FORMAÇÃO AVANÇADA

FORMAÇÃO ONLINE POR VIDEOCONFERÊNCIA

PROGRAMA DE FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

ENGENHARIA SOCIAL
Outubro (6, 11, 13, 18, 20, 25 e 27)

SECURITY & PRIVACY BY DESIGN
Novembro (8, 10, 15 e 17)

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO
(a agendar)

SEGURANÇA DE INFORMAÇÃO NA ÓTICA DO UTILIZADOR
(a agendar)

TECNOLOGIAS DE SEGINFO E CIBERSEGURANÇA
(a agendar)

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.

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.

PROGRAMA DE FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

ENGENHARIA SOCIAL

DURAÇÃO 21 horas

HORÁRIO 09h30 – 12h30

PREÇOS	Associados	Tabela Geral
Engenharia Social		
Nível I (3 horas)	200 €	230 €
Nível II (6 horas)	350 €	402 €
Nível III (12 horas)	600 €	690 €
Programa completo	950 €	1 092 €

FORMAÇÃO AVANÇADA

ENGENHARIA SOCIAL

Nível I

3 horas

Conceitos Elementares de Engenharia Social
- Definições
- Tipologia de atacantes e vítimas
- O processo de *intelligence*
- Tipologia dos ataques
- Factores psicológicos
- Modelo de defesa multinível – a criação da *Firewall* Humana

Nível II

6 horas

Análise de Risco de Engenharia Social
- Definições
- Ativos (Valor) x Ameaças x Vulnerabilidades / Contramedidas
- Risco Aceitável

Análise de Casos Práticos
- Ataques de *phishing, vishinge smishing* – utilização de vídeos e chamadas telefónicas (de ataques simulados)
- Análise das vulnerabilidades utilizadas nos ataques
- Possíveis políticas de segurança de informação que mitiguem os ataques analisados

Nível III

12 horas

Recolha de Informação e Produção de *Intelligence*
- Processo de OSINT (*Open Source Intelligence*)
- Recolha de informação sobre alvo
- Análise da informação recolhida por tipologia
- Produção de *Intelligence*

Planeamento do Ataque
- Matriz de ataques de engenharia social
- Ataques de *phishing, vishing, smishing*–definição teórica dos ataques a desenvolver
- Criação de um plano ataque

Políticas de Segurança
- Análise do risco para a Organização relativamente a:
  - informação recolhida na primeira fase
  - ataques definidos na segunda fase
- Definição de políticas de segurança para mitigar os riscos considerados elevados
- Definição de canais de reporte de incidentes de engenharia social (segurança de sistemas)

Programa de Sensibilização
- Para todas as políticas definidas na terceira fase, definir um plano de sensibilização de colaboradores
- Planeamento do programa e escolha de ferramentas passíveis de facilitar a sensibilização

Case Study

***Case Study* – "Um ataque de CEO *Fraud*"**

Neste *case study* o formando participará ativamente nas fases de recolha e planeamento de um ataque de "CEO *Fraud*" e, com base neste conhecimento, irá desenvolver novas políticas de segurança de informação (ou a melhoria das já existentes), bem como irá planear um programa de sensibilização para a comunicação destas políticas a todo o universo de utilizadores. Os formandos deverão dedicar 1 hora de análise de documentação entregue, fora do horário de formação

ENTIDADE FORMADORA CERTIFICADA

FULL MEMBER OF

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.

PROGRAMA DE FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

SECURITY & PRIVACY BY DESIGN

DURAÇÃO 12 horas

HORÁRIO 09h30 – 12h30

PREÇOS	Associados	Tabela Geral
Security & Privacy by Design		
Nível I (3 horas)	200 €	230 €
Nível II (3 horas)	200 €	230 €
Nível III (3 horas)	350 €	402 €
Programa completo	650 €	747 €

FORMAÇÃO AVANÇADA

SECURITY & PRIVACY BY DESIGN

Nível I **3 horas**	**Segurança e Desenvolvimento de *Software*** • Orientações Gerais para o Desenvolvimento de *Software* Seguro • *Design*, Implementação e Operação de uma Política de Segurança no *Software* • Aquisição, Desenvolvimento e Manutenção de Sistemas
Nível II **3 horas**	**Especificação de Requisitos de SegInfo e Cibersegurança** • Análise e Discussão dos Principais Conceitos • Processo de Captura de Requisitos Funcionais e não Funcionais • Requisitos de Segurança no Desenvolvimento de *Software*
Nível III **6 horas**	**Desenvolvimento Seguro de *Software*** • Principais Vulnerabilidades do *Software* • Segurança de Aplicações WEB • Auditorias e Testes a *Software*

ENTIDADE FORMADORA CERTIFICADA

FULL MEMBER OF

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.

PROGRAMA DE FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

DURAÇÃO 24 horas

HORÁRIO 09h30 – 12h30

PREÇOS	Associados	Tabela Geral
Cibersegurança e Segurança da Informação		
Nível I (3 horas)	200 €	230 €
Nível II (6 horas)	350 €	402 €
Nível III (15 horas)	650 €	747 €
Programa completo	1 000 €	1 150 €

FORMAÇÃO AVANÇADA

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

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.

FULL MEMBER OF

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.

SEGURANÇA DA INFORMAÇÃO NA ÓTICA DO UTILIZADOR

DURAÇÃO 15 horas

HORÁRIO 17h00 – 20h00

PREÇOS	Associados	Tabela Geral
Segurança da informação na Ótica do Utilizador	650 €	747 €

FORMAÇÃO AVANÇADA

SEGURANÇA DA INFORMAÇÃO NA ÓTICA DO UTILIZADOR

Nível I **15 horas**	**Gestão da Informação e de Equipamento Informático** • Gestão Segura da Informação • Criação e Manutenção de *Passwords* Seguras • Segurança Física do Equipamento Informático • Eliminação e Recuperação de Informação
	Engenharia Social e *Phishing* • Definições • Tipologia de atacantes e vítimas • O processo de *intelligence* • Tipologia dos ataques de *phishing, vishinge smishing* – utilização de vídeos e chamadas telefónicas (de ataques simulados) • Factores psicológicos • Modelo de defesa multinível –a criação da *Firewall* Humana • A Gestão da Dor Organizacional
	Internet e Serviços • Proteção da Informação na Internet • Configuração Segura do *Browser* • Teletrabalho • Correio Eletrónico • Redes Públicas Wi-Fi
	Mecanismos Tecnológicos de Segurança • *Hardening* do Sistema Operativo • Mitigação das Vulnerabilidades das Aplicações • Antivírus e Procedimentos com *Malware* • *Firewall* Pessoal • Criptografia Aplicada

ENTIDADE FORMADORA CERTIFICADA

FULL MEMBER OF

PROGRAMA DE FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

TECNOLOGIAS DE SEGINFO E CIBERSEGURANÇA

DURAÇÃO 9 horas

HORÁRIO 09h30 – 12h30

PREÇOS	Associados	Tabela Geral
Tecnologias de SegInfo e Cibersegurança		
Nível I (3 horas)	200 €	230 €
Nível II (3 horas)	200 €	230 €
Nível III (3 horas)	200 €	230 €
Programa completo	500 €	575 €

FORMAÇÃO AVANÇADA

TECNOLOGIAS DE SEGINFO E CIBERSEGURANÇA

Nível I

3 horas

Segurança em Redes de Computadores
- Conceitos de Redes de Computadores
- Funcionamento Geral da Internet
- Principais Abordagens de Cibersegurança

Nível II

3 horas

Controlos Tecnológicos de Cibersegurança
- Controlos Básicos de Cibersegurança
- Controlos Fundamentais de Cibersegurança
- Controlos Organizacionais de Cibersegurança

Nível III

3 horas

Cibersegurança e *Machine Learning*
- Principais Conceitos
  - O *Hacker*, o estatístico e o especialista de segurança
  - Obter, ler e explorar os dados para resolver um problema
  - Desmistificara *Machine Learning* (com exemplos de Cibersegurança)
  - O desafio de usar *Machine Learning* na Cibersegurança
- Deteção de Intrusões, *Big Data* e SIEMs
  - Tipos de Sistemas de Deteção de Intrusão
  - Tecnologias e *Frameworks* para processamento de *Big Data*
  - Aplicação nos Sistemas de Gestão de Eventos de Segurança (SIEM)
- Exemplos práticos
  - Análise exploratória dos dados de segurança
  - Deteção de tráfego anómalo/malicioso com *Machine Learning*
  - Visualizar os dados

ENTIDADE FORMADORA CERTIFICADA

FULL MEMBER OF

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 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.

DGERT ENTIDADE FORMADORA CERTIFICADA

FULL MEMBER OF

EBTN EUROPEAN BANKING & FINANCIAL SERVICES TRAINING ASSOCIATION AISBL