



FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA



OFFACADEMY



PRR
Plano de Recuperação
e Resiliência



REPÚBLICA
PORTUGUESA



Financiado pela
União Europeia
NextGenerationEU

Nível B

Formação para Responsável de (Ciber)Segurança - Edição 07-04-2025 | 2 ECTS

Instituto Politécnico de Viana do Castelo
35 horas / B-Learning / 50€

Sinopse

Ao concluir esta unidade curricular, os alunos serão capazes de:

1. Interpretar regulamentos de Cibersegurança e Proteção de Dados.
2. Compreender funções de Responsável de (Ciber)Segurança e Ponto de Contato Permanente.
3. Aplicar os quadros de referência CIS, COBIT, ISO/IEC e NIST.
4. Realizar análise, gestão e mitigação de riscos.
5. Implementar ferramentas de análise e gestão de risco.
6. Definir medidas técnicas e organizativas de Cibersegurança.
7. Descrever processos de monitorização e auditoria.
8. Gerir e classificar ativos organizacionais.
9. Gerir incidentes de Cibersegurança, incluindo análise, resposta e notificação.
10. Elaborar Política de Segurança da Informação.
11. Desenvolver Plano de Cibersegurança.
12. Preparar Relatório Anual de Cibersegurança conforme legislação.
13. Definir plano de ação para conformidade regulatória e melhoria da maturidade organizacional em Cibersegurança.

Short bio do Formador

Ricardo Jorge da Cunha Montenegro, Licenciado em Engenharia Informática com Pós-Graduação em Informática de Segurança e Computação Forense. Foi docente de algumas disciplinas de segurança no Instituto Politécnico de Viana do Castelo.

É quadro do Município de Paredes de Coura há mais de 20 anos, onde é especialista de sistemas e tecnologias de informação.

Desde dezembro de 2022 é Responsável de Segurança, de acordo com o Decreto-Lei n.º 65/2021 (Artigo 5.º), que Regulamenta o Regime Jurídico da Segurança do Ciberespaço.

Pedro Emanuel Cardoso de Sousa, Licenciado em Engenharia Informática e com Pós-Graduação em Administração de Redes e Sistemas Informáticos. Membro da Ordem dos Engenheiros e da Ordem dos Engenheiros Técnicos. Engenheiro Técnico Especialista em Sistemas de Informação.

Titulo de Especialista na Área de Ciências Informáticas. Foi membro dos Serviços de Informática do IPVC durante 17 anos, 13 dos quais na coordenação. Perito judicial para vários processos de tecnologias de informação. Responsável por implementar várias redes de telecomunicações e centros de dados, em entidades públicas e privadas. Certificações nas áreas de Redes, Segurança e Administração de Sistemas (Oracle, Microsoft, Sophos (Cyberoam), UBNT, ITIL, ...). Professor de Ensino Superior no IPVC e também já exerceu no IPCA e na FEUP. Formação de Auditor de Segurança pela Rumos e Proteção de Dados pelo ICS. Formador certificado com CCP. Nos últimos anos dedica-se a projetos de DevOps e DevSecOps modernizando equipas de desenvolvimento.

António Marques é um profissional motivado pelo desafio de atingir metas, aplicando ampla visão e experiência em diferentes áreas de tecnologia e processos, para entregar consistência, eficiência e segurança. Responsável por conquistas como a criação do primeiro CSIRT não governamental e internacionalmente acreditado, em Portugal.

Conteúdos Programáticos

- 1) Legislação aplicável à Cibersegurança;
- 2) Frameworks CIS, COBIT, ISO/IEC, NIST, etc;
- 3) Análise e gestão de risco;
- 4) Ferramenta Monarc;
- 5) Medidas técnicas e organizativas;
- 6) Auditoria e monitorização da Cibersegurança;
- 7) Inventário de ativos;
- 8) Gestão de incidentes de cibersegurança;
- 9) Política de Segurança da Informação (PSI);
- 10) Plano de Segurança;
- 11) Relatório Anual de Cibersegurança;
- 12) Plano para conformidade com o Regime Jurídico de Segurança no Ciberespaço (RJSC);
- 13) Esquema de certificação Quadro Nacional de Referência para a Cibersegurança (QNRCS);
- 14) Selo de maturidade digital da cibersegurança.

Avaliação e Certificado

Os tópicos são ainda explorados através da realização de exercícios práticos para cada um dos diferentes tópicos suportados em guiões fornecidos pelo docente e realizados em grupo. Os exercícios são efetuados recorrendo a simulações, correspondendo a 50% da nota. Os resultados de aprendizagem são avaliados individualmente através de 1 exame escrito (restantes 50% da nota). Assim a nota final será 50% teórica + 50% prática ($NF=0,5*T+0,5*P$).

Pré-requisitos para quem vai frequentar a formação:

- 1) Formação ou experiência profissional em área relacionada com as tecnologias de informação e comunicação, conhecimentos do funcionamento de sistemas operativos e de redes de comunicação (tipos de equipamentos, tecnologias, entre outros).
- 2) Conhecimentos técnicos ao nível da segurança dos sistemas de informação.

Observações: Não aplicável.

Calendário

Local	Dia	Horário	Formato
	7/4/2025	18:30-22:30	Online
	8/4/2025	18:30-22:30	Online

	9/4/2025	18:30-22:30	Online
	10/4/2025	18:30-21:30	Online
	11/4/2025	18:30-22:30	Online
	14/4/2025	18:30-22:30	Online
	15/4/2025	18:30-22:30	Online
Instituto Politécnico de Viana do Castelo	16/4/2025	18:30-22:30	B-Learning (presencial com possibilidade de participar remotamente)
Instituto Politécnico de Viana do Castelo	17/4/2025	18:30-22:30	B-Learning (presencial com possibilidade de participar remotamente)