IFB INSTITUTO DE FORMAÇÃO BANCÁRIA
ASSOCIAÇÃO PORTUGUESA DE BANCOS

EXECUTIVE EDUCATION

FORMAÇÃO AVANÇADA

FORMAÇÃO ONLINE POR VIDEOCONFERÊNCIA

FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

NÍVEL I: 17, 18 e 19 de junho

NÍVEL II: 23, 25 e 26 de junho

NÍVEL III: 30 de junho, 01 e 02 de julho

2026
JUN/JUL.26*

INFORMAÇÕES
Catarina Santos
c.santos@ifb.pt
+351 217916293**

* As formações calendarizadas funcionam com um número mínimo e máximo de formandos, pelo que, a realização das mesmas encontra-se sujeita a confirmação.

 | ** Custo de chamada para a rede fixa nacional

FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

IFB INSTITUTO DE FORMAÇÃO BANCÁRIA
ASSOCIAÇÃO PORTUGUESA DE BANCOS

FORMAÇÃO AVANÇADA

DESTINATÁRIOS: Programa dirigido a Decisores e Gestores Intermédios, Diretores, TFE´S, Quadros e Técnicos que pretendam ter uma visão global do tema ou especialização em determinadas áreas.

DOCENTES:

Agostinho Valente - Docente universitário, Consultor Sénior responsável pela implementação de sistemas de gestão de Segurança da Informação e Cibersegurança, Privacidade e dados pessoais, projeto de implementação do SOC2 e projetos de Governance, Risk and Compliance (GRC).

André Calvinho - Especialista em Cibersegurança, nas áreas de Information Assurance, Vulnerability Assessment, Penetration Testing, Forensics, Configuration Analysis, Security Analysis, Hardening e Incident Response. É docente e conferencista universitário em cursos de cibersegurança.

José Dinis - Dedica-se ao estudo do Security Operations Center - Capacidades e Liderança. Docente na Academia Militar no Mestrado de Guerra da Informação, no Curso de Segurança de Informação da CIIWA, no CINEL e na ATEC. Atualmente é consultor de Segurança de Informação e Cibersegurança, é vice-presidente da AFCEA e membro da Direção da CIIWA.

DURAÇÃO: 24 horas **HORÁRIO:** 17h00 – 20h00

PREÇOS:	Associados APB	Tabela Geral
Nível	408 €	469 €
Programa completo	1 166 €	1 341 €

PROGRAMA:

Nível I
8 horas

Nível Básico
- Cenário Inicial do Use Case
- Principais Ameaças às Organizações
- Gestão de Segurança da Informação e Cibersegurança
- Introdução à Engenharia Social

Objetivo: Introduzir conceitos fundamentais, boas práticas e um panorama inicial sobre gestão de segurança da informação e cibersegurança.

Nível II
8 horas

Nível Intermédio
- Evolução do Use Case: Deteção do Incidente
- Metodologias de Testes de Penetração
- Auditoria e Conformidade
- Gestão de Risco na Cibersegurança
  - Identificação de Riscos
  - Avaliação e Análise de Riscos
  - Tratamento de Riscos
  - Estudo de Caso Prático

Objetivo: Desenvolver competências práticas na gestão de incidentes e mitigação de riscos

Nível III
8 horas

Nível Avançado
- Gestão de Incidentes e Medidas de Defesa
- Exploração de Vulnerabilidades
- Ataques de Rede
- Principais pontos do Plano de Continuidade de Negócio (PCN)
- Tabletop Exercise: Ciberataque e Continuidade de Negócio
- Liderança Digital

Objetivo: Capacitar para testes de penetração, exploração de vulnerabilidades e gestão de continuidade.

Metodologia:
- Estudo de Caso Continuado: O use case evolui ao longo da formação, promovendo reflexão contínua e aplicação prática.
- Metodologias Ativas: Simulações, exercícios práticos e análise de cenários.
- Avaliação Contínua: Quizzes, participação em simulações e produção de relatórios.
- Feedback em Tempo Real: Reflexão sobre decisões tomadas ao longo do exercício.

Entidade Formadora Certificada dgert

FULL MEMBER OF EBTN EUROPEAN BANKING & FINANCIAL SERVICES TRAINING ASSOCIATION AISBL

Pedidos de Cancelamento: Só poderão dar origem ao reembolso total do valor pago, quando recebidos até 5 dias úteis antes da data de início do curso. A partir deste prazo, a inscrição será paga na totalidade, podendo, no entanto, o participante ser substituído por outro; Deverão ser efetuados por e-mail e rececionados pelo IFB dentro do prazo acima estabelecido.