IFB INSTITUTO DE FORMAÇÃO BANCÁRIA
ASSOCIAÇÃO PORTUGUESA DE BANCOS

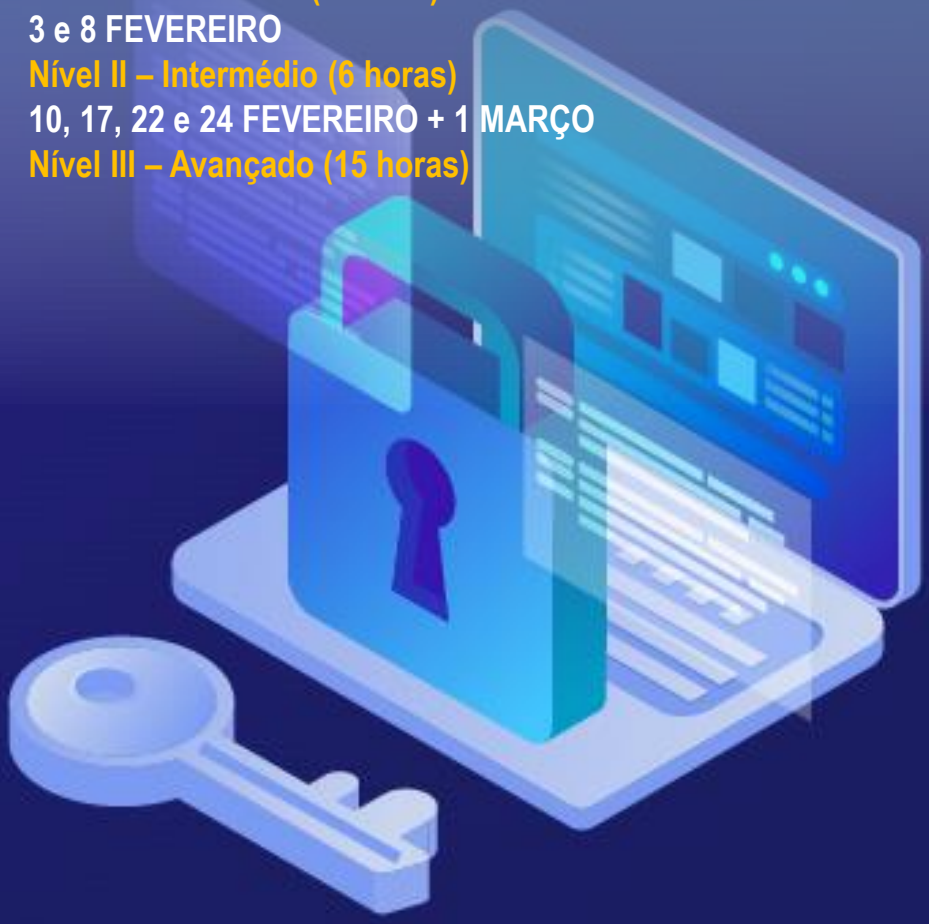
FORMAÇÃO AVANÇADA

FORMAÇÃO ONLINE POR VIDEOCONFERÊNCIA

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

Programa de Especialização

1 FEVEREIRO
Nível I – Elementar (3 horas)
3 e 8 FEVEREIRO
Nível II – Intermédio (6 horas)
10, 17, 22 e 24 FEVEREIRO + 1 MARÇO
Nível III – Avançado (15 horas)



EDIÇÕES: 2021*

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.

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO
Programa de Especialização

IFB INSTITUTO DE FORMAÇÃO BANCÁRIA
ASSOCIAÇÃO PORTUGUESA DE BANCOS

DESTINATÁRIOS

Decisores e Gestores Intermédios
Diretores, TFE´S, Quadros e Técnicos que pretendam ter uma visão global do tema

HORÁRIO

Nível I – 09h30 - 12h30
Nível II – 09h30 - 12h30
Nível III – 09h30 - 12h30

FORMAÇÃO AVANÇADA

NÍVEL I		
Avaliação Teste online: Questões de Escolha Múltipla (20 minutos)	**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	3h
NÍVEL II		
Avaliação Teste online: Questões de Escolha Múltipla (45 minutos)	**Implementação de um SGSI (Método)** • Visão Geral dos Principais Controlos da ISO/IEC 27001. • Método de Implementação de um SGSI suportado na ISO/IEC 27001. • Principais Fatores de Sucesso.	3h
	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)	3h
NÍVEL III		
Avaliação Discussão e Participação no Caso de Estudo	**Gestão do Risco de Segurança da Informação** • Principais Conceitos de Gestão do Risco. • Visão Geral das Normas ISO / IEC 31000 e 27005. • Principais Fatores de Sucesso	3h
	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.	3h
	Modelação de Métodos de Ataque (Técnicas Gerais) • Arvores de Ataque (exemplos). • Taxonomia de Análise de Vulnerabilidades – STRIDE (exemplos). • Cenarização – Análise Morfológica Geral (exemplo).	3h
	Case Study - Identificação, Avaliação e Tratamento de Riscos • Análise e Discussão de um Caso de Estudo (Empresa). • Elaboração de uma Matriz de Riscos de SegInfoe Cibersegurança.	6h

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

Programa completo: 24h

PREÇO:

	Associados	Tabela Geral
Nível I	200 €	230 €
Nível II	400 €	460 €
Nível III	1 000 €	1 150 €
Programa completo	1 250 €	1 440 €

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.

FORMAÇÃO AVANÇADA

DOCENTES

Carlos Alexandre

Licenciatura em Organização e Gestão de Empresas – ISCTE. Pós-Graduação Gestão de Sistemas de Informação – ISCTE. Pós-Graduação Guerra de Informação e Competitive Intelligence – Academia Militar. Certificação CISA - Certified Information Systems Auditor. Dedica-se ao estudo, e respetiva aplicação, do elo mais fraco na segurança de Sistemas de Informação. Ministra aulas ou sessões de sensibilização sobre os riscos de Engenharia Social.

Jorge Custódio

Mestre em Engenharia Informática. Parte do Doutoramento em Engenharia Informática pela Universidade Nova de Lisboa. Partner e CIO da Feelsec Consulting. Participou em vários projetos de relacionados com: arquitetura de infraestruturas com tolerância a falhas, para o suporte de aplicações críticas; segurança de infraestruturas; gestão de identidades e acessos; desenvolvimento de aplicações em diversas linguagens; monitorização de ativos; testes de intrusão; design de políticas de Segurança de Informação; e de gestão de vulnerabilidades, incidentes e inventário.

José 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. Partner da FeelSec Consulting, CISO, Gestor de projetos de Segurança da Informação e Cibersegurança e docente universitário.

Luís Dias

É Major de Transmissões do Exército Português, especializado em Segurança da Informação e docente na Academia Militar. Doutorando no IST. Diploma de estudos avançados em Segurança de Informação, Mestre e licenciado em Engenharia Eletrotécnica Militar. Detém várias certificações da Indústria das quais se salientam: SANS GCFE, EC-Council ECSA e ENSA, entre outras. É membro do GIAC advisory board.