TÉCNICO+
FORMAÇÃO AVANÇADA

EM COOPERAÇÃO COM inesc

Curso de Especialização

Proteção e segurança de dados para profissionais não tecnológicos

A capacidade da aplicação dos regulamentos relativos à segurança informática e à proteção de dados, é, atualmente, uma das áreas de formação mais necessárias. De forma a responder a esta necessidade, o curso cobre as principais competências digitais que os Data Protection Officers (DPOs) e outros quadros profissionais empresariais, devem aprender e compreender para poderem exercer as suas competências específicas, para além de conseguirem manter um diálogo profícuo com os profissionais das Tecnologias da Informação e Comunicação (TIC), nomeadamente os gestores dos sistemas informáticos.

OBJETIVOS

- Dominar as principais tecnologias da informação e comunicação atuais.
- Compreender e aplicar ferramentas, métodos e tecnologias para resolver problemas concretos.
- Ser capaz de desenhar, aplicar e manter políticas de privacidade adequadas, documentação e processos para o exercício dos direitos dos titulares.
- Ser capaz de aferir os riscos para a privacidade dos dados, para além de identificar e executar as melhores práticas, no que diz respeito à identificação dos riscos relacionados com o tratamento dos dados.

DESTINATÁRIOS

Todos os profissionais DPOs com formação de base não tecnológica e todos os profissionais com responsabilidades em atividades que envolvem, ou requerem, segurança e proteção de dados.

Carga Horária Presencial de 30h

17, 18, 24 e 25 junho
1,2,8,9,15 e 16 julho

Campus Alameda

18h00 às 21h00

1500€

2 ECTS

tecnicomais.pt

COORDENAÇÃO

Prof. José Tribolet
É "Distinguished Professor", Catedrático de Sistemas de Informação do Instituto Superior Técnico da Universidade de Lisboa e Presidente do INESC. Os seus interesses académicos envolvem as áreas de Engenharia, Arquitetura, Governação e Transformação Empresarial, com ênfase na Arquitetura da Informação e na Governação da Transformação Digital das Organizações.

Prof. Miguel Pupo Correia
É Professor Associado do Instituto Superior Técnico da Universidade de Lisboa e investigador sénior do INESC-ID. Esteve envolvido em vários projetos de investigação no âmbito da cibersegurança e privacidade, entre os quais se destacam os projetos europeus MAFTIA, CRUTIAL, ReSIST, TCLOUDS, PCAS e SafeCloud. Os seus principais interesses são: blockchain e consenso bizantino; segurança e confiabilidade da cloud; trusted computing; segurança de software; segurança e confiabilidade móvel; deteção de intrusões e big data analytics; e segurança de comunicações.

PLANO DE ESTUDOS

1. Bases Conceptuais Fundamentais | 17 de junho

- Princípios fundamentais da realidade "física" da organização: dos atos realizados pelos atores, aos níveis holísticos de governação e controlo sistémico do todo empresarial
- Introdução aos pilares fundamentais da Arquitetura Empresarial, na vertente operacional: as dimensões Informacional, Funcional e Processual
- Introdução aos pilares fundamentais da Arquitetura Empresarial, na vertente holística: as dimensões do controlo *ex-ante*, da auditoria *ex-post* e da governação sistémica

2. Sistemas Informáticos Atuais

a. Infraestrutura de TI | 18 de junho

- Introdução - definição, evolução, drivers tecnológicos
- Componentes da infraestrutura - hardware, sistemas operativos, software empresarial, armazenamento de dados, redes, plataformas Internet, consultores e integração de sistemas
- Plataformas de hardware: dispositivos móveis, BYOD, virtualização, alojamento partilhado, cloud, computação de elevado desempenho
- Plataformas de software - Linux e código aberto, software para a web, cloud
- Administração da infraestrutura de IT - gestão da mudança, administração e governação, investimento

b. Internet e redes | 25 de junho

- Introdução e componentes de redes - o que é uma rede, principais tecnologias.
- Tipos de redes - digital vs. analógico, LAN / WAN, meios e velocidade de transmissão.
- Internet - endereçamento e arquitetura, serviços, a web.
- Protocolos de comunicação - tecnologias cliente e tecnologias servidor.
- Redes sem fios - redes celulares, Wi-Fi e Bluetooth, RFID e redes de sensores.

c. Bases de Dados | 24 de junho

- Problemas da gestão de dados em ficheiros.
- Principais funcionalidades dos sistemas de gestão de bases de dados.
- Principais tecnologias para processar grandes quantidades de dados.
- Políticas, gestão e qualidade dos dados.

3. Cibersegurança – Introdução e Conceitos | 1 e 2 de julho

- Definição e abrangência da cibersegurança (tecnológica e organizacional)
- Introdução à segurança da informação
- Tipos de vulnerabilidades comuns afetando hardware, software, redes, pessoal, instalações e a organização
- Ameaças típicas e o atual panorama de ameaças – inclui malware, e-mail, web, móvel, wifi, negação de serviço, ransomware, botnets, roubo de identidade, ameaças internas e outras atualmente relevantes.
- Valor da segurança

4. Cibersegurança – Mecanismos e controlos de segurança | 2 e 8 de julho

- Criptografia, certificados digitais e assinatura digital
- Anonimização e pseudoanonimização
- Gestão de identidades, autenticação e controlo de acessos (RBAC, MAC, DAC)
- Segurança de instalações e centros de processamento de dados
- Segurança periférica e de rede – firewalls, DMZs, VPNs, sistemas de deteção e prevenção de intrusões
- Gestão de eventos de segurança (SIEM), registos de eventos e operações (logs)
- Segurança de equipamentos terminais (incluindo equipamentos móveis) – antivírus e antispyware, proteção no acesso internet (browser e e-mail)
- Segurança de servidores, armazenamento e bases de dados – controlo de integridade e registo de operações
- Papel dos utilizadores - formação, sensibilização e comunicação de políticas, regras e boas práticas de segurança
- Qualidade de software e segurança na conceção de sistemas de informação (security by design)

5. Cibersegurança – Avaliação e gestão de segurança | 9 e 15 de julho

- Avaliação e gestão de risco – análise e tratamento
- Auditorias, análise de vulnerabilidades e testes de segurança das componentes humanas e tecnológicas das organizações
- Cadeia de abastecimento
- Outsourcing de segurança
- Segurança de serviços externos (cloud)
- Resposta a Incidentes – Planos de gestão de incidentes, recuperação de desastres e continuidade de negócio, CSIRTs e análise forense
-

6. Gestão do processo do registo de tratamento e Fecho | 16 de julho

- Discussão e síntese das aprendizagens e da sua relevância prática para o exercício da atividade profissional de DPOs

TESTEMUNHOS DE *ALUMNI*

Vim de Braga de propósito para fazer estes cursos e não estou nada arrependida. Acho o curso uma mais-valia, muito denso ao nível do conteúdo, permitindo uma aprendizagem sobre os mais variados aspetos.
Lara Feio, formada em Engenharia

Valeu muito a pena. Acho que o curso é extremamente rico ao nível dos conhecimentos que fornece. Enquanto DPO de um conjunto de entidades públicas e privadas acho extremamente relevante apostarmos neste tipo de formação, se tiver o selo de qualidade do Técnico ainda melhor.
Nuno Pereira