UNIVERSIDADE
AbERTA
www.uab.pt

Luís Carlos Crispim Pereira
Rua da Tábua, 45
4900-847 Meadela

Sua referência:	Data	Nossa referência: DSA/SA: 2300163	Data

05 J _ 2024 003605

ASSUNTO: Envio de certificado de formação

Junto se envia certificado relativo ao curso de formação.

Com os melhores cumprimentos.

A Diretora dos Serviços Académicos

(Mestre Isabel Saraiva)

VITORIA

SEDE | PALÁCIO CEIA
Rua da Escola Politécnica, 147
1269-001 Lisboa
Rua da Imprensa Nacional, 100
1250-127 Lisboa
Portugal
Tel.: (+351) 213 916 300
uab@uab.pt

UNIVERSIDADE ABERTA
www.uab.pt

CERTIFICADO DE FORMAÇÃO

Certifica-se que

Luís Carlos Crispim Pereira

portador(a) do documento de identificação número 13019195, concluiu com aproveitamento e classificação final de 15 valores, numa escala de 0 a 20 valores, o curso

Microcredencial: Fundamentos de Cibersegurança

que decorreu de 23 de abril a 28 de maio de 2024. A microcredencial tem o nível 4 do Quadro Nacional de Qualificações e teve a duração total de 52 horas, a que correspondem 2 ECTS da Universidade Aberta.

Lisboa, 5 de julho de 2024

A Diretora dos Serviços Académicos

Isabel Saraiva

alv Aprendizagem ao Longo da Vida

Curso: Microcredencial em Fundamentos de Cibersegurança

Modalidade de Formação: Formação a distância em regime de e-learning

Área de Formação: 481 – Ciências informáticas

Conteúdos Programáticos do Curso

Módulos	Conteúdos	Duração (h)
0. Ambientação ao Contexto Online	Ambientação ao contexto online do curso e socialização. Treino com as ferramentas/funcionalidades da PlataformABERTA.	13
1. Fundamentos de cibersegurança, redes de computadores e sistemas operativos	Introdução à cibersegurança. Redes de computadores. Sistemas operativos. Prática em contexto deformação.	13
2. Encriptação de dados	Fundamentos de criptografia. Encriptação em suportes físicos. Encriptação de correio eletrónico. Prática de encriptação em contexto de formação.	13
3. Fundamentos de ethical hacking	Introdução ao Ethical Hacking. Reconhecimento e vulnerabilidades. OSINT (Open source intelligence). Prática em contexto de formação.	13
4. Ciberhigiene	Segurança e hardening em sistemas Windows. Segurança na Internet. Virtualização e emulação de software. Prática em contexto de formação.	13

Objetivos do curso:

- Proporcionar conhecimentos e competências fundamentais em redes de computadores e sistemas operativos, os principais alvos de ataques.
- Proporcionar conhecimentos e competências que permitam aos participantes caracterizar os ataques típicos bem como as defesas correspondentes.
- Capacitar os participantes a identificar, reagir e proteger das principais ciberameaças.

Competências:

- Aprender o funcionamento de sistemas operativos, das redes em geral e da internet em particular;
- Conhecer as principais normas e leis de referência do cibercrime e da proteção de dados incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD);
- Navegar na Internet de forma segura;
- Reagir e responder de forma adequada às principais ciberameaças incluindo o ciberbullying;
- Gerir e proteger identidade digital;
- Usar mecanismos de autenticação forte;
- Cifrar a informação existente em todo o suporte informático e nas comunicações por correio eletrónico;
- Proteger e configurar de forma segura os seus dispositivos eletrónicos e a rede de internet doméstica;
- Aprender a forma de ataque de um hacker (ethical hacking);
- Capturar credenciais numa comunicação de rede;
- Extrair informação de fontes abertas para planeamento e execução de um ataque - OSINT (Open source intelligence);
- Detetar vulnerabilidades em redes empresariais e em ambiente pessoal.