

CONTEXTO DA AVALIAÇÃO DO PEDIDO DE ACREDITAÇÃO DE NOVO CICLO DE ESTUDOS

Nos termos do regime jurídico da avaliação do ensino superior (Lei n.º 38/2007, de 16 de agosto), a entrada em funcionamento de um novo ciclo de estudos exige a sua acreditação prévia pela A3ES.

O processo de acreditação prévia de novos ciclos de estudo (Processo NCE) tem por elemento fundamental o pedido de acreditação elaborado pela instituição avaliada, submetido na plataforma da Agência através do Guião PAPNCE.

O pedido é avaliado por uma Comissão de Avaliação Externa (CAE), composta por especialistas selecionados pela Agência com base no seu currículo e experiência e apoiada por um funcionário da Agência, que atua como gestor do procedimento. A CAE analisa o pedido à luz dos critérios aplicáveis, publicitados, designadamente, em apêndice ao presente guião.

A CAE, usando o formulário eletrónico apropriado, prepara, sob supervisão do seu Presidente, a versão preliminar do relatório de avaliação do pedido de acreditação. A Agência remete o relatório preliminar à instituição de ensino superior para apreciação e eventual pronúncia, no prazo regularmente fixado. A Comissão, face à pronúncia apresentada, poderá rever o relatório preliminar, se assim o entender, competindo-lhe aprovar a sua versão final e submetê-la na plataforma da Agência.

Compete ao Conselho de Administração a deliberação final em termos de acreditação. Na formulação da deliberação, o Conselho de Administração terá em consideração o relatório final da CAE e, havendo ordens e associações profissionais relevantes, será igualmente considerado o seu parecer. O Conselho de Administração pode, porém, tomar decisões não coincidentes com a recomendação da CAE, com o intuito de assegurar a equidade e o equilíbrio das decisões finais. Assim, o Conselho de Administração poderá deliberar, de forma fundamentada, em discordância favorável (menos exigente que a Comissão) ou desfavorável (mais exigente do que a Comissão) em relação à recomendação da CAE.

Composição da CAE: A composição da CAE que avaliou o presente pedido de acreditação do ciclo de estudos é a seguinte (os CV dos peritos podem ser consultados na página da Agência, no separador Acreditação e Auditoria / Peritos):

Altair Olivo Santin

Manuel Martins Barata (Presidente)

Rui Miguel Silva

1. Caracterização Geral

1.1.a. Outras Instituições de Ensino Superior (proposta em associação com instituições nacionais) (PT)

[sem resposta]

1.1.a. Outras Instituições de Ensino Superior (proposta em associação com instituições nacionais) (EN)

[sem resposta]

1.1.b. Outras Instituições de Ensino Superior (proposta em associação com instituições estrangeiras)

[sem resposta]

1.1.c. Outras Instituições (em cooperação)

[sem resposta]

1.2.a. Identificação da(s) unidade(s) orgânica(s) da(s) entidade(s) parceira(s) (faculdade, escola, instituto,

[sem resposta]

1.2.a. Identificação da(s) unidade(s) orgânica(s) da(s) entidade(s) parceira(s) (faculdade, escola, instituto,

[sem resposta]

1.3. Designação do ciclo de estudos. (PT)

Cibersegurança Aplicada

1.3. Designação do ciclo de estudos. (EN)

Applied Cybersecurity

1.4. Grau. (PT)

Mestrado - 2º ciclo

1.4. Grau. (EN)

Master's Degree - 2nd Cycle

1.5. Área científica predominante do ciclo de estudos. (PT)

Engenharia Informática

1.5. Área científica predominante do ciclo de estudos. (EN)

Computer Engineering

1.6.1. Classificação CNAEF - primeira área fundamental

[0481] Ciências Informáticas
Informática
Ciências, Matemática e Informática

1.6.2. Classificação CNAEF - segunda área fundamental, se aplicável

[sem resposta]

1.6.3. Classificação CNAEF - terceira área fundamental, se aplicável

[sem resposta]

1.7. Número de créditos ECTS necessário à obtenção do grau.

60.0

1.8. Duração do ciclo de estudos.

1 ano

1.8.1. Outra

[sem resposta]

1.9. Número máximo de admissões proposto

30.0

1.10. Condições específicas de ingresso (alínea f) do artigo 3.º do Decreto-Lei n.º 74/2006, de 24 de março

- 1) Titulares do grau de licenciado ou equivalente legal nas áreas de Tecnologias de Informação e áreas afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
 - 2) Titulares de um grau académico superior estrangeiro nas áreas de Tecnologias de Informação e áreas afins que seja reconhecido como satisfazendo os objetivos do grau de licenciado pelo Conselho Técnico-Científico, nas mesmas áreas de 1) e afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
 - 3) Detentores de currículo académico, científico ou profissional, cuja capacidade seja reconhecida pelo CTC da escola, nas áreas referidas em 1), com experiência profissional, mínima de 5 anos, devidamente comprovada;
- Os candidatos serão avaliados e seriadados considerando a sua formação curricular e a natureza e relevância da sua experiência profissional, sendo privilegiados profissionais, executivos, quadros e dirigentes que pretendam estruturar conhecimento e o aplicar em Cibersegurança.

1.10. Condições específicas de ingresso (alínea f) do artigo 3.º do Decreto-Lei n.º 74/2006, de 24 de março

- 1) Holders of a bachelor's degree or legal equivalent in the areas of Computer Engineering and related areas, with at least 5 years' professional experience duly proven;
 - 2) Holders of a foreign higher academic degree that is recognized as meeting the objectives of the Bachelor's degree by the Scientific-Technical Council, in the same areas as 1) and with at least 5 years' professional experience duly proven;
 - 3) Holders of an academic, scientific or professional curriculum, whose capacity is recognized by the Scientific- Technical Council of the School, in the areas referred to in 1), with at least 5 years' professional experience duly proven.
- Candidates will be evaluated and graded considering their curriculum background and the nature and relevance of their professional experience, with professionals, executives, staff and managers with or without training in management who wish to structure knowledge and applying it in Cybersecurity.

1.10.1. Apreciação da adequação e conformidade legal das condições específicas

Existem, é adequado e cumpre os requisitos legais.

1.10.1.1. Evidências que fundamentam a apreciação expressa. (PT)

- 1) Titulares do grau de licenciado ou equivalente legal nas áreas de Tecnologias de Informação e áreas afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
- 2) Titulares de um grau académico superior estrangeiro nas áreas de Tecnologias de Informação e áreas afins que seja reconhecido como satisfazendo os objetivos do grau de licenciado pelo Conselho Técnico-Científico, nas mesmas áreas de 1) e afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
- 3) Detentores de currículo académico, científico ou profissional, cuja capacidade seja reconhecida pelo CTC da escola, nas áreas referidas em 1), com experiência profissional, mínima de 5 anos, devidamente comprovada; Os candidatos serão avaliados e seriadados considerando a sua formação curricular e a natureza e relevância da sua experiência profissional.

Cumprem os requisitos fixados no Artigo 17.º e na alínea iv) do n.º 2 do Artigo 18.º do Decreto-Lei n.º 74/2006, de 24 de março.

1.10.1.1. Evidências que fundamentam a apreciação expressa. (EN)

- 1) Holders of a bachelor's degree or legal equivalent in the areas of Computer Engineering and related areas, with at least 5 years' professional experience duly proven;
- 2) Holders of a foreign higher academic degree that is recognized as meeting the objectives of the Bachelor's degree by the Scientific-Technical Council, in the same areas as 1) and with at least 5 years' professional experience duly proven;
- 3) Holders of an academic, scientific or professional curriculum, whose capacity is recognized by the Scientific- Technical Council of the School, in the areas referred to in 1), with at least 5 years' professional experience duly proven. Candidates will be evaluated and graded considering their curriculum background and the nature and relevance of their professional experience.

They meet the requirements set out in Article 17 and in subparagraph iv) of paragraph 2 of Article 18 of Decree-Law no. 74/2006, of 24 March.

1.11. Modalidade do ensino

Presencial (Decreto-Lei n.º 65/2018, de 16 de agosto)

1.11.1. Regime de funcionamento, se presencial

Pós-laboral

1.11.1.a. Se outro, especifique. (PT)

[sem resposta]

1.11.1.a. Se outro, especifique. (EN)

[sem resposta]

1.12. Local onde o ciclo de estudos será ministrado (se aplicável). (PT)

Campus do IPCA - Barcelos

1.12. Local onde o ciclo de estudos será ministrado (se aplicável). (EN)

Campus do IPCA - Barcelos

1.13. Regulamento de creditação de formação académica e de experiência profissional, publicado em Diário

[1.13. Despacho-n.º9030_2020_RA_IPCA-40-45_compressed.pdf](#) | PDF | 199.1 Kb

1.13.1. Apreciação da existência e conformidade do regulamento de creditação com os preceitos legais

Existe, é adequado e cumpre os requisitos legais.

1.13.1.1. Evidências que fundamentam a apreciação expressa. (PT)

O regulamento de creditação de formação e experiência profissional encontra-se especificado no capítulo V do Despacho n.º 9030/2020. Cumpre todos os requisitos legais em vigor.

1.13.1.1. Evidências que fundamentam a apreciação expressa. (EN)

The regulation for accreditation of training and professional experience is specified in Chapter V of Order No. 9030/2020. It complies with all legal requirements in force.

1.14. Observações. (PT)

[sem resposta]

1.14. Observações. (EN)

[sem resposta]

2. Formalização do pedido

2.1. Deliberações dos órgãos que legal e estatutariamente foram ouvidos no processo de criação do ciclo de

Existem, são adequadas e cumprem os requisitos legais.

2.1.1. Evidências que fundamentam a apreciação expressa (PT)

Documentos apresentados:

- Extrato da ata nº 33, de 14 de novembro de 2022 do Conselho Académico do IPCA. No ponto nº 4 é dado parecer favorável ao Mestrado em Cibersegurança Aplicada;*
- Minuta de Ata nº 14 de 11 de novembro de 2022 do Conselho Técnico-Científico (CTC) da Escola Superior de Tecnologia (EST) do IPCA. No ponto sete é dado parecer favorável ao mestrado em Cibersegurança Aplicada ;*
- Extrato da Minuta da ata nº 13 de 11 de novembro de 2022 do Conselho Pedagógico (CP) da EST do IPCA. No ponto nove aprova a proposta do Mestrado em Mestrado em Cibersegurança Aplicada.*

2.1.1. Evidências que fundamentam a apreciação expressa (EN)

Documents submitted:

- Extract from the minutes nº 33, of November 14th 2022 of the Academic Council of the IPCA. In point four, a favorable vote is given to the Master in Applied Cybersecurity;*
- Extract of Minutes nº 14, of 11th November 2022 of the Technical-Scientific Council (TSC) of the Higher School of Technology (EST) of the IPCA in point seven approve the proposal for the master in Applied Cybersecurity;*
- Extract from the Minutes nº 13 of the Pedagogical Council (PC) of the EST of the IPCA. In point nine, it approves the proposal for the master's in Applied Cybersecurity.*

3. Âmbito e objetivos do programa de estudos. Adequação ao projeto

3.1. Objetivos gerais definidos para o ciclo de estudos.

Sim

3.2. Objetivos de aprendizagem (conhecimentos, aptidões e competências) a desenvolver pelos estudantes.

Sim

3.3. Justificar a adequação do objeto e objetivos do ciclo de estudos à modalidade do ensino.

Sim

3.4. Justificar a inserção do ciclo de estudos na estratégia institucional de oferta formativa.

Sim

3.5. Designação do ciclo de estudos.

Sim

3.6.1. Apreciação global (PT)

Os objetivos gerais visam completar a formação adquirida num primeiro ciclo de estudos em Engenharia Informática e áreas afins, com pelo menos 5 anos de experiência profissional na área do ciclo de estudos, dotando os estudantes de competências que lhes permitam organizar, implementar, coordenar e controlar um sistema informático com características de segurança, numa organização.

Os objetivos de aprendizagem a desenvolver pelos estudantes estão claramente definidos e suficientemente desenvolvidos. Contemplam: as principais normas no âmbito da Cibersegurança; técnicas de inteligência artificial e de algoritmos criptográficos; legislação aplicável e principais falhas de segurança. Os objetivos de aprendizagem apresentados estão em linha com os conhecimentos e prática que os estudantes devem desenvolver para se atingir os objetivos gerais do ciclo de estudos.

O IPCA é uma Instituição de Ensino Superior Público com intervenção nas áreas das tecnologias tendo como missão contribuir para o desenvolvimento da sociedade, estimular a criação cultural, a investigação e pesquisa aplicadas.

A designação do ciclo de estudos é adequada face aos objetivos gerais e de aprendizagem apresentados.

3.6.1. Apreciação global (EN)

The general objectives aim to complete the training acquired in a first study programme in Computer Engineering and related areas, with at least 5 years of professional experience in the area of the study programme, providing students with skills that allow them to organize, implement, coordinate and control a computer system with security features in an organization.

The learning objectives to be developed by the students are clearly defined and sufficiently developed. They include: the main norms in the context of Cybersecurity; artificial intelligence techniques and cryptographic algorithms; applicable legislation and major security flaws. The presented learning objectives are in line with the knowledge and practice that students must develop in order to achieve the general objectives of the study programme.

IPCA is a Public Higher Education Institution intervening in the areas of technology with the mission of contributing to the development of society, stimulating cultural creation, research and applied research.

The designation of the study programme is adequate in view of the general and learning objectives presented.

3.6.2. Pontos fortes (PT)

- A importância da Cibersegurança e necessidades emergentes de técnicos capazes de a assegurar;
- Ciclo de estudos apelativo para a formação ao longo da vida;
- Bom enquadramento nos programas de Recuperação e Resiliência e STEAM.

3.6.2. Pontos fortes (EN)

- The importance of Cybersecurity and the emerging needs of technicians capable of ensuring it;
- Appealing cycle of studies for lifelong training;

3.6.3. Pontos fracos (PT)

Nada a assinalar.

3.6.3. Pontos fracos (EN)

Nothing to report.

4. Desenvolvimento Curricular

4.1. Áreas Científicas.

4.2. Unidades curriculares do ciclo de estudos.

4.2.1. Objetivos de aprendizagem das unidades curriculares.

Sim

4.2.2 Conteúdos programáticos das unidades curriculares.

Em parte

4.3. Unidades curriculares do ciclo de estudos (opções).

4.4. Percursos do ciclo de estudos.

4.4.1. Estrutura curricular.

Sim

4.4.2 Plano de estudos.

Sim

4.5.1. Justificação do desenho curricular.

Sim

4.5.1.2. Percentagem de créditos ECTS de unidades curriculares lecionadas predominantemente a**4.5.2. Metodologias e fundamentação****4.5.2.1. Metodologia de ensino e aprendizagem****4.5.2.1.1. Modelo pedagógico que constitui o referencial para a organização do processo de ensino e***Sim***4.5.2.1.2. Anexos do modelo pedagógico.****4.5.2.1.3. Adequação das metodologias de ensino e aprendizagem aos objetivos de aprendizagem.***Sim***4.5.2.1.4. Identificação das formas de garantia da justeza, fiabilidade e acessibilidade das metodologias e***Sim***4.5.2.1.5. Avaliação da aprendizagem dos estudantes.***Sim***4.5.2.1.6. Acompanhamento do percurso e do sucesso académico dos estudantes.***Sim***4.5.2.1.7. Participação dos estudantes em atividades científicas (quando aplicável).***Sim***4.5.2.2. Fundamentação do número total de créditos ECTS do ciclo de estudos.****4.5.2.2.1. Fundamentação do número total de créditos ECTS do ciclo de estudos.***Sim***4.5.2.2.2. Forma de verificação de que a carga média de trabalho que será necessária aos estudantes***Sim***4.5.2.2.3. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de***Sim*

4.6.1. Apreciação global (PT)

O desenvolvimento curricular está enquadrado numa lógica suportada em três linhas curriculares, nomeadamente:

(i) uma no domínio do Desenvolvimento de Software, com duas unidades curriculares, sendo uma sobre criptografia e outra sobre desenvolvimento de software seguro, ambas abordadas numa perspetiva prática sustentadas em conteúdos programáticos teóricos bem organizados, o que permitirá aos alunos uma consolidação dos conhecimentos adquiridos, adequada à proposta do ciclo de estudos;

(ii) outra no domínio das Redes de Computadores e Administração de Sistemas no contexto da Cibersegurança, com quatro unidades curriculares, sendo que uma delas incide sobre a utilização de técnicas de Inteligência Artificial no âmbito da Cibersegurança numa perspetiva de otimização de ferramentas de cibersegurança;

(iii) e outra nos domínios da Segurança Organizacional e do Direito, com três unidades curriculares, sendo uma sobre Segurança da Informação em Organizações que faz parte do percurso obrigatório do curso e duas outras, das quais os alunos devem escolher apenas uma, sendo uma focada nas questões do Direito como as Leis da Cibersegurança e do Cibercrime, que se enquadra perfeitamente na justificação apresentada do desenvolvimento curricular, e a outra sobre Auditoria Informática, que apresenta alguma sobreposição com a unidade curricular de Segurança da Informação em Organizações, e que portanto, a sua contribuição para o aumento do conhecimento dos alunos será menor, sugere-se a eliminação da unidade curricular de Auditoria Informática, deixando de existir as opções, ficando a unidade curricular de Direito e Ética na Cibersegurança como obrigatória, pois considera-se que os alunos não frequentarem esta unidade curricular não cumprem os Objetivos de aprendizagem definidos na secção 3.2 da proposta de ciclo de estudos, por exemplo no objetivo definido como "Legislação atual e aplicável".

Relativamente ao conteúdo das unidades curriculares apresentam-se as seguintes notas:

(i) na unidade curricular de Criptografia Aplicada à Cibersegurança é referido nos objetivos de aprendizagem "Aplicar técnicas de criptoanálise", contudo nenhum dos conteúdos programáticos refere este tópico;

(ii) na unidade curricular de Inteligência Artificial aplicada à Cibersegurança, a avaliação é feita com base na escrita de um artigo com qualidade de apresentação numa conferência, contudo este método de avaliação contrasta com os métodos das outras unidades curriculares, que privilegiam o desenvolvimento de trabalhos práticos para efeitos de avaliação, como estímulo ao conhecimento prático das matérias; acresce que na justificação do desenho curricular, esta unidade curricular é apresentada tendo como objetivo o "aumento do desempenho das ferramentas", pelo que as metodologias de avaliação deveriam estar suportadas nestas bases de enquadramento do curso; contudo, este método de avaliação poderá ser entendido como um compromisso ao estímulo da atividade científica, sendo esse o caso, considera-se adequado, mas os resultados deverão ser quantificáveis na reavaliação do ciclo de estudos.

(iii) na unidade curricular de Laboratório de Testes de Intrusão, o conjunto de conteúdos programáticos é excessivo para o tempo disponível de 20 horas de contacto; comparativamente a outras unidades curriculares, esta unidade curricular deveria ter mais horas de contacto, ou pelo menos, mais horas de trabalho autónomo; caso contrário, será muito difícil haver uma correspondência entre os conteúdos programáticos e os objetivos de aprendizagem; por outro lado, a existência do tópico da Criptografia não faz sentido nesta unidade curricular, pois existe uma unidade curricular unicamente dedicada à Criptografia;

(iv) na unidade curricular de Segurança da Informação em Organizações, o foco incide sobre a gestão da segurança da informação nas organizações, abordando a gestão do risco, as boas práticas e os controlos, tendo como base as normas da família ISO 27000 e do NIST, sendo ainda referidas matérias no âmbito da governança como a delineação de estratégias para a cibersegurança com alinhamento com o plano estratégico da organização; contudo nos conteúdos programáticos apenas se identificam matérias relacionadas com a gestão da segurança da informação nas organizações, não sendo focadas as matérias no âmbito da governança;

Relativamente aos cálculos do tempo médio de trabalho necessário por unidade de ECTS apresentados na secção 4.5.2.2.2 (Forma de verificação de que a carga média de trabalho que será necessária aos estudantes corresponde ao estimado em créditos ECTS) de 26,6 horas, conflitua com a base do cálculo que se apresenta na unidade curricular de Estágio / Projeto de 750, pois dá 28,2 ECTS e esta unidade curricular apresenta 30 ECTS; contudo, analisado a distribuição de ECTS pelas unidades curriculares e considerando 25 horas por unidade de ECTS, os valores apresentados estão todos corretos, existindo portanto apenas incongruência com o valor de 26,6 horas apresentado na secção 4.5.2.2.2.

Uma última nota relativa ao número de horas de contacto semanais, pois sendo o ciclo de estudos proposto para regime pós-laboral, com uma carga de 240 horas de contacto por semestre, a que correspondem 16 horas de contacto semanal, poderá ser muito exigente para os alunos; esta questão deverá ser ponderada, considerando a possibilidade de aproveitar os sábados para maximizar o rendimento dos alunos.

4.6.1. Apreciação global (EN)

Curriculum development is framed in a logic supported by three curricular lines, namely:

(i) one in the field of Software Development, with two curricular units, one on cryptography and the other on secure software development, both approached from a practical perspective supported by well-organized theoretical syllabus contents, which will allow students to consolidate their knowledge acquired, adequate to the proposal of the study programme;

(ii) another in the field of Computer Networks and Systems Administration in the context of Cybersecurity, with four curricular units, one of which focuses on the use of Artificial Intelligence techniques in the context of Cybersecurity from a perspective of optimizing cybersecurity tools;

(iii) and another in the fields of Organizational Security and Law, with three curricular units, one on Information Security in Organizations which is part of the mandatory course path and two others, from which students must choose only one, one of which focused on legal issues such as the Laws of Cybersecurity and Cybercrime, which fits perfectly in the presented justification of the curricular development, and the other on Computer Audit, which presents some overlap with the curricular unit of Information Security in Organizations, and therefore its contribution to increasing students' knowledge will be smaller, it is suggested to eliminate the curricular unit of Computer Auditing, no longer existing options, leaving the curricular unit of Law and Ethics in Cybersecurity as mandatory, as it is considered that students who do not attend this curricular unit do not meet the learning objectives defined in section 3.2 of the study programme proposal, for example in the objective defined as "Current and applicable legislation".

Regarding the content of the curricular units, the following notes are presented:

(i) in the Cryptography Applied to Cybersecurity curricular unit it is mentioned in the learning objectives "Applying cryptanalysis techniques", however none of the syllabus mentions this topic;

(ii) in the curricular unit of Artificial Intelligence applied to Cybersecurity, the evaluation is based on the writing of an article with quality of presentation in a conference, however this evaluation method contrasts with the methods of the other curricular units, which privilege the development of practical assignments for assessment purposes, as a stimulus to practical knowledge of the subjects; in addition, in the justification of the curricular design, this curricular unit is presented with the objective of "increasing the performance of the tools", so that the evaluation methodologies should be supported in these bases of framework of the course; however, this assessment method may be understood as a commitment to stimulating scientific activity, which being the case, it is considered adequate, but the results should be quantifiable in the reassessment of the study programme.

(iii) in the Intrusion Testing Laboratory curricular unit, the set of syllabus contents is excessive for the available time of 20 contact hours; compared to other curricular units, this curricular unit should have more contact hours, or at least more hours of autonomous work; otherwise, it will be very difficult to have a correspondence between the syllabus contents and the learning objectives; on the other hand, the existence of the topic of Cryptography does not make sense in this curricular unit, as there is a curricular unit solely dedicated to Cryptography;

(iv) in the Information Security in Organizations curricular unit, the focus is on the management of information security in organizations, addressing risk management, good practices and controls, based on the ISO 27000 family standards and the NIST, also mentioning matters within the scope of governance such as the delineation of strategies for cybersecurity in line with the organization's strategic plan; however, in the syllabus, only subjects related to the management of information security in organizations are identified, not focusing on subjects within the scope of governance;

Regarding the calculations of the average workload required per unit of ECTS presented in section 4.5.2.2.2 (Method of verifying that the average workload that will be required for students corresponds to the estimate in ECTS credits) of 26.6 hours, conflicts with the basis of the calculation presented in the 750 Internship / Project curricular unit, since it gives 28.2 ECTS and this curricular unit presents 30 ECTS; however, analyzing the distribution of ECTS by curricular units and considering 25 hours per ECTS unit, the values presented are all correct, therefore there is only inconsistency with the value of 26.6 hours presented in section 4.5.2.2.2.

A final note on the number of contact hours per week, as the study cycle is proposed for an after-work regime, with a load of 240 contact hours per semester, which corresponds to 16 hours of contact per week, it could be very demanding for the students; this issue should be considered, considering the possibility of taking advantage of Saturdays to maximize student performance.

4.6.2. Pontos fortes (PT)

A estrutura curricular proposta.

4.6.2. Pontos fortes (EN)

The proposed curriculum structure.

4.6.3. Pontos fracos (PT)

A carga horária excessiva para o regime pós-laboral.

4.6.3. Pontos fracos (EN)

The excessive workload for the after-work regime.

5. Corpo Docente

5.1.1. Coordenação do ciclo de estudos.

Em parte

5.1.2. Adequação da carga horária.

Sim

5.2.1. Cumprimento de requisitos legais.

Sim

5.2.2. Estabilidade do corpo docente.

Sim

5.2.3. Dinâmica de formação do corpo docente.

Sim

5.3. Avaliação do pessoal docente.

Sim

5.4.1. Apreciação global (PT)

O docente responsável pelo ciclo de estudos é doutorado em Engenharia Informática com formação e currículo científico em Engenharia Informática. É no entanto desejável que apresente uma lista de publicações em revistas de Cibersegurança Aplicada mais forte.

O corpo docente é constituído por 8,7 ETI e não integra nenhum docente com o Título de Especialista. Da análise às fichas curriculares dos docentes, verifica-se que o serviço docente atribuído é adequado. Contudo convém notar que o serviço docente indicado diz apenas respeito a outros ciclos de estudos e ocupa já cerca de 60% do horário letivo semanal completo. Existe um docente contratado a 15% que não indicou serviço docente; presume-se que irá colaborar neste ciclo de estudos. Verifica-se o cumprimento dos requisitos legais: corpo docente próprio (80,46%), academicamente qualificado (88,51%) e especializado (59,20%). Assim verificou-se que a percentagem de docentes doutores especializados nestas duas áreas científicas é superior ao mínimo de 50% exigido.

Existe estabilidade do corpo docente por um período superior a três anos: os docentes contratados a 100% são docentes de carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018 (80,46%).

Existe um docente inscrito em programas de doutoramento há mais de um ano.

O Pessoal docente é avaliado pelo Regulamento consagrado no Despacho n.º 11965/2010, publicado em Diário da República, 2.ª série - N.º 142 - 23 de Julho de 2010, revisto e republicado conforme Declaração de Retificação N.º 1312/2014 publicado no Diário da República, 2.ª série, N.º 246 de 22 de dezembro. Cumpre os requisitos legais.

5.4.1. Apreciação global (EN)

The professor responsible for the study programme holds a Ph.D. in Computer Engineering with training and a scientific curriculum in Computer Engineering. However, it is desirable that he presents a stronger list of publications in Applied Cybersecurity journals.

The teaching staff is made up of 8.7 FTE and does not integrate any teacher with the Title of Specialist. From the analysis of the teachers' CVs, it appears that the assigned teaching service is adequate. However, it should be noted that the indicated teaching service concerns only other study programmes and already occupies around 60% of the full weekly teaching schedule. There is a teacher contracted at 15% who did not indicate teaching service; it is assumed that he will collaborate in this study programme.

Compliance with legal requirements is verified: own faculty (80.46%), academically qualified (88.51%) and specialized (59.20%). Thus, it was verified that the percentage of doctoral professors specialized in these two scientific areas is higher than the minimum of 50% required.

There is stability of the faculty for a period of more than three years: 80.46% of the professors hired are career professors (Art. 3, paragraph k) of DL-74/2006, in the wording established by DL-65/2018 (80, 46%).

There is a professor enrolled in doctoral programs for over a year.

Teaching staff is evaluated by the Regulation enshrined in Dispatch No. 11965/2010, published in Diário da República, 2nd series - No. 142 - July 23, 2010, revised and republished in accordance with Declaration of Rectification No. 1312/2014 published in the Diário da República, 2nd series, No. 246 of 22 December. Complies with legal requirements.

5.4.2. Pontos fortes (PT)

Todos os docentes encontram-se integrados em centros de I&D acreditados pela FCT com muito bom ou excelente.

5.4.2. Pontos fortes (EN)

All teachers are integrated in R&D centers accredited by FCT with very good or excellent.

5.4.3. Pontos fracos (PT)

Nada a assinalar.

5.4.3. Pontos fracos (EN)

Nothing to report.

6. Pessoal técnico, administrativo e de gestão.

6.1. Adequação em número.

Sim

6.2. Qualificação profissional e técnica.

Sim

6.3. Avaliação do pessoal técnico, administrativo e de gestão.

Sim

6.4. Apreciação global do pessoal técnico, administrativo e de gestão.

6.4.1. Apreciação global (PT)

O número e o regime de trabalho do pessoal não-docente parecem corresponder às necessidades do ciclo de estudos. Para além do apoio dado pelos serviços centrais do IPCA, a EST conta com um chefe de divisão e três colaboradores administrativos. Destes 4 colaboradores, dois possuem formação superior (licenciatura) e dois têm como habilitação o ensino secundário (12ºano).

São avaliados de acordo com o SIADAP e é promovida a formação contínua.

6.4.1. Apreciação global (EN)

The number and work regime of non-teaching staff seems to correspond to the needs of the cycle of studies. In addition to the support provided by the central services of the IPCA, EST has a division head and three administrative employees. Of these five employees, two have higher education (degree) and two have secondary education (12th year) as qualifications.

They are evaluated according to the SIADAP and continuous training is promoted.

6.4.2. Pontos fortes (PT)

Nada a assinalar.

6.4.2. Pontos fortes (EN)

Nothing to report.

6.4.3. Pontos fracos (PT)

Nada a assinalar.

6.4.3. Pontos fracos (EN)

Nothing to report.

7. Instalações e Equipamentos

7.1. Instalações.

Sim

7.2. Sistemas tecnológicos e recursos digitais.

Sim

7.3. Equipamentos.

Sim

7.4. Apreciação global das instalações e equipamentos.

7.4.1. Apreciação global (PT)

A proposta refere a existência de sete salas de aulas diversos gabinetes de docentes, uma sala de computadores e um auditório. Adicionalmente são referidos os laboratórios MFactory Lab, Internet Of Things, Automação e Robótica, Redes, Desenvolvimento de Jogos Digitais, Eletrónica, Ensaios e Caracterização, Instrumentação Médica e mais três associados ao centro de investigação da EST. Os equipamentos referidos parecem ser adequados às necessidades do ciclo de estudos..

7.4.1. Apreciação global (EN)

The proposal refers to the existence of seven classrooms, several faculty offices, a computer room and an auditorium. Additionally, the MFactory Lab, Internet Of Things, Automation and Robotics, Networks, Digital Game Development, Electronics, Testing and Characterization, Medical Instrumentation and three other laboratories associated with the EST research center are mentioned. The referred equipment seems to be adequate to the needs of the cycle of studies.

7.4.2. Pontos fortes (PT)

Infraestrutura de suporte à atividade letiva adequada.

7.4.2. Pontos fortes (EN)

Support infrastructure adequate for the teaching activity.

7.4.3. Pontos fracos (PT)

Nada a assinalar.

7.4.3. Pontos fracos (EN)

Nothing to report.

8. Atividades de investigação e desenvolvimento e/ou de formação avançada e desenvolvimento profissional de alto nível.

8.1. Unidade(s) de investigação, no ramo de conhecimento ou especialidade do ciclo de estudos.

Em parte

8.2. Integração em projetos e parcerias nacionais e internacionais.

Em parte

8.3. Produção científica.

Em parte

8.4. Atividades de desenvolvimento, formação avançada e desenvolvimento profissional de alto nível e/ou

Em parte

8.5. Apreciação global das investigação e desenvolvimento e/ou de formação avançada e desenvolvimento**8.5.1. Apreciação global (PT)**

Para avaliar tudo o que os docentes fazem para mostrar que estão actualizados na área ou têm a sua autoria reconhecida em projectos ou artigos, esta análise considerou 3 indicadores: produção científica, bolsas de projectos e formação (cursos) ou qualificações nos últimos 5 anos. Em geral, há publicações científicas em revistas/journals ou conferências com revisão por pares, o que se observa em cerca de 90% dos casos de docentes. Apenas 1 docentes não têm produção registada no ORCID. No entanto, do ponto de vista da pesquisa de impacto (publicações indexadas de renome), esta foi observada em apenas 70% dos casos para os docentes do curso (apenas 2 docentes têm 2+ publicações no Q1 - ocupado pelo top 25% das revistas, no Scimago Journal & Country Rank), mas outros 2 docentes tem ao menos 1 publicação Q1, junto com outros publicações em journal. No entanto, 50% dos docentes não tem publicações publicações indexadas de impacto, sendo que 2 deste 5 pesquisadores pelo menos têm bolsas para projectos em curso. Os outros 3 docentes (30% dos professores do curso) não têm indicadores que mostrem estar atualizados com o perfil investigativo recomendado para atuar num curso de mestrado.

8.5.1. Apreciação global (EN)

In order to evaluate all that the lecturers, do to show that they are up to date in the area or have their authorship recognized in projects or papers, this analysis considered 3 indicators: scientific production, project grants and training (courses) or qualifications in the last 5 years. In general, there are scientific publications in peer-reviewed journals or conferences, which is observed in about 90% of the course lecturers' cases. Only 1 lecturer has no production registered in ORCID. However, from the point of view of impact research (reputable indexed publications), this was observed in only 70% of the cases for the course lecturers, but only 2 lecturers have 2+ publications in Q1 - occupied by the top 25% of journals, in Scimago Journal & Country Rank; additionally other 2 lecturers have at least 1 Q1 publication, along with other journal publications. However, 50% of the faculty have no impact indexed publications, and 2 of these 5 researchers at least have grants for ongoing projects. The other 3 lecturers (30% of the course faculty) do not have indicators that show they are up to date with the investigative profile recommended for a master's course.

8.5.2. Pontos fortes (PT)

A maioria (90%) dos professores vê a necessidade de se manter actualizada na área da cibersegurança e 70% deles distinguiram-se pela escrita de artigos científicos ou pela apresentação de propostas de desenvolvimento que obtiveram subsídios para projectos.

8.5.2. Pontos fortes (EN)

The majority (90%) of lecturers see the need to stay up to date in cybersecurity area, and 70% of them have distinguished themselves by writing scientific papers or making development proposals that have been awarded project grants.

8.5.3. Pontos fracos (PT)

Apenas 40% dos docentes têm pelo menos 1 publicação no Q1 - ocupado pelo top 25% das revistas no Scimago Journal & Country Rank. Para além disso, existem vários pontos de atenção em torno destas publicações de investigação, por exemplo, vários autores publicam na mesma revista ou o mesmo investigador publica várias vezes na mesma revista, observa-se também várias publicações de impacto fora da área da cibersegurança. É importante notar que, embora seja possível, em alguns casos, publicações feitas repetidamente com muitos autores chamarem a atenção, também é importante notar que não é bem visto publicações em revistas consideradas predatórias e se isso for feito com muitos autores fica ainda mais estranho do ponto de vista autoral. É importante ter um perfil de pesquisador para fazer parte do corpo docente de um programa de mestrado, mas 30% dos docentes do curso precisam ser estimulados a desenvolver esse perfil. A proposta não demonstra claramente a integração de actividades científicas, tecnológicas e artísticas em projectos e/ou parcerias nacionais e internacionais. Não são referidos projectos significativos de cibersegurança.

8.5.3. Pontos fracos (EN)

Only 40% of lecturers have at least 1 publication in Q1 - occupied by the top 25% of journals in the Scimago Journal & Country Rank. Furthermore, there are several points of attention around these research publications, for example, several authors publish in the same journal or the same researcher publishes several times in the same journal, it is also observed several impact publications outside the cybersecurity area. It is important to note that, although it is possible, in some cases, publications made repeatedly with many authors draw attention, it is also important to note that it is not well seen publications in journals considered predatory and if this is done with many authors it gets even weirder from the authorial point of view. It is important to have a researcher profile to be part of the teaching staff of a master's program, but 30% of the course lecturers need to be encouraged to develop this profile. The proposal does not clearly demonstrate the integration of scientific, technological and artistic activities in national and international projects and/or partnerships. No significant cyber security projects are mentioned.

9. Política de proteção de dados (regulamento (ue) n.º 679/2016, de 27 de abril transposto para a lei n.º 58/2019, de 8 de agosto).

Política de proteção de dados

Sim

10. Comparação com ciclos de estudos de referência no espaço europeu de ensino superior (ees).

10.1. Ciclos de estudos similares em instituições de referência do Espaço Europeu de Ensino Superior

Em parte

10.2. Comparação com objetivos de aprendizagem de ciclos de estudos similares.

Em parte

10.3. Apreciação global do enquadramento no Espaço Europeu de Ensino Superior.

10.3.1. Apreciação global (PT)

Pesquisamos no site <https://tus.ie/courses/> e no google e não conseguimos encontrar o curso de Mestrado em Redes de Computadores e Segurança da TUS -- parceria IPCA na rede RUN-EU, mencionado como vital em várias secções da proposta. Em comparação com outras instituições citadas na proposta é importante mencionar a necessidade de protagonismo e autonomia do curso proposto dentro das parcerias, pois percebemos uma certa fragilidade no hall de conhecimentos específicos em cibersegurança de vários docentes do curso. Isso pode deixar o curso em uma situação difícil, já que ele é de curta duração, apenas 1 ano, e, portanto, depende muito das experiências diversas dos profissionais que vêm do mercado. Refletindo sobre identificamos o seguinte ponto de atenção: se o curso depender de profissionais com grande experiência na área de cibersegurança, será que eles se sentirão motivados a fazer o curso, já que dominam a área?

É importante mencionamos que o curso pretende ter mestres com a competência "Monitorizar e avaliar a eficiência dos controlos de cibersegurança adoptados por uma organização com o objectivo de garantir que estes fornecem o nível de segurança desejado". Observando as unidades curriculares, Auditoria e Segurança de Redes e Administração de Sistemas poderiam cobrir este tema, mas talvez a carga horária não seja suficiente, principalmente porque os níveis adequados dependem de políticas que necessitam de planos, planeamento, políticas e processos, por exemplo, que seriam adquiridos numa unidade curricular de governação, que o curso não oferece.

Identificamos mais um ponto crítico na proposta que vem do seguinte objetivo "Delinear uma estratégia para a Cibersegurança, destacando a visão, missão e objetivos, e garantindo o alinhamento com o plano estratégico da organização". Como mencionado não há suporte com tópicos nas unidades curriculares para desenvolver esta competência, pois no mínimo seria necessária uma UC de governança em cibersegurança para desenvolver este tema. Observamos que o curso é abordado assim nos centros de CE referência mencionados na proposta no semestre 1 do estágio 1 do curso de Mestrado em Cibersegurança - Universidade Tecnológica de Munster; governação e segurança da informação do Mestrado em Cibersegurança - Universidade de Northumbria, ou Gestão da Segurança da Informação do Mestrado em Cibersegurança e Resiliência, Universidade de Ciências Aplicadas de St.

10.3.1. Apreciação global (EN)

We could not find the Master in Computer Networks and Security of the TUS -- IPCA partnership in the RUN-EU network, which is mentioned as essential in several sections of the proposal, by searching the website <https://tus.ie/courses/> and Google. Compared to other institutions mentioned in the proposal, it is important to mention the need for protagonism and autonomy of the proposed master within the partnerships. Because we noticed a certain weakness in the cybersecurity know-how of several master lecturers. This can put the course in a difficult situation, since it is short, only 1 year. Therefore, it depends a lot on the diverse experiences of professionals coming from the market. After thinking about it, we have come to the following point of attention: If the course relies on professionals with a lot of experience in the field of cybersecurity, will they have the motivation to take the course, since they dominate the field?

Notably, the course states that those graduating with this competency will "monitor and evaluate the effectiveness of an organization's cybersecurity controls and ensure that they provide the desired level of security." Looking at the master units, Auditing and Network Security and Systems Administration could cover this topic, but the load may not be enough, mainly because the appropriate levels depend on policies that require plans, cybersecurity strategy, architecture, and management process, for example, which would be acquired in a Governance curricular units that the course does not offer.

We see another critical point in the proposal that comes from the following objective, "Outline a strategy for cybersecurity, highlighting the vision, mission, and goals and ensuring alignment with the organization's strategic plan." As noted above, since at a minimum a Cybersecurity Governance curricular units would be required to develop this topic, there is no support for topics in the curricular units to develop this competency. The courses are therefore addressed in the CE reference centers mentioned in the proposal in stage 1 - Semester 1 of the Master in Cybersecurity - TU Münster, Governance and Information Security of the Master in Cybersecurity - Northumbria University, or Information Security Management of the Master in Cybersecurity and Resilience, University of Applied Sciences St. George's University.

10.3.2. Pontos fortes (PT)

Segundo o ISC2, existe um défice de mão-de-obra de cerca de 317.000 postos de trabalho na região EMEA (Europa, África e Médio Oriente). Por conseguinte, a oferta de mais um curso de mestrado em CiberSegurança contribui de forma importante para colmatar este défice.

10.3.2. Pontos fortes (EN)

There is a labour gap of approximately 317,000 jobs in the EMEA (Europe, Africa and the Middle East) region, according to ISC2. Therefore, offering another master in CyberSecurity makes an important contribution to closing this gap.

10.3.3. Pontos fracos (PT)

Consideramos importante que os proponentes façam um estudo mais aprofundado dos EEES de cibersegurança, em especial das instituições citadas na secção "ciclos de estudos existentes nas instituições de referência", pois tal como apontado na secção 10.3.1 existem várias inconsistências na avaliação comparativa.

10.3.3. Pontos fracos (EN)

We consider it important for the proponents to do a more in-depth study of the cybersecurity EEES, especially of the institutions cited in the "existing study cycles in benchmark institutions" section, because as pointed out in section 10.3.1 there are several inconsistencies in the benchmarking.

11. Estágios e/ou períodos de formação em serviço (quando aplicável).

11.1. Locais de estágio e/ou formação em serviço.

Não

11.2. Orientadores externos.

11.3. Plano de distribuição dos estudantes e Recursos Institucionais.

11.3.1. Plano de distribuição dos estudantes pelos locais de estágio e/ou formação em serviço

11.3.2. Recursos da instituição para o acompanhamento dos estudantes.

Sim

11.4. Mecanismos de avaliação e seleção dos orientadores cooperantes de estágio e/ou formação em

Não

11.5. Garantia da qualidade dos estágios e períodos de formação em serviço.

Sim

11.6. Apreciação global das condições de estágio ou formação em serviço.

11.6.1. Apreciação global (PT)

Embora na secção 11.3.2 da proposta de ciclo de estudos se refira que existem "diversos protocolos de cooperação com empresas nacionais e internacionais", na secção 11.1 são apresentados apenas 6 protocolos com entidades disponíveis para receber alunos do ciclo de estudos para realizar a unidade curricular de Estágio Projeto; das 8 entradas apresentadas, duas são repetidas.

Considerando o número total de trinta vagas para o ciclo de estudo, admitindo que metade destes alunos escolhe a realização de Estágio, é necessário que três das seis entidades tenha capacidade para receber em simultâneo dois alunos de Estágio, e as outras três entidades tenham capacidade para receber em simultâneo três alunos de Estágio. Configura-se excessivo. Recomenda-se o aumento do número de Protocolos com entidades que possam receber alunos de Estágio, ou a redução do número total de vagas do ciclo de estudos.

Por outro lado, de acordo com o artigo 6º do Regulamento da Unidade Curricular de Dissertação/Projeto/Estágio dos Cursos de Mestrado do IPCA, apresentado na proposta de ciclo de estudos, a orientação nas entidades receptoras de Estágios deverá ser assegurada por uma pessoa com grau de doutor, mestre, ou título de especialista com provas públicas, ou ainda, um profissional de mérito na área científica do relatório de estágio desde de que reconhecido pelo conselho técnico-científico da respetiva escola; contudo dos 6 protocolos apresentados, verifica-se que apenas dois estão nas condições do regulamento.

É necessário o aumento do número de protocolos de cooperação com entidades receptoras de Estágios do ciclo de estudos, de acordo com o regulamento supra-referido.

Nota: existe ainda uma gralha numa das entidades duplicadas, concretamente na entidade Squarenet, onde numa das entradas se indica uma experiência de 7 anos e noutra uma experiência de 8 anos por parte da pessoa na empresa que poderá orientar os Estágios.

11.6.1. Apreciação global (EN)

Although in section 11.3.2 of the study programme proposal it is mentioned that there are "various cooperation protocols with national and international companies", in section 11.1 only 6 protocols are presented with entities available to receive students from the study programme to carry out the Project Internship curricular unit; of the 8 entries presented, two are repeated.

Considering the total number of thirty vacancies for the study programme, admitting that half of these students choose to carry out an Internship, it is necessary that three of the six entities have the capacity to simultaneously receive two Internship students, and the other three entities have the capacity to simultaneously receive three Internship students. It sets up excessive. It is recommended to increase the number of Protocols with entities that can receive Internship students, or to reduce the total number of vacancies in the study programme.

On the other hand, in accordance with article 6 of the Regulation for the Dissertation/Project/Internship of IPCA's Master's Courses, presented in the study programme proposal, guidance at entities receiving Internships must be ensured by a person with degree of doctor, master, or specialist title with public evidence, or a professional of merit in the scientific area of the internship report, provided that it is recognized by the technical-scientific council of the respective school; however, of the 6 protocols presented, it appears that only two are in compliance with the regulations.

It is necessary to increase the number of cooperation protocols with entities that receive Internships of the study cycle, in accordance with the aforementioned regulation.

Note: there is still a typo in one of the duplicate entities, specifically in the Squarenet entity, where one of the entries indicates 7 years of experience and another 8 years of experience on the part of the person in the company who will be able to guide the Internships.

Although in section 11.3.2 of the study cycle proposal it is mentioned that there are "various cooperation protocols with national and international companies", in section 11.1 only 6 protocols are presented with entities available to receive students from the study programme to carry out the Project Internship curricular unit; of the 8 entries presented, two are repeated.

Considering the total number of thirty vacancies for the study programme, admitting that half of these students choose to carry out an Internship, it is necessary that three of the six entities have the capacity to simultaneously receive two Internship students, and the other three entities have the capacity to simultaneously receive three Internship students. It sets up excessive. It is recommended to increase the number of Protocols with entities that can receive Internship students, or to reduce the total number of vacancies in the study cycle.

On the other hand, in accordance with article 6 of the Regulation for the Dissertation/Project/Internship of IPCA's Master's Courses, presented in the study cycle proposal, guidance at entities receiving Internships must be ensured by a person with degree of doctor, master, or specialist title with public evidence, or a professional of merit in the scientific area of the internship report, provided that it is recognized by the technical-scientific council of the respective school; however, of the 6 protocols presented, it appears that only two are in compliance with the regulations.

It is necessary to increase the number of cooperation protocols with entities that receive Internships of the study programme, in accordance with the aforementioned regulation.

Note: there is still a typo in one of the duplicate entities, specifically in the Squarenet entity, where one of the entries indicates 7 years of experience and another 8 years of experience on the part of the person in the company who will be able to guide the Internships.

11.6.2. Pontos fortes (PT)

Nada a referir.

11.6.2. Pontos fortes (EN)

Nothing to report.

11.6.3. Pontos fracos (PT)

Número insuficiente de protocolos com entidades receptoras de alunos de Estágio, considerando o número total de vagas para o ciclo de estudos.

11.6.3. Pontos fracos (EN)

Insufficient number of protocols with institutions that receive Internship students, considering the total number of vacancies for the study cycle.

12. Observações finais.

12.1. Apreciação da pronúncia da instituição (quando aplicável) (PT)

[sem resposta]

12.1. Apreciação da pronúncia da instituição (quando aplicável) (EN)

[sem resposta]

12.2. Observações (PT)

[sem resposta]

12.2. Observações (EN)

[sem resposta]

12.3. PDF (500KB).

[sem resposta]

13. Conclusões

13.1. Apreciação global da proposta do novo ciclo de estudos (PT)

O ciclo de estudos em Cibersegurança Aplicada, tem por objetivo completar a formação adquirida num primeiro ciclo de estudos em Engenharia Informática e áreas afins, com pelo menos 5 anos de experiência profissional na área do ciclo de estudos, dotando os estudantes de competências que lhes permitam organizar, implementar, coordenar e controlar um sistema informático com características de segurança, numa organização.

Está em consonância com a missão da Instituição, cumpre os requisitos legais em termos de estrutura curricular, plano de estudos, ECTS e carga de trabalho envolvida e enquadra-se no projeto educativo, científico e cultural da Instituição. A Instituição parece dispor dos recursos necessários em termos de Instalações, Laboratórios, Equipamentos, Biblioteca e pessoal técnico necessários para assegurar o seu bom funcionamento. O ciclo de estudos tem associado um corpo docente que cumpre os requisitos legais: corpo docente próprio, academicamente qualificado e especializado com afetação de serviço docente adequada.

Verifica-se uma percentagem boa (66,7%) de docentes envolvidos em unidades de investigação acreditadas pela FCT com classificação de Muito Bom ou Excelente, porém o número de publicações em revistas internacionais na área principal do ciclo de estudos é ainda baixo necessitando de ser reforçado.

Sendo um ciclo de estudos vocacionado para trabalhadores com cinco ou mais anos de experiência profissional, dada a sua natureza, as perspectivas de procura por parte dos estudante afiguram-se ser boas.

Da análise à sua estrutura curricular e conteúdos programáticos das unidades curriculares verificou-se que estas se encontram bem estruturadas no sentido de cumprirem os objetivos delineados para o ciclo de estudos. Há no entanto alguns aspetos que poderão ser melhorados e que se encontram identificadas na secção 4.6.1 deste relatório recomendando-se vivamente a sua análise e consideração nomeadamente a carga horária que se afigura excessiva para um regime de funcionamento pós-laboral.

Ao longo deste relatório foram encontrados aspetos que podem ser melhorados, pelo que recomendamos esforços no sentido de implementação das sugestões de melhoria apresentadas.

13.1. Apreciação global da proposta do novo ciclo de estudos (EN)

The study programme in Applied Cybersecurity, aims to complete the training acquired in a first study programme in Computer Engineering and related areas, with at least 5 years of professional experience in the area of the study programme, providing students with skills that allow them to organize, implement, coordinate and control a computer system with security features in an organization.

It is in line with the institution's mission, meets the legal requirements in terms of curriculum structure, study plan, ECTS and workload involved, and fits into the institution's educational, scientific and cultural project. The Institution seems to have the necessary resources in terms of Facilities, Laboratories, Equipment, Library, and technical personnel necessary to ensure its proper functioning. The cycle of studies is associated with a teaching staff that meets the legal requirements: its own teaching staff, academically qualified and specialized with adequate allocation of teaching service.

There is a good percentage (66.7%) of professors involved in research units accredited by the FCT with a rating of Very Good or Excellent, however the number of publications in international journals in the main area of the study programme is still low, requiring further be reinforced.

As a study programme aimed at workers with five or more years of professional experience, given its nature, the prospects for demand by students appear to be good.

From the analysis of its curricular structure and syllabus contents of the curricular units, it was verified that these are well structured in order to fulfill the objectives outlined for the study programme. There are, however, some aspects that could be improved and which are identified in section 4.6.1 of this report, strongly recommending their analysis and consideration, namely the workload, which appears to be excessive for an after-work regime.

Throughout this report, aspects that can be improved were found, so we recommend efforts to implement the suggestions for improvement presented.

13.2. Recomendação final.

A acreditação do ciclo de estudos

13.3. Período de acreditação condicional (se aplicável).

[sem resposta]

13.4. Condições (se aplicável) (PT)

[sem resposta]

13.4. Condições (se aplicável) (EN)

[sem resposta]