



EDUCAÇÃO

Gabinete do Secretário de Estado Adjunto e da Educação

Despacho n.º 4780/2020

Sumário: Criação e autorização de funcionamento do curso de especialização tecnológica em Cibersegurança no Instituto Profissional de Tecnologias Avançadas para a Formação, L.^{da}

O Decreto-Lei n.º 88/2006, de 23 de maio, alterado pelo Decreto-Lei n.º 113/2014, de 16 de julho, inscreve-se num quadro de política que visa promover o alargamento das competências, aptidões e qualificações dos portugueses, dignificar o ensino e potenciar a criação de novas oportunidades, impulsionando o crescimento sociocultural e económico do País, ao possibilitar uma oferta de recursos humanos qualificados geradores de uma maior competitividade.

Considerando a necessidade de conciliar a vertente do conhecimento, através do ensino e da formação, com a componente da inserção profissional qualificada, os cursos de especialização tecnológica (CET) visam criar novas oportunidades e formação ao longo da vida.

Considerando que a decisão de criação e entrada em funcionamento de um CET num estabelecimento de ensino público, particular ou cooperativo com autonomia ou paralelismo pedagógico que ministre cursos de nível secundário de educação é da competência do ministro da tutela, podendo ser delegada, nos termos do artigo 43.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

Considerando ainda que, nos termos do artigo 42.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual, o pedido foi instruído e analisado pela Agência Nacional para a Qualificação e o Ensino Profissional, I. P., a qual, no âmbito da reorganização dos serviços centrais do Ministério da Educação, assumiu as atribuições da Direção-Geral de Formação Vocacional, designada, nos termos do artigo 41.º do mesmo diploma, como serviço instrutor, pelo Despacho n.º 1647/2007, de 8 de janeiro, publicado no *Diário da República*, 2.ª série, de 1 de fevereiro.

Considerando, por último, que foi ouvida a Comissão Técnica para a Formação Tecnológica Pós-Secundária, nos termos do artigo 34.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

Assim, ao abrigo do artigo 43.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual, determino:

1 — É criado o curso de especialização tecnológica em Cibersegurança, proposto pela Escola Profissional denominada IPTA — Instituto Profissional de Tecnologias Avançadas para a Formação L.^{da}, e autorizado o seu funcionamento nas instalações desta entidade, sitas em Rua Dr. Alves da Veiga, n.º 142, loja, 4000-072 Porto, nos termos do anexo ao presente despacho, que dele faz parte integrante.

2 — O presente despacho é válido por um período de quatro anos, devendo o primeiro ciclo de formação iniciar-se até ao início do ano letivo subsequente à data de entrada em vigor do presente diploma, e os restantes durante o período de vigência.

3 — O presente despacho entra em vigor no dia seguinte ao da sua publicação.

4 — Cumpra-se o disposto no artigo 44.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

7 de abril de 2020. — O Secretário de Estado Adjunto e da Educação, *João Miguel Marques da Costa*.

ANEXO

1 — Instituição de formação:

IPTA — Instituto Profissional de Tecnologias Avançadas para a Formação L.^{da}

2 — Denominação do curso de especialização tecnológica:

Curso de Especialização Tecnológica em Cibersegurança

3 — Área de educação e formação:

481 — Ciências Informáticas

4 — Perfil profissional:

Técnico/a Especialista em Cibersegurança

5 — Descrição geral:

Implementar e gerir plataformas e sistemas de cibersegurança em organizações, bem como intervir em 1.ª linha em incidentes de cibersegurança.

6 — Referencial de competências a adquirir:

Articular diferentes módulos para formar um sistema de computação.

Caracterizar as principais componentes de um sistema operativo.

Identificar as principais componentes dos sistemas operativos (Windows e Unix).

Operar e instalar, configurar e manter sistemas operativos (Windows e Unix).

Modificar e implementar programas para autonomizar tarefas no âmbito dos diversos sistemas operativos.

Aplicar as técnicas de instalação, configuração, administração e apoio de sistemas de gestão de bases de dados estruturadas com segurança.

Utilizar ferramentas complementares de gestão de sistemas e redes, de modo a implementar políticas de segurança definidas nas organizações.

Utilizar ferramentas de gestão de sistemas e redes, de modo a detetar falhas de segurança, problemas técnicos e corrigi-los.

Utilizar as várias tecnologias de infraestruturas de rede.

Planear, instalar, manter e gerir uma rede LAN.

Identificar e analisar as ameaças às plataformas de cibersegurança.

Definir e aplicar políticas de segurança (ativas e passivas), incluindo redes e sistemas.

Configurar ferramentas e mecanismos de segurança de acordo com a natureza das ameaças à cibersegurança.

Identificar a legislação relevante e os procedimentos a adotar para a salvaguarda e análise de informação relativa à recolha de evidências.

Utilizar ferramentas especializadas na recolha de *logs*, nos seus diferentes formatos e salvaguardá-los de forma a garantir a sua utilização como meio de prova numa análise forense.

Analisar *logs* de sistemas operativos, de serviços, tratamento e produção de relatórios.

Criar VPN *site to site*, *site to cliente* de forma segura.

Efetuar a análise com captura de pacotes através do *wireshark* (dados, voz e vídeo).

Analisar e monitorizar *logs* de IDS e IPS.

Utilizar ferramentas de extração, transporte e processamento de *logs*.

Utilizar ferramentas especializadas na análise de *logs*.

Elaborar *scripts* em linguagens de *scripting* para análise mais especializada de texto e *delogs*.

Adaptar os procedimentos de segurança de informação de acordo com o tipo de ameaças e incidentes

Adotar procedimentos destinados a garantir a ciberdefesa das organizações e fazer face à ocorrência de ciberataques.

Utilizar ferramentas especializadas na recolha, salvaguarda e pré-análise de informação e evidências, para posterior tratamento, em conformidade com as regras de rigor forense.

Elaborar e apresentar relatórios de investigação forense.



7 — Plano de Formação:

Plano de Formação do Curso de Especialização Tecnológica em Cibersegurança

Componentes de Formação (1)	Área de Educação e Formação (2)	Unidade de formação (3)	Carga Horária		ECTS (6)
			Total (4)	Contacto (5)	
Geral e Científica . . .	Filosofia Ética	Ética e deontologia profissionais	37,5	25	1,5
	Estatística	Probabilidades e estatística	75	50	3
	Matemática	Matemática	75	50	3
	Ciências Empresariais . . .	Empresa — estrutura e funções	37,5	25	1,5
		<i>Subtotal</i>	225	150	9
	Ciências Informáticas . . .	Primeiros conceitos de programação e algoritmia e estruturas de controlo num programa informático	37,5	25	1,5
		Legislação, segurança e privacidade	37,5	25	1,5
		Inglês Técnico	75	50	3
		Programação — Algoritmos	37,5	25	1,5
		Bases de Dados — conceitos	37,5	25	1,5
		Sistema Operativo cliente (plataforma proprietária)	37,5	25	1,5
		Sistema Operativo servidor (plataforma proprietária)	37,5	25	1,5
		Hardware e redes de computadores	37,5	25	1,5
		Redes de computadores (avançado)	37,5	25	1,5
		Instalação de redes locais	75	50	3
		Serviços de rede	37,5	25	1,5
		Modelos de gestão de redes e de suporte a clientes	37,5	25	1,5
		Fundamentos de cibersegurança	37,5	25	1,5
		Tecnologias de análise de evidências	75	50	3
		Introdução à programação aplicada à cibersegurança	37,5	25	1,5
		Introdução às técnicas de análise de evidências	75	50	3
		Análise de vulnerabilidades — iniciação	75	50	3
		Análise de vulnerabilidades — desenvolvimento	75	50	3
		Introdução à cibersegurança e à ciberdefesa	75	50	3
		Enquadramento operacional da cibersegurança	75	50	3
		Cibersegurança ativa	75	50	3
		Wargamming	75	50	3
		<i>Subtotal</i>	1 200	800	48
Em Contexto de Trabalho.		Formação Prática em Contexto de Trabalho	560	560	22
	<i>Total</i>		1 985	1 510	79

Notas

Na coluna (4) indicam-se as horas totais de trabalho.

Na coluna (5) indicam-se as horas de contacto, de acordo com o disposto na alínea *d*) do artigo 2.º e no n.º 1 do artigo 15.º, ambos do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

Na coluna (6) indicam-se os créditos segundo o *European Credit Transfer and Accumulation System* (sistema europeu de transferência e acumulação de créditos), de acordo com a definição expressa na alínea *b*) do artigo 2.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

8 — Condições de acesso e ingresso:

- Ser titular de um curso do ensino secundário ou equivalente;
- Os indivíduos que tenham tido aprovação em todas as disciplinas do 10.º e 11.º anos e que tenham estado inscritos no 12.º ano de um curso secundário ou de habilitação legalmente equivalente não o tenham concluído;
- Os titulares de uma qualificação profissional de nível 3;
- Os titulares de um diploma de especialização tecnológica ou de um diploma de ensino superior que pretendam requalificar-se profissionalmente.

e) Aprovação nas áreas curriculares, no âmbito do curso do ensino secundário ou equivalente, que concluiu ou frequentou, fixadas como referencial de competências de ingresso: Conteúdos do Plano de Formação Adicional.

8.1 — O ingresso no CET dos indivíduos a que se referem as alíneas a), b) e c), do n.º 8, que não cumpram a condição definida na alínea e), do mesmo número, fica condicionado à aprovação em unidades curriculares que integrem as áreas curriculares identificadas.

8.2 — Para efeitos do disposto no ponto anterior, cabe ao IPTA — Instituto Profissional de Tecnologias Avançadas para a Formação L.^{da}, aferir as competências de ingresso através da realização de provas de avaliação.

8.3 — Os candidatos ao ingresso no CET que se encontrem na situação prevista no n.º 8.1 e não tenham obtido aprovação nas provas de avaliação, devem frequentar, no todo ou em parte, de acordo com análise curricular e os resultados das provas de avaliação, o Plano de Formação Adicional definido no ponto 11 do presente anexo.

8.4 — Sem prejuízo do estabelecido no ponto anterior, os formandos que não sejam titulares de um curso de ensino secundário ou de habilitação legalmente equivalente, devem cumprir integralmente o Plano de Formação Adicional constante do ponto 11 do presente anexo.

9 — A formação adicional estabelecida no ponto 11 do presente anexo é parte integrante do plano de formação do CET.

10 — Número máximo de formandos:

10.1 — Em cada admissão de novos formandos: 30/ciclo.

10.2 — Na inscrição em simultâneo no curso: 60.

11 — Plano de Formação Adicional (a que se reportam os artigos 8.º e 16.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual):

Componentes de Formação (1)	Unidade de formação (2)	Carga Horária		ECTS (5)
		Total (3)	Contacto (4)	
Geral e Científica	Língua Portuguesa	75	50	3
	Língua Inglesa	75	50	3
	Matemática	150	100	6
Tecnológica	Introdução às redes e sistemas informáticos.	150	100	6
Total		450	300	18

Notas

Na coluna (3) indicam-se as horas totais de trabalho.

Na coluna (4) indicam-se as horas de contacto, de acordo com o disposto na alínea d) do artigo 2.º e nos termos do n.º 1 do artigo 15.º ambos do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

Na coluna (5) indicam-se os créditos segundo o *European Credit Transfer and Accumulation System* (sistema europeu de transferência e acumulação de créditos), de acordo com a definição expressa na alínea b) do artigo 2.º do Decreto-Lei n.º 88/2006, de 23 de maio, na sua redação atual.

313175374