APDPO – Portugal

PROGRAMA

Curso de Especialização Profissional em Engenharia Informática (CEPEI)

Proteção e Segurança de Dados para Profissionais Não Tecnológicos

Consórcio CEPEI - IST/INESC /APDPO

18.09.2018

1. INTRODUÇÃO

O Consórcio CEPEI - Proteção e Segurança de Dados para Profissionais Não Tecnológicos é constituído pelo IST/DEI e INESC. O IST tem a responsabilidade científica e pedagógica dos cursos de especialização profissional ministrados pelo Consórcio CEPEI, sendo estes cursos não conferentes de grau académico.

O Consórcio considera estar em condições de desenvolver esta formação nos exatos termos do pretendido pela APDPO dado que:

- O IST fornece o enquadramento académico, pautado pelos mais distintos padrões científicos e técnicos.
- O INESC detém uma prática de mais de duas décadas de promoção e operacionalização de cursos de formação para altos quadros das melhores e mais conceituadas entidades nacionais e estrangeiras, em íntima colaboração com o seu principal associado académico, o IST.
- A estratégia integrada pelos consorciados assegura que a formação tenha um real impacto na vida prática dos formandos ao serviço das empresas e organizações, contribuindo para um maior enriquecimento do tecido empresarial do País.

2. O CURSO

2.1 OBJETIVOS

O Curso de Especialização Profissional em **Proteção e Segurança de Dados para Profissionais Não Tecnológicos** cobre as principais competências digitais que os DPOs e outros quadros profissionais empresariais com responsabilidades em atividades que envolvem ou requerem segurança e proteção de dados devem aprender e compreender para poderem por um lado exercer cabalmente as suas competências específicas, e por outro manterem diálogo profícuo com os profissionais das Tecnologias da Informação e Comunicação (TIC), nomeadamente os gestores dos sistemas informáticos.

Controlar o risco operacional constitui uma parte essencial de uma supervisão ponderada. Este controlo abrange as operações de identificação, análise e avaliação da segurança, integridade e resiliência das redes e dos sistemas de informação - que incluem requisitos relativos à avaliação dos riscos e a análise detalhada e completa a todos os controlos de referência - e, face aos objetivos de controlo, o apuramento de qual o atual nível de maturidade e de capacidade na aplicabilidade das boas práticas. Esta avaliação, através do modelo de maturidade, permite orientar a organização na subida de nível e na melhoria, de forma incremental, das atividades na Gestão do Risco e Segurança.

Através desta formação ficará consagrada a capacidade dos destinatários poderem desenhar as medidas que forem adequadas e eficazes, assim como a aptidão de poder comprovar que as operações sobre a informação dos titulares dos dados são efetuadas em conformidade com os regulamentos de segurança da recolha e tratamento, incluindo a capacidade de medir a eficácia das medidas adotadas, de acordo com a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares.

A formação integra uma possibilidade de adquirir um conhecimento sólido teórico de conceitos fundamentais nas áreas da Informática e da Arquitetura Informacional e Organizacional diretamente relevantes para os objetivos do curso, associada a uma componente de formação prática vocacionada para a resolução de problemas complexos relacionados com a proteção de dados suportado em normativas técnicas e na legislação em vigor. A formação integra aspetos relacionados com gestão de processos, segurança do tratamento de dados, análise e tratamento de grandes volumes de dados e modelação de sistemas de informação.

De relevar ainda o aspeto da capacitação dos formandos para o diálogo informado e construtivo, e sempre difícil com os profissionais das TICs, nomeadamente de Informática, pela aquisição e compreensão de elementos fundamentais da sua linguagem especializada, que tão frequentemente inibem e mesmo impedem a indispensável comunicação.

A formação está vinculada ao princípio da necessidade de formar quadros que possam cumprir com os princípios de responsabilidade nas organizações e entidades públicas relativamente a proteção dos dados em conformidade com as recomendações referidas pelo Grupo de Trabalho sobre Proteção de Dados do Artigo 29º. A demonstração da conformidade,

na prática, exige a necessidade de dotar as organizações de profissionais devidamente formados, capazes de realizar e acompanhar múltiplas atividades legais, organizativas e tecnológicas, bem como a capacidade de analisar e produzir documentação adequada e manutenção de registos com a finalidade de demonstrar o cumprimento das regras sobre proteção do tratamento dos dados pessoais.

O plano de formação está dividido em módulos com prática em contexto real, de modo a fornecer um conjunto de conhecimentos, aptidões e competências que possam ser diretamente transpostas para as funções desempenhadas pelos formandos nas suas organizações.

Desta forma, apresentam-se seguidamente os principais objetivos de aprendizagem:

- Dominar as principais tecnologias da informação e comunicação atuais.
- Dominar os conceitos de proteção da privacidade dos dados essenciais à execução de projetos de segurança do tratamento.
- Ter sentido crítico na análise dos métodos e ferramentas disponíveis, dos resultados obtidos, para avaliar as qualidades, limitações e aplicabilidade dos mesmos.
- Compreender e aplicar ferramentas, métodos e tecnologias para resolver problemas concretos.
- Comunicar as conclusões dos trabalhos efetuados assim como os pressupostos teóricos e metodológicos subjacentes de forma clara.
- Ter capacidade de aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que os tratamentos dos dados são realizados com segurança.
- Ser capaz de desenhar, aplicar e manter políticas de privacidade adequadas em matéria de proteção de dados na qualidade do responsável pelo tratamento ou subcontratante.
- Ser capaz de fornecer comunicação relativamente ao tratamento dos dados, de forma concisa, transparente, inteligível e de fácil acesso.
- Ser capaz de desenhar, operar e manter a documentação e os processos para o exercício dos direitos dos titulares.
- Ser capaz de aferir os riscos para a privacidade dos dados, resultante do seu tratamento, com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado.

- Ser capaz de identificar e executar as melhores práticas, no que diz respeito à identificação dos riscos relacionados com o tratamento dos dados, sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como a identificação das medidas para a atenuação dos riscos, de acordo com os códigos de conduta que venham a ser aprovados.
- Ser capaz de evitar o tratamento dos dados em violação e preservar a sua segurança, através da capacidade de avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem e a pseudoanonimização de modo a poder assegurar a sua confidencialidade a e integridade, tendo em conta as técnicas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger.

A formação é concebida com base em objetivos estruturantes e fundamentais complementando a formação de licenciados e quadros de modo a permitir exercer funções em áreas diversas da privacidade de dados e segurança da informação.

Pretende-se que o público-alvo adquira as competências relativas à proteção do tratamento da informação e esteja apto a integrar funções verticais e horizontais, mais genéricas, na vertente da proteção de dados, nomeadamente em funções de controlo e operação de conformidade.

Pretende-se ainda capacitar os intervenientes de elaborar políticas relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal envolvido nas operações de tratamento de dados e auditorias correspondentes.

2.2 PROGRAMA

O programa divide-se em cinco partes/módulos, detalhados em seguida.

1º módulo: Bases Conceptuais Fundamentais (3h)

- 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.

2º módulo: Sistemas Informáticos Atuais (9h)

- 2a. Infraestrutura de IT
    - Introdução - definição, evolução, drivers tecnológicos.
    - Componentes da infraestrutura de IT - 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.
- 2b. Internet e redes
    - 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.

- 2c. Bases de Dados
  - 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.

3º módulo: Cibersegurança – Introdução e conceitos (5h)

- 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.

4º módulo: Cibersegurança – Mecanismos e controlos de segurança (5h)

- 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*).

5º módulo: Cibersegurança – Avaliação e gestão de segurança (5h)

- 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.

Fecho do Curso: Discussão e Síntese das Aprendizagens tidas e da sua relevância prática para o exercício da atividade profissional de DPOs. (3h)

2.3 ALINHAMENTO COM O RGPD

Através desta formação, ficará consagrada a capacidade dos destinatários de consolidarem os seus conhecimentos sobre os temas versados e o seu alinhamento com o regulamento geral de proteção de dados (RGPD).

Deste modo ficam habilitados a poderem acompanhar o processo de implementação e manutenção da Arquitetura de segurança das redes e sistemas de informação alinhada com o RGPD, podendo ainda acompanhar a execução das medidas técnicas e organizativas que forem adequadas e eficazes.

2.4 A QUEM SE DESTINA

O curso destina-se em particular a todos os profissionais DPOs com formação de base não tecnológica, e em geral a todos os profissionais com responsabilidades em atividades que envolvem ou requerem segurança e proteção de dados que devem aprender e compreender para poderem por um lado exercer cabalmente as suas competências específicas, e por outro manterem diálogo profícuo com os profissionais das TICs, nomeadamente os informáticos.

2.5 MATERIAL DE APRENDIZAGEM

Os temas são cobertos em aulas presenciais e adicionalmente pela visualização de alguns vídeos, a análise de casos de estudo. a realização de exercícios com perguntas (cujas respostas são revistas por outros participantes) e a participação em fóruns para discussão sobre os temas.

O material de apoio a este curso será disponibilizado na Plataforma Moodle deste CEPEI, através da qual toda a interação não presencial com os alunos se processará.

2.6 PRÉ-REQUISITOS

Não existem pré-requisitos específicos para este curso.

O curso é lecionado em português mas é importante que, para aproveitar ao máximo os conhecimentos que serão transmitidos, os participantes estejam à vontade com a literatura técnica em Inglês. A bibliografia recomendada para o curso está escrita em Inglês.

2.7 NÚMERO DE FORMANDOS

O número ideal recomendado para cada edição do curso é de 20 alunos. O limite é de 30. O IST reserva-se o direito de não realizar o curso caso o número de alunos inscritos seja inferior ao número ideal.

2.8 DURAÇÃO TOTAL

A duração do curso em modo presencial será de 30 horas.

2.9 DATAS DE REALIZAÇÃO E HORÁRIO

A 1ª Edição do curso decorrerá de 22 a 25 de outubro de 2018 entre as 9h e as 18h.

2.10 Organização e recursos a usar

Este é um curso presencial, que inclui exposição dos tópicos do programa, realização de exercícios individualmente e em grupo, e discussão de casos concretos.

As aulas realizar-se-ão nas instalações do Consórcio, na Rua Alves Redol, 9, 9º andar em Lisboa.

2.11 Avaliação

A avaliação é baseada nas respostas dadas nos exercícios realizados no final de cada módulo (60%) e a perguntas sobre um caso de estudo final (40%).

Os participantes com uma nota final igual ou superior a 50% terão direito a um certificado de Pós-Graduação Profissional CEPEI do IST (Instituto Superior Técnico) com a classificação final atribuída.

3 PREÇO

O preço de inscrição no curso é de 1500€ e os associados da APDPO beneficiam de um desconto de 20% sobre este preço.

4. FORMADORES

José Tribolet é "Distinguished Professor", Catedrático de Sistemas de Informação do Instituto Superior Técnico da Universidade de Lisboa e Presidente do INESC. É investigador sénior do INESC-ID. Licenciou-se em Engenharia Eletrotécnica pelo Instituto Superior Técnico e obteve o Mestrado e Doutoramento em Electrical Engineering and Computer Science no MIT, Cambridge, Mass., USA. É Agregado pelo IST em Teoria dos Sistemas. Fez uma Pós-Graduação na Sloan School of Management do MIT durante o ano sabático de 1997-98. Foi Professor Convidade no IWI - the Institute for Information Management da University of St. Gallen na Suiça durante o 2º semestre do ano letivo de 2011-2012.

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. É membro fundador da Academia de Engenharia e do Colégio de Engenharia Informática da Ordem dos Engenheiros. É um dos pioneiros na área emergente de Engenharia Empresarial, tendo orientado com sucesso desde 2007 10 doutoramentos neste novo domínio.

Mantém atividade profissional liberal como Assessor Executivo nos domínios da Arquitetura, Engenharia, Governação e Transformação Empresarial.

Miguel Pupo Correia é Professor Associado do Instituto Superior Técnico da Universidade de Lisboa e investigador sénior do INESC-ID. Tem uma licenciatura e um mestrado em Engenharia Eletrotécnica e de Computadores pelo Instituto Superior Técnico e um Doutoramento em Informática pela Faculdade de Ciências da Universidade de Lisboa.

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. Tem mais de 150 publicações em revistas, conferências e workshops. É co-autor do livro "Segurança no Software", com 2ª edição de 2017.

A sua investigação está focada em diversos aspetos de cibersegurança e confiabilidade, geralmente de sistemas distribuídos, no contexto de alguns domínios de aplicação (blockchain, cloud, dispositivos móveis, infraestruturas críticas). 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.

Nelson Escravana é Diretor da Área de Comunicações e Cibersegurança do INOV INESC Inovação, na qual coordena uma equipa de investigadores e engenheiros afeta à realização de projetos de investigação, desenvolvimento e integração de tecnologia nos campos da cibersegurança ofensiva, resposta a incidentes de cibersegurança, deteção de ciberintrusões em infraestruturas críticas e análise forense digital. É responsável pela realização de auditorias de segurança no âmbito da prevenção e resposta a incidentes, análise e conceção de soluções.

Licenciou-se em Engenharia Informática e de Computadores pelo Instituto Superior Técnico e possui uma especialização em Gestão pelo Instituto Superior de Economia e Gestão.

Possui mais de 20 anos de experiência profissional em telecomunicações e segurança da informação, sendo consultor regular de diversas entidades nacionais e internacionais, entre as quais se contam vários operadores de telecomunicações nacionais, instituições financeiras, Estado Português e a NATO. É regularmente responsável por realizar ações de formação e seminários em cibersegurança no Instituto Superior de Ciências Policiais e Segurança Interna e no Instituto Superior Técnico. Participou em mais de uma dezena de projetos europeus de I&D, entre os quais se destacam os projetos SECUR-ED, ECOSSIAN, DOGANA, COMPACT, ALFA e ASGARD.

Em 2011 foi responsável pela criação da unidade de serviços partilhados do grupo INESC em Lisboa, no qual ainda ocupa funções de Diretor com responsabilidade da equipa de resposta a ciber-incidentes do grupo (CSIRT). É desde 2015 membro dos órgãos sociais do INOV INESC Inovação.

António Gonçalves é Professor Adjunto de Sistemas de Informação no Instituto Politécnico de Setúbal (IPS) e coordenador da Licenciatura em BioInformática do mesmo instituto. É também investigador convidado do INESC-ID no grupo de Sistemas de Apoio à Decisões (IDSS).

Tem uma licenciatura em Engenharia Eletrotécnica e de Computadores pelo Instituto Superior Técnico, um Mestrado e um Doutoramento em Engenharia Informática, pelo mesmo Instituto.

Tem uma vasta experiência em projetos relacionados com a segurança e proteção de dados. Possui várias publicações científicas na área e tem vindo a acompanhar diversas organizações privadas e organismos públicos na implementação das suas políticas de privacidade, proteção de dados e segurança de informação.

Os seu principal interesse está focado na engenharia organizacional, em particular na adoção de boas práticas de proteção de dados e segurança de informação na arquitetura empresarial.

Miguel Mira da Silva é Professor Associado de Sistemas de Informação no Instituto Superior Técnico e coordenador do Mestrado em Informação e Sistemas Empresariais (MISE) que é lecionado a distância e oferecido em conjunto com a Universidade Aberta. É também responsável pela unidade de investigação "Transformação Digital" no INOV INESC Inovação.

Tem uma licenciatura e um mestrado em Engenharia Eletrotécnica e de Computadores pelo Técnico, um Doutoramento em Informática pela Universidade de Glasgow, e um mestrado em gestão (Sloan Fellowship) pela London Business School.

Tem uma larga experiência profissional, tendo criado 5 empresas e estado envolvido no desenvolvimento de diversos novos negócios. Já orientou 5 teses de doutoramento e mais de 100 teses de mestrado, e publicou quatro livros e mais de 230 artigos em revistas e conferências científicas, na sua maioria, internacionais. Já liderou inúmeros projetos científicos, tanto europeus como nacionais, muitos com empresas portuguesas.

Neste momento o seu principal interesse científico está focado na engenharia organizacional, em particular na adoção de boas práticas de gestão com base na arquitetura empresarial.

Pedro Adão é Professor Auxiliar no Departamento de Engenharia Informática (DEI) do Instituto Superior Técnico, Universidade de Lisboa (IST/UL). É Licenciado em Matemática Aplicada e Computação pelo IST (2002) e Doutorado em Matemática pela Universidade Técnica de Lisboa (2006) na área de Métodos Formais para Análise de Protocolos de Segurança. Durante o doutoramento foi exchange-student na Universidade da Pennsylvania, EUA, e research-intern na Microsoft Research em Cambridge, Inglaterra. Tem lecionado as cadeiras de Segurança de Redes e Sistemas, Segurança em Software, Especificação de Software, Qualidade de Software, e Algoritmos e Estruturas de Dados. É Membro do Security and Quantum Information Group do Instituto de Telecomunicações desde 2001. Os seus interesses de investigação na área da Segurança vão desde os fundamentos matemáticos da criptografia, até à segurança de aplicações.

Pedro Adão coordena a equipa de segurança STT (Security Team@Técnico), formada por alunos do IST, que participa em competições internacionais de segurança e que atualmente está classificada no top-50 mundial (top-20 se nos restringirmos apenas as equipas académicas).

ANEXO – TÓPICOS APDPO

A 11 de julho de 2018 a APDPO sugeriu uma série de tópicos de segurança que gostaria de ver contemplados no programa do curso. A tabela abaixo identifica os pontos do programa em que cada um desses tópicos é coberto.

#	Tema	Descrição	1ª	2a	2b	2c	3	4	5
1	RAISING USER AWARENESS	Make each user aware of the privacy and security challenges of the organisation	X				X		
2	AUTHENTICATING USERS	Recognising your users to manage their access rights	X	X				X	
3	ACCESS MANAGEMENT	Only allow access to data that the user really needs	X	X				X	
4	LOGGING ACCESS AND MANAGING INCIDENTS -	Log access and organise incident management procedures to manage incidents allowing to react in the event of data breach (breach of confidentiality, integrity or availability)						X	X
5	SECURING WORKSTATIONS	Prevent fraudulent access, the execution of viruses or remote-control takeover, in particular via the Internet		X			X		
6	SECURING MOBILE DATA PROCESSING	Anticipate data breach following the theft or loss of a mobile equipment			X			X	
7	PROTECTING THE INTERNAL NETWORK	Only authorise the network functions required for the processing implemented	X	X			X	X	
8	SECURING SERVERS	Strengthen the security measures applied to servers		X	X	X			
9	SECURING WEBSITES	Ensure that the basic best practices are applied to websites			X			X	
10	ENSURING CONTINUITY	Carry out regular backups to reduce the effect of undesired loss of data							X
11	ARCHIVING SECURELY	Archive data which is no longer used on a daily basis, but which has not yet reached the end of its data retention period, for example because it is kept to be used in the event of litigation				X		X	X
12	SUPERVISING MAINTENANCE AND DATA DESTRUCTION	Guarantee data security at all times in the life cycle of hardware and software							X
13	MANAGING DATA PROCESSORS	Supervise data security with subcontractors				X		X	X
14	SECURING EXCHANGES WITH OTHER ORGANISATIONS	Strengthen the security of every personal data transmissions						X	X
15	PHYSICAL SECURITY	Strengthen the security of the premises housing IT servers and network equipment		X					X
16	SUPERVISING SOFTWARE DEVELOPMENT	Integrate security and privacy as early as possible into projects			X	X	X		
17	ENCRYPTING, GUARANTEEING INTEGRITY AND SIGNING	Ensure the integrity, confidentiality and authenticity of a piece of information	X					X	