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:

NÍVEL II:

NÍVEL III:

EDIÇÃO 2024
A agendar*

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.

DOCENTE: **José Carlos Martins -** Doutor e Mestre em Tecnologias e Sistemas de Informação pela Universidade do Minho. Possui ainda pós-graduações em: (i) Guerra de Informação / Competitive Intelligence (AM); (ii) Tratamento Estatístico de Dados (ISCTE). É licenciado em Ciências Militares pela AM e em Engenharia Informática pela FCT / UNL. Atualmente é consultor sénior de Segurança da Informação e Cibersegurança da Pahl Consulting e docente universitário [e.g., Academia Militar (AM), IP Luso].

DURAÇÃO: 24 horas **HORÁRIO:** 17h30 – 20h30

PREÇOS:	Associados APB	Tabela Geral
Nível I (3 horas)	227 €	261 €
Nível II (6 horas)	398 €	458 €
Nível III (15 horas)	738 €	849 €
Programa completo	1 136 €	1 306 €

PROGRAMA:

Nível I **3 horas**	**Gestão de Segurança da Informação** • Principais Ameaças às Organizações • Visão integrada da Gestão de Segurança da Informação e Cibersegurança • Modelo de Atividades de Gestão de Segurança da Informação e Cibersegurança
Nível II **6 horas**	**Implementação de um Sistema de Gestão de Segurança da Informação (Método)** • Visão Geral dos Principais Controlos da ISO/IEC 27001 • Método de Implementação de um SGSI suportado na ISO/IEC 27001 • Principais Factores de Sucesso
	Principais Processos, Políticas e Planos de um SGSI • Visão Geral dos Principais Processos, Políticas de Planos • Análise e Discussão de um processo (Gestão de Segurança Informação) • Análise e Discussão de uma política (Segurança Informação)
Nível III **15 horas**	**Gestão do Risco de Segurança da Informação** • Principais Conceitos de Gestão do Risco • Visão Geral das Normas ISO / IEC 31000 e 27005 • Principais Factores de Sucesso
	Processo de Gestão do Risco • *Design*, Implementação e Operação do Processo de Gestão do Risco • Técnicas de Recolha de Informação • Técnicas de Identificação, Análise e Avaliação de Riscos
	Modelação de Métodos de Ataque (Técnicas Gerais) • Árvores de Ataque (exemplos) • Taxonomia de Análise de Vulnerabilidades - STRIDE (exemplos) • Cenarização - Análise Morfológica Geral (exemplo)
	***Case Study* - Identificação, Avaliação e Tratamento de Riscos** • Análise e Discussão de um Caso de Estudo (Empresa) • Elaboração de uma Matriz de Riscos de SegInfo e Cibersegurança

***Case Study* – "*NaturalSafetyQ*, uma empresa Online"**

O principal objetivo é treinar a identificação, análise, avaliação e tratamento do risco no âmbito da Segurança da Informação e Cibersegurança. Os participantes assumem o papel de CISO de uma empresa fictícia e através de um processo deliberativo em grupo, condicionado pelo tempo disponível, respondem a um conjunto de pedidos associados fundamentalmente à gestão do risco, tendo como objetivo final a elaboração de uma matriz de riscos. Os formandos deverão dedicar cerca de 2 horas na análise de documentação entregue fora do horário de formação.

DGERT ENTIDADE FORMADORA CERTIFICADA

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.