FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

# CACADEMY

PRR
Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

Nível E

# Auditoria de Vulnerabilidades - Edição 19-05-2025 | 4 ECTS

## Universidade de Coimbra

70 horas / B-Learning / 100€

### Sinopse

Os alunos que terminam com sucesso esta unidade curricular serão capazes de:

1. Conhecer o ciclo de vida de vulnerabilidades;
2. Conhecer ferramentas e processos de identificação de vulnerabilidades;
3. Avaliar e analisar o risco associado a vulnerabilidades;
4. Conhecimentos para explorar vulnerabilidades.

### Short bio do Formador

Nuno Seixas, Mestre em Engenharia de Software pela Carnegie Mellon University e Mestre em Engenharia Informática pela Universidade de Coimbra. Tem em curso o Doutoramento em Engenharia Informática pela mesma Universidade. Esta formação formal permitiu a obtenção de um conhecimento extenso dos princípios de desenvolvimento de software e que levou a uma diversa experiência em otimização de equipas de desenvolvimento de software, incluíndo diversos standadrs, como CMMI, ITIL e ISO27001. Nos últimos 20 anos assumiu diversos papéis no desenvolvimento de software, desde programador individual até Director sénior de operações. Com uma experiência alargada como formador em ambiente profissional, é também professor convidado na Universidade de Coimbra, onde lecciona cadeiras de Engenharia de Software, Auditoria e Cibersegurança.

Bruno Sousa, é Professor Auxiliar no Departamento de Engenharia Informática da Universidade de Coimbra, Portugal, desde dezembro de 2018, onde obteve o doutoramento em Engenharia Informática na disciplina de Multihoming para redes baseadas em IP, em dezembro de 2014. É investigador sénior do Centro de Informática e Sistemas da UC (CISUC), onde iniciou a sua actividade em 2006. É autor de vários capítulos de livros, diversas publicações em revistas e conferências internacionais. Participou no TPC de diversas conferências. Participou em vários projetos de investigação europeus e nacionais, como IST FP6 Integrated Projects, EuQoS e WEIRD, ICT FP7, MobiTRUst, SALUS, Mobile Cloud Networking, LiveCity e FI-WARE, e H2020 EMPATIA. Os seus interesses de investigação incluem mecanismos de resiliência em redes e aplicações/serviços, e deteção e prevenção de intrusões em redes 5G e para Internet das Coisas (IoT).

### Conteúdos Programáticos

1. Auditoria breve introdução
- Terminologia
- Relevância da auditoria
- Tipos de auditoria
- Aspetos importantes

2. Ciclo de Vida de Vulnerabilidades
- Contexto de uma Organização
- Contexto de um sistema de informação e assets
- Vulnerabilidades

- Monitorização de Vulnerabilidades
- Medidas, controlos de Vulnerabilidades
- Comunicação de vulnerabilidades

3. Vulnerabilidades de Aplicações e Sistemas
- Terminologia
- Vulnerabilidades em aplicações Web
- Vulnerabilidades em aplicações móveis
- Vulnerabilidades em aplicações empresariais
- Vulnerabilidades em aplicações cloud
- Vulnerabilidades em sistemas IoT

4. Avaliação e Análise de Vulnerabilidades
- Metodologias de identificação, avaliação e análise de vulnerabilidades
- Ferramentas de scan e avaliação de Vulnerabilidades
- Componente prática - Identificação

5. Exploração de vulnerabilidades
- Ferramentas de análise de comunicações
- Configurações de hardware, sistema e de aplicações
- Exploração de vulnerabilidades em organizações
- Exploração de vulnerabilidades
- Exercícios práticos

6. Perspetivas de futuro, tópicos emergentes
- AI
- Paradigma Zero Trust
- Conclusão

## Avaliação e Certificado

Os resultados de aprendizagem são avaliados através de:
• 1 exame escrito (individual) (10%), (T)
• realização dos exercícios práticos (em grupo) (50%) (P)
• apresentação de exercício prático (em grupo) (15%) (P)
• avaliação de pares acerca dos resultados do exercício prático (em grupo) (25%) (P)

Assim a nota final será 10% teórica + 90% prática [NF=0,10*T+ (0,50 + 0,15 + 0,25) * P ].

## Pré-requisitos para quem vai frequentar a formação:

1) Conhecimentos técnicos de Linux e Sistemas Operativos Windows

2) Conhecimentos práticos de instalação de aplicações/ programas

3) Conhecimentos práticos de utilização de ferramentas de virtualização (VirtualBox, VMWare Desktop)

4) Conhecimentos práticos de instalação de sistemas operativos e sua configuração de rede

5) Conhecimentos de segurança, na perspetiva de processos e operações dentro de uma organização

6) Conhecimentos genéricos de avaliação de risco e termos relacionados (atacante, ameaças)

**Observações:** Não aplicável.

# Calendário

| Local | Dia | Horário | Formato |
|---|---|---|---|
| Universidade de Coimbra | 19/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 20/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 21/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 22/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 23/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 26/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 27/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 28/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 29/5/2025 | 09:00-18:00 | B-Learning (presencial com possibilidade de participar remotamente) |
| Universidade de Coimbra | 30/5/2025 | 09:00-12:00 | B-Learning (presencial com possibilidade de participar remotamente) |