FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

CYBERSECURITY ACADEMY

PRR
Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

Nível D

Legislação, Política e Gestão de Ativos no Contexto da Cibersegurança - Edição 21-05-2025 | 2 ECTS

Instituto Politécnico de Viseu

35 horas / Online / 50€

Sinopse

Esta formação destina-se a todas as pessoas que pretendam adquirir um conjunto de conhecimentos associados a analista de incidentes.
Os formandos terão oportunidade de desenvolver as seguintes competências:
1. pensamento crítico e criativo;
2. gestão de risco;
3. deteção de ameaças;
4. análise de vulnerabilidades.

Depois de frequentar este curso: Legislação, Política e Gestão de Ativos no Contexto da Cibersegurança ganhará conhecimentos em:
1. Identificar e gerir os ativos da organização
2. Gerir o risco em cibersegurança
3. Analisar e responder a incidentes de cibersegurança;
4. Dotar as suas organizações de protocolos de resposta e metodologias e procedimentos em casos de ataques/incidentes.

Short bio do Formador

Mara Almeida Pereira, desenvolve maioritariamente a sua prática na área de Direito Público, Direito Administrativo, Regulatório, Proteção de Dados e Cibersegurança, trabalhando com entidades públicas e privadas, seja em projetos de consultoria, como projetos de implementação nas áreas acima descritas.

Conteúdos Programáticos

1) Introdução à Cibersegurança
- Compreender no que consiste e qual a importância da cibersegurança

2) Considerações Legais e Eticas
- Compreender e analisar algumas considerações legais e éticas mais relevantes no âmbito nacional e europeu

3) Quadro normativo ISO/IEC 27001 Segurança da Informação
- Clarificar quais os fundamentos da segurança da informação

4) Política de Segurança
- Compreender o processo de desenvolvimento, estruturação e implementação de políticas de cibersegurança

5) Gestão de Ativos de TI
- Explicar e clarificar no que consiste a identificação, classificação e avaliação de ativos de TI

6) Gestão de Equipamentos em Redes
- Compreender no que consiste e como funciona a arquitetura e estrutura das redes cibernéticas, incluindo os seus equipamentos e funções

7) Gestão de Riscos
- Compreender e analisar como é feita a identificação, análise e avaliação de risco

8) Gestão de Incidentes de Segurança
- Compreender a importância da gestão de incidentes e quais as várias fases de um plano de resposta a incidentes

9) Treino e Conscencialização
- Explicar a importância de programas de treino e sensibilização em cibersegurança

10) Auditoria e Conformidade
- Analisar o processo de auditoria e todos os seus componentes, relevância e regulamentações relevantes associadas

11) Continuidade de Negócio e Recuperação de Desastres
- Explicar a importância, processo e componentes de um Plano de Continuidade de Negócio e de um Plano de Recuperação de Desastres

12) Tendências e Desenvolvimentos Futuros
- Clarificar e analisar quais as principais tendências e desafios em cibersegurança

Avaliação e Certificado

Os resultados de aprendizagem são avaliados individualmente através de 1 exame escrito (restantes 70% da nota). Assim a nota final será 70% exame + 30% participação.

Pré-requisitos para quem vai frequentar a formação:

1) Formação ou experiência profissional em áreas relacionadas com as tecnologias de informação e comunicação, conhecimento do funcionamento de sistemas operativos e de redes de comunicação (tipos de equipamentos, tecnologias, entre outros)
2) Estar familizarizado com regulamentos e/ou quadros normativos relacionados com a privacidade de dados e segurança da informação
3) Conhecimentos técnicos relativos a cibersegurança e sistemas de informação

Observações: Não aplicável.

Calendário

Local	Dia	Horário	Formato
	21/5/2025	18:30-21:30	Online
	26/5/2025	18:30-21:30	Online
	28/5/2025	18:30-21:30	Online

	2/6/2025	18:30-21:30	Online
	4/6/2025	18:30-21:30	Online
	9/6/2025	18:30-21:30	Online
	11/6/2025	18:30-21:30	Online
	16/6/2025	18:30-21:30	Online
	18/6/2025	18:30-21:30	Online
	23/6/2025	18:30-21:30	Online
	25/6/2025	18:30-21:30	Online
	7/7/2025	18:30-21:30	Online