

CURSO DE ESPECIALIZAÇÃO TECNOLÓGICA

Técnico/a Especialista em

Cibersegurança

Híbrido (B-Learning) — Pós-laboral Remoto (Síncrono) e Presencial aos Sábados

Sobre o Curso

O curso de Técnico/a Especialista em Cibersegurança é uma qualificação de Nível 5 QNQ que prepara profissionais para implementar e gerir sistemas de segurança em organizações, contribuindo para a prevenção, deteção e mitigação de ameaças cibernéticas. Combina formação teórica em legislação, redes e sistemas com competências técnicas avançadas em pentesting, forense digital e gestão de incidentes.

DURAÇÃO TOTAL

1025h Formação

+ 400h Estágio Profissional

QUALIFICAÇÃO

Diploma de Técnico/a Especialista

Nível 5 QNQ / QEQ · Código: 481RA057

Áreas de Atuação Profissional

Centros de Operações de Segurança (SOC)

Monitorização contínua de eventos e resposta em 1.^a linha a incidentes de cibersegurança.

Equipas de Pentest / Red Team

Realização de testes de penetração e análise de vulnerabilidades em sistemas e redes.

Forense Digital e Compliance

Recolha de evidências, análise forense e suporte à elaboração de relatórios técnicos e legais.

Competências Desenvolvidas

- Configurar plataformas de cibersegurança e segurança perimétrica
- Monitorizar eventos e detetar ameaças no ciberespaço
- Realizar testes de penetração (pentesting)
- Responder a incidentes de cibersegurança em 1.^a linha
- Analisar evidências e apoiar relatórios forense
- Gerir sistemas IDS e ferramentas de análise de logs
- Desenvolver scripts de segurança e normalização
- Simular cenários de ciberdefesa (wargaming)

COMPONENTE GERAL E CIENTÍFICA

Unidades de Competência — Obrigatórias

Cód.	N.º	Unidade de Competência (UC)	Horas	Créditos
UC01476	1	Implementar a legislação relativa à cibersegurança	25	2,25
UC01477	2	Aplicar métodos estatísticos	50	4,50
UC00598	3	Efetuar operações e cálculos matemáticos aplicados a projetos da área de informática	50	4,50
UC00599	4	Interagir em inglês nas atividades do setor da informática	50	4,50
Total de Pontos de Crédito da Componente Geral e Científica: 15,75			175	15,75

COMPONENTE TECNOLÓGICA

Unidades de Competência — Obrigatórias

Cód.	N.º	Unidade de Competência (UC)	Horas	Créditos
UC00245	1	Desenvolver algoritmos	25	2,25
UC00606	2	Desenvolver programas em linguagem estruturada	50	4,50
UC00602	3	Modelar bases de dados relacionais	25	2,25
UC00631	4	Planear e instalar a infraestrutura de redes locais	50	4,50
UC01478	5	Configurar redes de computadores	25	2,25
UC00634	6	Instalar, configurar e manter sistema operativo de cliente	25	2,25
UC00633	7	Instalar e parametrizar sistemas operativos de servidor (plataforma proprietária)	50	4,50
UC00635	8	Configurar serviços de rede	25	2,25
UC01479	9	Implementar mecanismos de proteção contra ameaças cibernéticas	25	2,25
UC01480	10	Analisar evidências de ataques cibernéticos	50	4,50
UC01481	11	Desenvolver scripts aplicados à cibersegurança	25	2,25
UC01482	12	Programar scripts de normalização e filtragem de logs	50	4,50
UC01483	13	Detetar e analisar vulnerabilidades em soluções web	50	4,50
UC01484	14	Detetar e analisar vulnerabilidades em sistemas de rede	50	4,50
UC01485	15	Instalar e configurar ferramentas de análise e recolha de logs e evidências	50	4,50
UC01486	16	Gerir sistemas de deteção de intrusos (IDS)	50	4,50
UC01487	17	Simular cenários de cibersegurança e ciberdefesa (wargaming)	50	4,50
UC00616	18	Implementar as normas de segurança e saúde no trabalho no setor de Informática	25	2,25
Total de pontos de crédito: 63,00			700	63,00

Para obter a qualificação, para além das UC Obrigatórias, terão também de ser realizadas UC Opcionais correspondentes ao total de 13,5 pontos de crédito.

COMPONENTE TECNOLÓGICA

Unidades de Competência — Opcionais

Para obter a qualificação, para além das UC Obrigatórias, terão também de ser realizadas UC Opcionais correspondentes ao total de 13,5 pontos de crédito.

Cód.	N.º	Unidade de Competência (UC)	Horas	Créditos
UC00033	1	Comunicar e interagir em contexto profissional	50	4,50
UC00034	2	Colaborar e trabalhar em equipa	50	4,50
UC00600	3	Analisar as funções e estrutura da organização	25	2,25
UC00613	4	Gerir políticas de segurança em sistemas informáticos	25	2,25
UC01488	5	Gerir a segurança da informação e criptografia	25	2,25
UC01489	6	Implementar procedimentos de recolha e análise forense digital	50	4,50
UC01490	7	Executar técnicas de hacking ético	25	2,25
UC00627	8	Instalar e configurar servidores Web	25	2,25
UC01491	9	Projetar e administrar sistemas de bases de dados	50	4,50

Formação em Contexto de Trabalho (FCT)

400 Horas Obrigatórias

A componente de formação em contexto de trabalho visa aplicar conhecimentos e saberes adquiridos às atividades práticas do respetivo perfil profissional e executar atividades sob orientação, utilizando as técnicas, os equipamentos e os materiais que se integram nos processos de produção de bens ou de prestação de serviços. Esta formação desenvolve-se em parceria estabelecida entre a instituição de formação e empresas, outras entidades empregadoras, associações empresariais ou socioprofissionais, e pode adotar diferentes modalidades, designadamente estágios.