* e outros desafios práticos, os formandos vão poder adquirir as principais competências críticas que as organizações procuram na atualidade e poderem assim integrar equipas e projetos de cibersegurança.

Razões para frequentar esta Academia?

- Formação imersiva e com forte componente prática nos principais domínios de ataque e defesa em cibersegurança
- 3 Certificações reconhecidas internacionalmente
- Os melhores profissionais certificados do mercado como formadores
- Possibilidade de estágio no final da formação
- Formação qualificada

Inclui as Certificações:

- CEH: Certified Ethical Hacking – Practical
- CompTIA Cybersecurity Analyst (CySA+)
- ISO/IEC 27001
- Certificação Rumos Expert (CRE): CyberSecurity Engineer

Saídas Profissionais:

- Especialista de Cibersegurança
- Consultor de Cibersegurança
- Administrador de Segurança Informática
- Penetration & Vulnerability Tester
- Analista de Cibersegurança
- Cyber Security Engineer
- Auditor de Segurança da Informação
- Chief Information Security Officer (CISO)

Estágio:

Esta Academia inclui a possibilidade de estágio, após a conclusão da formação mediante a realização dos exames de Certificação com aproveitamento.

Destinatários

Destina-se a todos os interessados em aprofundar os seus conhecimentos de redes e sistemas com especialização em cibersegurança.

Objetivos

- Preparar profissionais de cibersegurança capazes de dominar as principais ferramentas, técnicas de análise e de conformidade na segurança dos sistemas de informação.
- Dotar os formandos com conhecimentos de implementação de soluções de monitorização, análise e prevenção de intrusões. Lidar com sistemas críticos e criar planos de resposta a incidentes e recuperação de desastres. Desenvolver competências na resposta a novas ameaças. Realizar análises de vulnerabilidades e testes de intrusão. Compreender e dominar as estratégias de ataque e defesa de diferentes ângulos ao imitar as estratégias de ataque de hackers maliciosos.
- Desenvolver e capacitar os formandos com conhecimentos sólidos nas principais práticas de codificação em testes de segurança e integração contínua para o desenvolvimento de software. Configuração e proteção de redes Wi-Fi com técnicas robustas e seguras. Implementação de medidas de segurança eficazes em ambientes Cloud. Utilizar ferramentas avançadas em testes de penetração ofensiva. Utilizar ferramentas de Inteligência Artificial (IA) aplicadas à cibersegurança.
- Compreender Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) e Resposta Orquestrada a Ameaças e Automatizada (SOAR). Capacitar os participantes para a análise de ameaças e vulnerabilidades em redes e sistemas e na defesa proativa da segurança de uma organização.
- Desenvolver competências na implementação de frameworks internacionais e das principais normas de conformidade para segurança de informação: DevSecOps, Normas ISO/IEC 27001/27002, Regulamento Geral de Proteção de Dados (RGPD), Digital Operational Resilience Act – DORA, Network and Information Security Directive 2 – NIS2 e Cyber Resilience Act (CRA).
- Criar oportunidades de networking para os formandos construírem uma rede de contatos estratégica com outros formandos e profissionais especialistas em cibersegurança, fomentando colaborações futuras e oportunidades de carreira.
- Certificar as competências técnicas adquiridas através da obtenção de certificações internacionais.

Condições

- Taxa de inscrição: 290€, dedutível no valor total.
- Possibilidade de pagamento faseado para particulares, até 18 prestações, sem juros.
- Formandos 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;
- 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.

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 síncrono 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.
- 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:

- 16 Ações de Formação TI
- 1 Seminário Técnico
- 3 Ações de Preparação para Exame

- 4 Exames de Certificação
- 1 CTF
- 1 Hands-on-Labs
- 3 Momentos de auto-estudo

Exames de Certificação

- 3 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 10 dias úteis de antecedência à data pretendida;
- Os exames têm de ser realizados até 6 meses após a data de fim da formação;
- Modalidades dos exames:
 - Exame para certificação CompTIA Cybersecurity Analyst+: poderá optar por realizar em presencial ou remotamente
 - Exame para certificação Information Security Foundation based on ISO IEC 27001 (EXIN): apenas disponível em remoto
 - Exame para certificação CEH: na Academia está incluído o exame na modalidade presencial. Caso opte pela modalidade remota terá um custo adicional de 75€ + IVA (Isenção do valor do IVA a particulares)

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.

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

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

Programa

- Cybersecurity Framework
- Autoestudo dedicado a Fundamentos de PowerShell e Scripting
- Systems Hardening

- Noções básicas de direito + Lei do Cibercrime
- Autoestudo dedicado a Linux for Ethical Hackers
- Ethical Hacking and Penetration Testing
- Practical Ethical Hacking - CEH
- APE: Ação de Preparação para Exame CEH (Practical)
- Autoestudo dedicado a Fundamentos de Python
- Segurança no desenvolvimento de Software
- Wi-Fi Best Practices
- Cloud Security
- Offensive Penetration Testing Services
- CompTIA Cybersecurity Analyst + CertPrep (CySA+)
- Hand-on-Labs: SIEM and SOAR
- APE: Ação de Preparação para Exame CompTIA CySA+
- Capture the Flag - CTF
- AI in Cybersecurity
- DevSecOps Foundation
- Information Security Management ISO/IEC 27001/27002
- APE: Ação de Preparação para Exame EXIN ISO/IEC 27001
- Fundamentos de Proteção de Dados - RGPD
- Seminário: Digital Operational Resilience Act - DORA
- Network and Information Security Directive 2 - NIS2
- Cyber Resilience Act - CRA
- Certificação Rumos Expert (CRE): Cyber Security Engineer

Apresentação

Sessão de boas-vindas para esclarecimento de todos os processos e procedimentos existentes.

Cybersecurity Framework (21h)

A primeira etapa para quem está a iniciar-se ou a especializar-se em cibersegurança, é conhecer as boas práticas reconhecidamente eficazes pelos profissionais.

Este módulo foca-se no “NIST Cybersecurity Framework”, uma abordagem estruturada desenvolvida pelo National Institute of Standards and Technology (NIST) dos Estados Unidos da América, destinada a auxiliar organizações na melhoria da sua postura de cibersegurança. O NIST é uma agência governamental encarregada de promover e desenvolver padrões em várias áreas, incluindo a cibersegurança. O “NIST Cybersecurity Framework” foi concebido em resposta às ameaças digitais crescentes, visando fortalecer a resiliência de organizações públicas e privadas contra ciberataques. Este framework consiste em diretrizes, padrões e melhores práticas que orientam as organizações no planeamento, implementação, monitorização e aprimoramento das suas medidas de cibersegurança.

Programa:

- What is the NIST Cybersecurity Framework, and how can it be used by an organization.
- History and Creation of the Framework
- Uses and Benefits of the Framework
- Cybersecurity Framework Components
- The Five Functions of the Framework
- Identify
- Protect
- Detect
- Respond
- Recover
- Other related frameworks and standards

Autoestudo dedicado a Fundamentos de PowerShell e Scripting

Neste momento de autoestudo, pretende-se que os formandos possam adquirir os conceitos fundamentais de PowerShell que atualmente são utilizados em ferramentas de exploração de sistemas Windows, bem como uma primeira abordagem ao desenvolvimento de scripts.

Programa:

- Introduction to PowerShell
- Introduction to scripting in PowerShell
- Create and run scripts by using Windows PowerShell

Systems Hardening (28h)

O Systems Hardening consiste na utilização de ferramentas, técnicas e boas práticas para proteger sistemas informáticos contra ciberataques. Neste módulo vamos aprender a mitigar os riscos, eliminando potenciais vetores de ataque e minimizando a superfície de ataque à segurança dos sistemas.

Programa:

- Introduction to Systems Hardening
- Security Baselines
- Security Protocols and Specifications
- Vulnerability Assessment Tools
- Tools for assessment, measurement, and enforcement of security baselines
- Systems Hardening
- Application hardening
- Operating system hardening

- Endpoint hardening
- Server hardening
- Database hardening
- Network hardening

Noções básicas de direito + Lei do Cibercrime (7h)

Neste módulo iremos dar a conhecer os pontos chave da legislação em vigor relacionados com a cibersegurança e quais as consequências do seu não cumprimento.

Programa:

- Noções básicas de direito
- Lei do Cibercrime

Autoestudo dedicado a Linux for Ethical Hackers

Neste momento de autoestudo, serão facultados conteúdos de aproximadamente duas horas em formato de vídeo, que servirão como um guia individual de aprendizagem aos sistemas Linux através da distribuição Kali Linux.

Programa:

- Installing VMWare/Kali Linux
- Kali Linux Overview
- Navigating the File System
- Users and Privileges
- Common Network Commands
- Viewing, Creating, and Editing Files
- Starting and Stopping Services
- Installing and Updating Tools
- Advanced Bash-Scripting

Ethical Hacking and Penetration Testing (31,5h)

Contrariamente aos hackers maliciosos, os ethical hackers atuam com a devida autorização dos proprietários do sistema, tomando todas as precauções necessárias para assegurar a confidencialidade dos resultados.

Este módulo pretende dotar os formandos com as técnicas de hacking mais recentes e as técnicas de pentest mais avançadas utilizadas pelos hackers e profissionais de segurança informática, para que possam conhecer as ameaças e os cenários de vulnerabilidade que são originados pelos vários tipos de ataques, podendo assim criar estratégias de defesa e mitigar futuros ataques.

Programa:

- Introdução ao Hacking Ético
- Reconhecimento, Scanning e Enumeração
- System Hacking: Análise de Vulnerabilidades; Password Cracking; Acesso aos Sistemas e Esconder o Rasto
- Sniffing
- Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)
- Ameaças com Malware
- Engenharia Social
- Técnicas de evasão aos sistemas de Segurança
- Ataques a Web Servers e Web Applications (inclui Session Hijacking)
- SQL Injection
- Ataques a redes Wireless
- Ataques a Dispositivos Móveis
- Ataques a Cloud Computing
- Ataques a dispositivos IoT
- Ataques a plataformas OT
- Criptografia – algoritmos e ferramentas

Practical Ethical Hacking (35h)

Neste curso inteiramente prático, os formandos vão aplicar várias técnicas e também preparar-se para o exame prático de CEH da EC-Council. Este curso oferece uma experiência prática em técnicas avançadas de hacking ético, capacitando profissionais para identificar, avaliar e fortalecer sistemas contra ameaças.

Programa:

- Attack vectors
- Perform network scanning
- Identify live and vulnerable machines in a network
- OS banner grabbing
- Service
- User emulation
- System hacking
- Steganography
- Steganalysis attacks
- Cover attacks
- Identify and use viruses
- Computer worms

- Malware to exploit systems
- Packet sniffing
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Cryptography attacks
- Security loopholes
- Communication infrastructure
- End systems

Ação de Preparação para Exame Prático CEH (3,5h)

Tem como objetivo preparar os formandos o exame prático de CEH da EC-Council, esclarecendo dúvidas/questões bem como alertar para cuidados a que devem ser levados em conta, na altura em que se está envolvido no processo de exame.

Autoestudo dedicado a Fundamentos de Python

Neste momento de autoestudo será facultado um vídeo, que irá permitir uma primeira aproximação a uma linguagem de programação, que será o Python, não numa perspetiva de programador propriamente dito, mas numa perspetiva das necessidades e utilidade para um Ethical Hacker.

Programa:

- Basic Python Concepts
- Control Structures
- Functions and Challenges
- Web Basics and Security
- Networking and Hacking Tools
- Advanced Web Development and Cybersecurity Challenges

Segurança no desenvolvimento de Software (17,5h)

Este módulo irá proporcionar uma compreensão ao nível do desenvolvimento seguro de software através de uma análise do ciclo de vida do desenvolvimento de software, integrando práticas seguras de codificação, testes de segurança e integração contínua de segurança. Adicionalmente, serão identificados e discutidos desafios comuns na construção de aplicações seguras.

Programa:

- Understanding Key Security Concepts and Common Threats:
- Explore fundamental security concepts and the most prevalent types of threats.
- Identify various attack vectors such as injection attacks, cross-site scripting (XSS), and sensitive data

exposure.

- Recognizing Defense Techniques and Risk Mitigation:
 - Learn techniques to defend against security threats and mitigate risks in software development.
 - Understand practices like input validation, secure coding guidelines, and encryption to enhance application security.
- Understanding the Software Development Lifecycle and Security:
 - Gain insight into the software development lifecycle and the pivotal role of security at each phase.
 - Explore secure coding practices, security testing, and continuous security integration within the software development process.
- Identifying Challenges in Building Secure Applications:
 - Identify common pitfalls and challenges faced in creating secure applications.
 - Discuss real-world examples of security vulnerabilities in applications and explore strategies to address these issues effectively.

Wi-Fi Best Practices (3,5h)

Neste módulo vamos realçar as boas práticas essenciais para proteger redes sem fios e comunicações Bluetooth e NFC. Vamos começar com as configurações seguras de redes Wi-Fi, destacando a importância da criptografia robusta e senhas seguras. Em seguida, exploraremos técnicas de emparelhamento seguro para dispositivos Bluetooth e protocolos de segurança NFC, garantindo transações seguras. Abordaremos também o uso seguro dessas tecnologias em espaços públicos, realçando os riscos e as medidas preventivas necessárias.

Programa:

- Wireless Network Security Best Practices
- Bluetooth Security Measures
- NFC (Near Field Communication) Security Protocols
- Securing Wireless Communication in Public Spaces

Cloud Security (10,5h)

Neste módulo serão explorados os princípios fundamentais relacionados com Cloud Computing, abrangendo conceitos e definições essenciais. Este módulo tem como objetivo dar a conhecer os principais serviços Cloud disponíveis no mercado, explicar os modelos de responsabilidade partilhada entre fornecedores e utilizadores de serviços Cloud, bem como analisar os benefícios e riscos inerentes a estas tecnologias. Adicionalmente, serão abordados os frameworks e as melhores práticas de cibersegurança para a Cloud, capacitando os formandos a tomar decisões informadas e implementar medidas de segurança eficazes em ambientes Cloud.

Programa:

- Cloud Computing Definition and Concepts
- Main Cloud Services and Technologies Landscape
- Shared Responsibility in the Cloud
- Security Benefits of Cloud Computing
- Risks of Cloud Computing
- Cloud Cybersecurity Frameworks and Best Practices

Offensive Penetration Testing Services (24,5h)

Neste módulo inteiramente prático, com o acompanhamento do formador, os formandos vão explorar e utilizar algumas das ferramentas avançadas mais utilizadas em Ethical Hacking de forma a terem um pleno conhecimento ao nível do que é feito em Red Teams.

Programa:

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

CompTIA Cybersecurity Analyst + CertPrep (CySA+) (35h)

Este módulo está focado na análise comportamental às redes para melhorar o estado geral da segurança, identificando e combatendo malware e ameaças persistentes avançadas (APTs), resultando numa visibilidade aprimorada das ameaças numa superfície de ataque alargada. Contribuirá para capacitar um profissional de TI na defesa proactivamente e melhorar continuamente a segurança de uma organização.

Programa:

- Threat and Vulnerability Management
- Utilize and apply proactive threat intelligence to support organizational security and perform vulnerability management activities

- Software and Systems Security
- Apply security solutions for infrastructure management and explain software & hardware assurance best practices
- Compliance and Assessment
- Apply security concepts in support of organizational risk mitigation and understand the importance of frameworks, policies, procedures, and controls
- Security Operations and Monitoring
- Analyze data as part of continuous security monitoring activities and implement configuration changes to existing controls to improve security
- Incident Response
- Apply the appropriate incident response procedure, analyze potential indicators of compromise, and utilize basic digital forensics techniques

Hand-on Labs: SIEM and SOAR (14h)

Neste módulo, os formandos vão trabalhar num conjunto de exercícios para proporcionar uma compreensão abrangente dos Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) e Resposta Orquestrada a Ameaças e Automatizada (SOAR).

Programa:

- SIEM Overview
- Basic SIEM Configuration
- Hands-on Lab: Initial SIEM Setup
- Advanced Analysis with SIEM
- Introduction to SOAR
- Hands-on Lab: SIEM and SOAR Integration
- Automated Response with SOAR
- Best Practices and Case Studies

Ação de Preparação para Exame CompTIA CySA+ (7h)

Esta sessão tem como objetivo preparar os formandos no esclarecimento de dúvidas para o exame CS0-003 que permitirá alcançar a certificação CompTIA Cybersecurity Analyst (CySA+).

Capture the Flag – CTF (7h)

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

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, iremos abordar o propósito, benefícios, conceitos e vocabulário do DevSecOps, compreendendo como as práticas de segurança do DevOps se diferenciam de outras abordagens de segurança. Serão exploradas estratégias de segurança orientadas para o negócio e as melhores práticas, assim como a aplicação de datascience e segurança. A integração de partes interessadas corporativas nas práticas do DevSecOps e o aperfeiçoamento da comunicação entre as equipas de Desenvolvimento, Segurança e Operações também serão abordados. Além disso, os participantes irão compreender como os papéis do DevSecOps se encaixam numa cultura e organização DevOps.

Programa:

- Realizing DevSecOps Outcomes
- Defining the Cyberthreat Landscape
- Building a Responsive DevSecOps Model
- Integrating DevSecOps Stakeholders
- Establishing DevSecOps Best Practices
- Best Practices to get Started
- DevOps Pipelines and Continuous Compliance
- Learning Using Outcomes

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