



INSTITUTO POLITÉCNICO DE BRAGANÇA

Despacho n.º 2440/2021

Sumário: Altera o plano de estudos do curso técnico superior profissional de Cibersegurança, da Escola Superior de Tecnologia e Gestão.

De acordo com o disposto nos artigos 75.º a 80.º do Decreto-Lei n.º 74/2006, de 24 de março, alterado e republicado pelo Decreto-Lei n.º 65/2018, de 16/08, tendo em conta as recomendações da Agência de Avaliação e Acreditação do Ensino Superior (A3ES), é alterada a declaração de retificação n.º 251/2019, de 19 de março referente à alteração plano de estudos do curso técnico superior profissional de Cibersegurança, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança. As alterações foram registadas, na Direção-Geral do Ensino Superior, com o número R/Cr 54.1/2017, de 24 de abril de 2020.

24 de fevereiro de 2021. — O Presidente, *Orlando Isidoro Afonso Rodrigues*.

ANEXO

- 1 — Instituição de ensino superior: Instituto Politécnico de Bragança — Escola Superior de Tecnologia e de Gestão de Bragança (3043).
- 2 — Curso Técnico Superior Profissional: Cibersegurança (T316).
- 3 — Área de educação e formação: 481 — Ciências informáticas.
- 4 — Condições de Ingresso: A seguinte área: Matemática.
- 5 — Localidades de ministração: Bragança.
- 6 — Número máximo de estudantes:
 - 6.1 — A admitir em cada ano letivo: 25;
 - 6.2 — Total de inscritos em simultâneo: 58.
- 7 — Perfil Profissional:

Descrição geral: Projetar, implementar e administrar infraestruturas, serviços de rede e sistemas por forma a torná-los mais seguros, bem como instalar, administrar e utilizar serviços e sistemas de cibersegurança e intervir em primeira linha na deteção e resposta a incidentes de segurança informática, de forma autónoma ou em equipa, contribuindo para a minimização do risco e para a otimização de processos e recursos das organizações alvo.

Atividades principais:

- a) Planear, instalar e gerir infraestruturas de rede locais e de área alargada de média dimensão de forma segura;
- b) Efetuar trabalhos de instalação e administração de sistemas operativos e serviços aplicativos num ambiente de rede, seguindo procedimentos seguros;
- c) Implementar políticas de segurança em redes e sistemas informáticos;
- d) Analisar eventos e detetar ameaças à segurança informática;
- e) Gerir e responder a eventos e incidentes de cibersegurança;
- f) Realizar atividades de recolha e tratamento de informação e evidências, utilizando ferramentas especializadas;
- g) Auditar a segurança de sistemas, redes e aplicações informáticas, de modo a identificar e mitigar ameaças;
- h) Colaborar com especialistas na preparação de relatórios forenses seguindo as melhores práticas.

8 — Referencial de competências:

Conhecimentos:

- a) Conhecimentos abrangentes de matemática, álgebra e algoritmia;
- b) Conhecimentos abrangentes de técnicas de comunicação, relacionamento interpessoal e motivação;



- c) Conhecimentos abrangentes sobre o funcionamento das redes de dados (tecnologias de rede, arquiteturas protocolares, equipamentos de interligação, aplicações e serviços);
- d) Conhecimentos especializados de desenvolvimento de ferramentas para automatizar tarefas na área da cibersegurança;
- e) Conhecimentos especializados de instalação e administração de sistemas operativos e respetivos serviços de forma segura;
- f) Conhecimentos especializados de instalação, administração e utilização de soluções de cibersegurança;
- g) Conhecimentos especializados de planeamento, instalação e administração de redes de dados;
- h) Conhecimentos especializados de sistemas de gestão de bases de dados;
- i) Conhecimentos especializados relacionados com a análise de vulnerabilidades e evidências;
- j) Conhecimentos especializados sobre ameaças, riscos à cibersegurança e suas formas de mitigação;
- k) Conhecimentos especializados sobre as melhores práticas na área de cibersegurança.

Aptidões:

- a) Analisar políticas de segurança e implementar mecanismos e controlos adequados;
- b) Aplicar raciocínio lógico e implementar algoritmos para a resolução de problemas concretos;
- c) Auditar e realizar testes de intrusão, utilizando diversas técnicas de análise, de modo a detetar e conter ameaças à cibersegurança;
- d) Configurar e gerir sistemas operativos e serviços em rede, utilizando metodologias seguras;
- e) Consultar, interpretar e redigir documentação técnica, incluindo em língua inglesa;
- f) Detetar eventos e reagir aos incidentes de segurança;
- g) Implementar e administrar infraestruturas de rede locais e de área alargada de média dimensão de forma segura;
- h) Implementar, configurar e colocar em produção sistemas de cibersegurança nas organizações;
- i) Monitorizar eventos para identificar ameaças à cibersegurança;
- j) Recolher e tratar dados para a elaboração de relatórios forenses;
- k) Utilizar ferramentas para a recolha e tratamento de informação e evidências.

Atitudes:

- a) Demonstrar capacidade analítica e pensamento lógico;
- b) Demonstrar capacidade de adaptação à evolução dos procedimentos e das tecnologias;
- c) Demonstrar capacidade de comunicação;
- d) Demonstrar capacidade de gestão do tempo e de cumprimento de objetivos;
- e) Demonstrar capacidade de relacionamento interpessoal, nomeadamente ao nível da gestão de conflitos e da motivação;
- f) Demonstrar capacidade de relacionamento técnico e funcional com colaboradores e parceiros;
- g) Demonstrar iniciativa e autonomia para a resolução de problemas de natureza técnica;
- h) Demonstrar iniciativa na obtenção de soluções adequadas para a resolução de problemas.

9 — Estrutura curricular:

Área de educação e formação	Créditos	% do total de créditos
481 — Ciências informáticas	117	98 %
461 — Matemática	3	3 %
<i>Total</i>	120	100 %

10 — Plano de estudos:

Unidade curricular (1)	Área de educação e formação (2)	Componente de formação (3)	Ano curricular (4)	Duração (5)	Horas de contacto (6)	Das quais de aplicação (7)	Outras horas de trabalho (8)	Das quais correspondem apenas ao estágio (8.1)	Horas de trabalho totais (9)=(6)+(8)	Créditos (10)
Introdução aos Sistemas Informáticos	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Introdução à Programação de Scripts	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Normas de Segurança e de Privacidade	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Introdução às Redes	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Introdução à Cibersegurança	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Introdução às Bases de Dados	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Matemática	461 — Matemática	Geral e científica	1.º ano	Semestral	30	0	51	0	81	3
Projeto Integrado I	481 — Ciências informáticas	Técnica	1.º ano	Semestral	60	60	102	0	162	6
Administração de Bases de Dados	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Administração de Sistemas I	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Redes de Área Local	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Redes Empresariais	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Administração de Sistemas II	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Programação Aplicada à Cibersegurança	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Análise de Vulnerabilidades	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Análise de Evidências	481 — Ciências informáticas	Técnica	1.º ano	Trimestral	30	23	51	0	81	3
Projeto Integrado II	481 — Ciências informáticas	Técnica	1.º ano	Semestral	90	90	153	0	243	9
Introdução à IoT	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Segurança em Redes Informáticas	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Laboratórios de Segurança em Redes Informáticas	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Administração de Serviços de Rede	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Robustecimento de Sistemas	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Cibersegurança Ativa	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Wargaming	481 — Ciências informáticas	Técnica	2.º ano	Trimestral	30	23	51	0	81	3
Projeto Integrado III	481 — Ciências informáticas	Técnica	2.º ano	Semestral	90	90	153	0	243	9
Estágio	481 — Ciências informáticas	Em contexto de trabalho.	2.º ano	Semestral			810	810	810	30
<i>Total</i>					900	723	2 340	810	3 240	120

Na coluna (2) indica-se a área de educação e formação de acordo com a Portaria n.º 256/2005, de 16 de março.

Na coluna (3) indica-se a componente de formação de acordo com o constante no artigo 40.º-J do Decreto-Lei n.º 74/2006, de 24 de março, na redação dada pelo Decreto-Lei n.º 63/2016, de 13 de setembro.

Na coluna (6) indicam-se as horas de contacto, de acordo com a definição constante do Decreto-Lei n.º 42/2005, de 22 de fevereiro, alterado pelo Decreto-Lei n.º 107/2008, de 25 de junho.

Na coluna (7) indicam-se as horas de aplicação de acordo com o disposto no artigo 40.º-N do Decreto-Lei n.º 74/2006, de 24 de março, na redação dada pelo Decreto-Lei n.º 63/2016, de 13 de setembro.

Na coluna (8) indicam-se as outras horas de trabalho de acordo com o constante no artigo 5.º do Decreto-Lei n.º 42/2005, de 22 de fevereiro, alterado pelo Decreto-Lei n.º 107/2008, de 25 de junho.

Na coluna (8.1) indica-se o número de horas dedicadas ao estágio.

Na coluna (9) indicam-se as horas de trabalho totais de acordo com o constante no artigo 5.º do Decreto-Lei n.º 42/2005, de 22 de fevereiro, alterado pelo Decreto-Lei n.º 107/2008, de 25 de junho.

Na coluna (10) indicam-se os créditos segundo o *European Credit Transfer and Accumulation System* (sistema europeu de transferência e acumulação de créditos), fixados de acordo com o disposto no Decreto-Lei n.º 42/2005, de 22 de fevereiro, alterado pelo Decreto-Lei n.º 107/2008, de 25 de junho.

314009658