



FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA



OFFACADEMY



Financiado pela
União Europeia
NextGenerationEU

Nível B

Formação Intermédia em Cibersegurança - Edição 11- 02-2025 | 2 ECTS

Instituto Politécnico do Porto

35 horas / Híbrido / 50€

Sinopse

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

1. Reconhecer técnicas de Engenharia Social e comportamentos de risco associados.
2. Gerir eficazmente situações de crise e comunicar de forma clara em momentos críticos.
3. Desenvolver um ambiente de trabalho seguro e habilidades para influenciar comportamentos seguros.
4. Agir em conformidade com políticas de segurança, gestão de riscos, e implementar medidas de segurança adaptadas ao contexto profissional.

Short bio do Formador

Módulos

1) Engenharia Social

Definição e técnicas de Engenharia Social
Comportamentos de risco nas redes sociais
Comportamentos de risco em ambiente laboral
Navegação segura na Internet

2) Comunicação de Crise e Risco

Conhecimento dos programas, funções e responsabilidades de resposta a incidentes
Conhecimento de categorias de incidentes e respetivas respostas
Conhecimento de planeamento de ações em situações de crise
Conhecimento dos procedimentos e ferramentas de documentação e de consulta de incidentes, problemas e eventos reportados

3) Técnicas de Sensibilização e Capacitação do Fator Humano

Conhecimento de formas de demonstrar profissionalismo, através do exemplo, aos colegas
Conhecimento de formas de providenciar a equipas um ambiente facilitador de trabalho em equipa, de desenvolvimento de relação e de desenvolvimento pessoal e profissional das pessoas
Conhecimento de comportamentos físicos e fisiológicos que podem indicar atividade suspeita ou anormal
Conhecimento de formas de encorajar e guiar os outros a adotar um ponto de vista, a mudarem ou a agir

4) Cibersegurança em Contexto Profissional/ Cibersegurança em Serviços Essenciais

Conhecimento das políticas, normas e procedimentos para a correta utilização das tecnologias de informação da organização (e.g., criação de contas, regras de password, controlos de acesso).

Avaliação e Certificado

Os resultados de aprendizagem são avaliados através de um teste individual de escolha múltipla (20%), um trabalho de grupo de pesquisa com apresentação (30%) e, no final da formação, um exame individual composto por questões de resposta aberta (50%).

(NF=0,2 *T+0, 3*TG +0x5*E).

Pré-requisitos para quem vai frequentar a formação:

Conhecimento de bases de cibersegurança, incluindo ameaças, vulnerabilidades, ataques comuns, técnicas de defesa e boas práticas.

Conhecimentos básicos de redes de comunicação, nomeadamente, tipos de equipamentos, topologias, serviços, e questões de segurança relacionadas com a rede.

Familiaridade com conceitos fundamentais de segurança da informação, como confidencialidade, integridade, disponibilidade, autenticidade e não repúdio.

Utilização de sistemas operativos Windows, Linux ou macOS e instalação de ferramentas nesses ambientes.

Calendário

Local	Dia	Horário	Formato
CIM Tâmega e Sousa - Av. José Júlio, 42, 4560-547 - Penafiel	11/2/2025	19:00-22:00	Presencial
	13/2/2025	19:00-22:00	Online
	18/2/2025	19:00-22:00	Online
	20/2/2025	19:00-22:00	Online
	25/2/2025	19:00-22:00	Online
	27/2/2025	19:00-22:00	Online
	6/3/2025	19:00-22:00	Online
	11/3/2025	19:00-22:00	Online
	13/3/2025	19:00-22:00	Online
	18/3/2025	19:00-22:00	Online
	20/3/2025	19:00-22:00	Online

CIM Tâmega e Sousa
- Av. José Júlio, 42,
4560-547 - Penafiel

25/3/2025

19:00-21:00

Presencial
