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):

Henrique Manuel Dinis Santos (Presidente) - 0000-0001-5389-3285/B618-62ED-57FD

Dr. John Impagliazzo - 0000-0002-0143-1553

Luís Antunes - D815-6DD4-A938

António Mendes - 0000-0001-6659-660X/861D-3518-E20A

1. Caracterização geral do ciclo de estudos

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 e Resiliência

1.3. Designação do ciclo de estudos. (EN)

Cybersecurity and Resiliency

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)

480 - Informática

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

480 - Computer Science

1.6.1. Classificação CNAEF - primeira área fundamental

*[0480] 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.

120.0

1.8. Duração do ciclo de estudos.

2 anos

1.8.1. Outra

[sem resposta]

1.9. Número máximo de admissões proposto

35.0

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

Requisitos gerais definidos por lei:
- Titulares do grau de licenciado ou equivalente legal;
- Titulares de um grau académico superior estrangeiro conferido na sequência de um primeiro ciclo de estudo organizado segundo o processo de Bolonha;
- Titulares de um grau académico superior estrangeiro que seja reconhecido como satisfazendo os objetivos do grau de licenciado;
- Detentores de um curriculum escolar, científico ou profissional reconhecido como atestando capacidade para realização do mestrado.

Para serem elegíveis ao Mestrado, recomenda-se que os candidatos possuam formação na área das ciências informáticas. Na avaliação e seriação dos candidatos serão tidos em conta a formação académica e o desempenho curricular, bem como a experiência profissional.

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

General requirements defined by law:
- Holders of an under-graduate degree or legal equivalent;
- Foreign under-graduate degree according to Bologna;
- Foreign college degree that meets the objectives of the under-graduate degree;
- Holders of academic, scientific or professional curriculum, attesting the ability to carry out the master"s degree.

To be eligible for the Master"s degree, it is recommended that candidates have a background in the field of computer science. In the evaluation and ranking of candidates, consideration will be given to their education, academic performance, as well as professional experience.

1.10.1. Apreciação da adequação e conformidade legal das condições específicas

[ ] Existem, é adequado e cumpre os requisitos legais. [X] Existem, mas não é adequado ou não cumpre os requisitos legais. [ ] Não existem.

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

São indicadas as condições gerais de acesso de acordo o artigo nº. 17 do DL 74/2006, na redação introduzida no DL 65/2018. No entanto, as condições específicas de ingresso não parecem adequadas, nomeadamente no que respeita à não exigência de uma formação de base em Tecnologias de Informação e Comunicações.

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

The general conditions of access are indicated following article no. 17 of DL 74/2006, in the wording introduced in DL 65/2018. However, specific entry conditions were not mentioned.

1.11. Modalidade do ensino

[X] Presencial (Decreto-Lei n.º 65/2018, de 16 de agosto) [ ] A Distância (EaD) (Decreto-Lei n.º 133/2019, de 3 de setembro)

1.11.1. Regime de funcionamento, se presencial

[ ] Diurno [X] Pós-laboral [ ] Outro

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)

Iscte-Sintra
Avenida Heliodoro Salgado nº 3, Sintra
2710-569 Sintra

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

Iscte – University Institute of Lisbon (Sintra)
Avenida Heliodoro Salgado nº 3, Sintra
2710-569 Sintra

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

RegulamentoCreditacoes_Iscte_emRevisao.pdf | PDF | 157.4 Kb

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

[X] Existe, é adequado e cumpre os requisitos legais. [ ] Existe, mas não é adequado ou não cumpre os requisitos legais. [ ] Não existe.

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

Foi submetido o regulamento, na forma de documento em revisão, já aprovado pelo Concelho Científico e acomodando as alterações solicitadas pelas Portaria n.º 181-D/2015, de 19 de junho, Portaria n.º 305/2016, de 6 de agosto, Portaria n.º 249 -A/2019, de 5 de agosto e Portaria n.º 150/2020, de 22 de junho.

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

The regulation was submitted as a document under review, already approved by the Scientific Council, and accommodating the changes requested by Order no. 181-D/2015, of June 19th, Order no. 305/2016, of August 6th, Order no. 249 -A/2019, of August 5th, and Order no. 150/2020, of June 22nd.

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

[X] Existem, são adequadas e cumprem os requisitos legais. [ ] Existem, mas não são adequadas ou não cumprem os requisitos legais. [ ] Não existem.

2.1.1. Evidências que fundamentam a apreciação expressa (PT)

No processo de criação deste novo ciclo de estudos foram ouvidos a Comissão Científica do ISCTE-Sintra, os Conselhos Pedagógico e Científico do ISCTE, sendo todos os pareceres favoráveis. Posteriormente, a autorização de funcionamento foi dada pela Reitora dos ISCTE. O processo cumpre com o estipulado no artigo 61º, nº 2, do DL 62/2007.

2.1.1. Evidências que fundamentam a apreciação expressa (EN)

In creating this new study cycle, the Scientific Committee of ISCTE-Sintra, the Scientific Council and the Pedagogical Council of ISCTE were heard. All organs support the proposal. Subsequently, the authorisation to operate was provided by the Dean of ISCTE. The process complies with the provisions of article 61, no. 2, of DL 62/2007.

3. Âmbito e objetivos do programa de estudos. Adequação ao projeto educativo, científico e cultural da instituição

3.1. Objetivos gerais definidos para o ciclo de estudos.

[X] Sim [ ] Não [ ] Em parte

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

[ ] Sim [ ] Não [X] Em parte

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

[X] Sim [ ] Não [ ] Em parte

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

[X] Sim [ ] Não [ ] Em parte

3.5. Designação do ciclo de estudos.

[ ] Sim [ ] Não [X] Em parte

3.6.1. Apreciação global (PT)

Relativamente ao ponto 3.2, os resultados de aprendizagem listados precisam de ser mais explicitos, pois devem ser mensuráveis. A submissão utiliza palavras como conhecer, explorar e termos semelhantes que não são mensuráveis. Isto pode tornar difícil avaliar objectivamente estes resultados e determinar se o programa e os seus alunos atingiram os seus objectivos. Por conseguinte, os resultados de aprendizagem listados devem ser revistos para garantir que são claros, precisos e mensuráveis, aumentando a eficácia do programa. Adicionalmente, uma vez que existem já referenciais internacionais bem conhecidos neste âmbito, era expectável que os resultados de aprendizagem estivessem claramente alinhados com esses referenciais.
No que respeita ao ponto 3.5, em toda a proposta, o termo resiliência é por vezes utilizado em relação às ameaças à cibersegurança. Os conteúdos e os objetivos dos cursos demonstram isso mesmo. No entanto, o mesmo termo é referido de forma mais genérica na caracterização geral, nas designações das unidades curriculares, bem como nos conteúdos (por exemplo, "Criptografia para Cibersegurança e Resiliência" sugere uma abordagem à cibersegurança e resiliência, os resultados de aprendizagem também indicam uma diferença, mas o conteúdo descreve principalmente técnicas criptográficas, como esperado, exceto um tópico referente à aplicação da criptografia para a resiliência cibernética. Ao nível organizacional, a resiliência incluirá ameaças à cibersegurança, mas também ações de mudança empresarial motivadas por outros fatores, incluindo tecnológicos, estratégicos e até sociais. A caracterização geral do programa e a utilização do termo resiliência nas unidades curriculares não é clara e nem sempre coerente.

3.6.1. Apreciação global (EN)

Regarding 3.2, the program learning outcomes need to be stronger, as they should be measurable. The application uses words such as know, explore, and similar terms that are not measurable. This could make it difficult for the program to objectively assess these outcomes and determine whether the program and its students met their objectives. Therefore, the program should revise these learning outcomes to ensure they are clear, precise, and measurable, enhancing the program's effectiveness. Additionally, since there are already well-known international references in this context, the learning outcomes were expected to be clearly aligned with these references.
Concerning 3.5, throughout the proposal, the term resilience is sometimes used in connection with Cybersecurity threats. The contents and objectives of the courses demonstrate this. However, the same term is referred to more generically in the general characterisation, in course designations, as well in contents (e.g., "Cryptography for Cybersecurity and Resilience" suggests an approach to cybersecurity and resilience, the learning outcomes also indicate a difference, but the content describes mainly cryptographic techniques, as expected, except one topic referring application of cryptography for cyber resilience. At the organisational level, resilience will include cybersecurity threats but also business change actions motivated by other factors, including technological, strategic, and even societal. The general characterisation of the program and the use of the term resilience across curricular units is not clear and not always coherent.

3.6.2. Pontos fortes (PT)

Os objetivos gerais apontam para o desenvolvimento de competências de reação a situações novas, que constitui um bom alinhamento para o ciclo de estudos de 2º ciclo, especialmente na área da segurança informática.
A instituição indica o envolvimento em algumas iniciativas externas ligadas à cibersegurança, o que é um bom indicador da maturidade na área.

3.6.2. Pontos fortes (EN)

The general objectives point to the development of competencies for reacting to new situations, which is a good match for the second study cycle, especially in the area of IT security.
The institution indicates involvement in some external initiatives linked to cybersecurity, which indicates maturity in the area.

3.6.3. Pontos fracos (PT)

Alguns objetivos de aprendizagem são ambíguos ou carecem de profundidade (por exemplo, "Conhecer as principais recomendações, normas...", "Conhecer e explorar o cruzamento de diferentes áreas..."). A definição de objetivos muito gerais pode levar à formação de profissionais com perfil menos especializado do que o pretendido. O Quadro de Qualificações no Espaço Europeu do Ensino Superior (FQ-EHEA) afirma que os resultados de aprendizagem para um projeto de segundo ciclo devem abordar um nível mais profundo de conhecimento em vez de uma compreensão básica, que deve ser alcançada em um programa educacional de primeiro ciclo. A proposta aqui em apreciação não alinha corretamente com esse pressuposto.
Além disso, uma vez que já existem algumas referências internacionais essenciais para definir competências em Cibersegurança (e.g., NIST e ENISA), um alinhamento com essas iniciativas seria mais eficaz.

3.6.3. Pontos fracos (EN)

Some learning objectives are ambiguous or lack depth (e.g., "Know the main recommendations, standards...", "Explore the intersection of cybersecurity with different areas..."). The definition of very general objectives can lead to the training of professionals with a less specialized profile than intended. The Framework of Qualifications in the European Higher Education Area (FQ-EHEA) states that learning outcomes for a second-cycle project should address a deeper level of knowledge rather than a basic understanding, which should be achieved in a first-cycle educational program. The proposal under consideration here does not correctly align with this assumption.
Furthermore, since there are already some essential international references for defining competencies in Cybersecurity (e.g., NIST and ENISA), alignment with these initiatives would be more effective.

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 [ ] Não [X] Em parte

4.2.2 Conteúdos programáticos das unidades curriculares.

[ ] Sim [ ] Não [X] Em parte

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

4.4. Percursos do ciclo de estudos.

4.4.1. Estrutura curricular.

[ ] Sim [ ] Não [X] Em parte

4.4.2 Plano de estudos.

[X] Sim [ ] Não [ ] Em parte

4.5.1. Justificação o desenho curricular.

[X] Sim [ ] Não [ ] Em parte

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 [ ] Não [X] Em parte

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 [ ] Não [X] Em parte

4.5.2.1.4. Identificação das formas de garantia da justeza, fiabilidade e acessibilidade das metodologias e

[X] Sim [ ] Não [ ] Em parte

4.5.2.1.5. Avaliação da aprendizagem dos estudantes.

[X] Sim [ ] Não [ ] Em parte

4.5.2.1.6. Acompanhamento do percurso e do sucesso académico dos estudantes.

[X] Sim [ ] Não [ ] Em parte

4.5.2.1.7. Participação dos estudantes em atividades científicas (quando aplicável).

[X] Sim [ ] Não [ ] Em parte

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.

[X] Sim [ ] Não [ ] Em parte

4.5.2.2.2. Forma de verificação de que a carga média de trabalho que será necessária aos estudantes

[X] Sim [ ] Não [ ] Em parte

4.5.2.2.3. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de

[X] Sim [ ] Não [ ] Em parte

4.6.1. Apreciação global (PT)

No que diz respeito ao ponto 4.2.1., os objectivos do curso são uma componente crucial do programa. No entanto, apenas algumas UCs apresentam os objetivos claros, concretos e mensuráveis. Termos como aprender, familiarizar, conhecer, compreender e adquirir não são mensuráveis e não devem ser utilizados como resultados objetivos de aprendizagem. A IES deve reestruturar os resultados de aprendizagem do curso de modo a que sejam claros, objetivos e quantificáveis, o que é essencial para a eficácia do programa. A candidatura deverá também indicar o processo utilizado para avaliar os conhecimentos, aptidões e competências dos alunos, embora o Acordo de Bolonha possa abranger esta dimensão.

Relativamente ao ponto 4.2.2, na maioria das UCs, a secção 4.2.12 não responde à questão colocada (coerência entre os programas e os resultados de aprendizagem pretendidos), centrando-se nas metodologias pedagógicas que deveriam ser incluídas na secção 4.2.13. Por exemplo, na UC Arquiteturas de Segurança e Modelos de Confiança Zero, o campo 7 deve demonstrar a coerência dos programas e objetivos de aprendizagem. No entanto, começa com "As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC". Os conteúdos abordam apenas as metodologias pedagógicas, sobrepondo-se parcialmente ao campo 10, que aborda corretamente os métodos pedagógicos. O mesmo acontece em várias outras unidades curriculares.

Além disso, algumas unidades curriculares revelam incoerências. Por exemplo, para "Segurança e Resiliência de Infraestruturas e Redes de Comunicação", todos os OA refletem "Analisar", mas os conteúdos (e os pressupostos, num plano de estudos de Cibersegurança, 2º ciclo, típico) deste curso sugerem incluir saber como implementar e gerir os controlos de segurança. O mesmo se aplica a outras UCs de carácter mais tecnológico, como a "Criptografia para Cibersegurança e Resiliência".

Finalmente, várias UCs incluem laboratórios, alguns dos quais serão realizados em grupo. Não é claro o que isto envolve, se é necessário algum equipamento tecnológico específico e como os alunos terão acesso a ele, uma vez que a maioria destas unidades curriculares é predominantemente à distância.

No que respeita ao ponto 4.4.1, é necessário que existam alguns esclarecimentos sobre as duas unidades curriculares de 42 ECTS (Dissertação e Projecto). Na descrição dessas unidades curriculares (secção 4.2), consta que terão 28,57% das horas de contacto à distância. Contudo, na secção 4.3, aparecem as mesmas unidades curriculares com 85,71% de horas de contacto remoto. Esta discrepância deve ser esclarecida, pois alteraria a classificação do curso de presencial para à distância. Assumindo que a informação da secção 4.2 está correta, seria útil compreender a opção de realizar o seminário de 32 horas em modelo presencial, indicado na UC de Dissertação e de Trabalho de Projeto, pois não se justifica e não se alinha com o objetivo indicado de ter alunos a residir noutras regiões ou países.

Adicionalmente, existe alguma sobreposição entre algumas das unidades curriculares, nomeadamente entre Fundamentos de Gestão de Cibersegurança e Resiliência e Gestão do Ciber-risco para Resiliência (no que diz respeito à Gestão do Risco); e Verificação de Segurança e Resiliência de Sistemas, Segurança e Resiliência de Software e Aplicações e Incidentes de Cibersegurança e Resiliência (relativos a Segurança e Testes de Software e Resposta a Incidentes).

Relativamente à secção 4.5.2.1.1, a IES inclui uma lista de possíveis metodologias pedagógicas que os professores podem adotar nas diferentes unidades curriculares. No entanto, não inclui quaisquer recomendações ou reflexão sobre quais as adequadas aos objetivos de aprendizagem de cada unidade curricular do programa em avaliação.

No que respeita ao item 4.5.2.1.3, a metodologia de ensino-aprendizagem é exatamente a mesma em todos os cursos da área de Informática. Contudo, dada a natureza de algumas UCs, seria de esperar uma metodologia mais adaptada. Por exemplo, "Segurança e Resiliência de Infraestruturas e Redes de Comunicação" deverá exigir métodos mais eficazes para uma componente experimental.

4.6.1. Apreciação global (EN)

Concerning 4.2.1., the course objectives are a crucial component of the program. However, only some course units had clear, concrete, and measurable objectives. Terms such as learn, familiarize, know, understand, and acquire are not measurable and should not be used as objective learning outcomes. The HEI must restructure the course learning outcomes to be clear, objective, and quantifiable, which is essential for the program's effectiveness. The application should also indicate the process used to assess student knowledge, skills, and competencies, although the Bologna Accord may cover this dimension.

Concerning 4.2.2, in most courses, section 4.2.12 doesn't answer the stated question (coherence between syllabi and intended learning outcomes), focusing on pedagogical methodologies that should be included in section 4.2.13. For example, in the Security Architectures and Zero-Trust Models course, field 7 should demonstrate the coherence of syllabi and learning objectives. However, it starts with "The teaching methodologies have been selected to match the learning objectives of the course." The contents only address pedagogical methodologies, partially overlapping field 10, which correctly addresses pedagogical methods. The same happens in several other courses.

Furthermore, some curricular units reveal inconsistencies. For example, for "Security and Resilience of Infrastructure and Communication Networks", all LOs reflect "Analyze", but the contents (and the assumption, in a typical Cybersecurity study plan, 2nd cycle) of this course suggest including knowing how to implement and manage security controls. The same is true for other UCs of a more technological nature, such as "Cryptography for Cybersecurity and Resilience".

Finally, several courses include laboratories, some of which will be realized as group work. It is unclear what this involves, if some specific technological equipment is necessary, and how the students will access it since most of those courses are predominantly at a distance.

Involving 4.4.1, there needs to be some clarification about the two 42 ECTS curricular units (Dissertation and Project). In these curricular unit forms (section 4.2), it is stated that they will have 28.57% of the contact hours at a distance. However, in section 4.3, the same curricular units appear with 85.71% remote contact hours. This should be clarified, as it would change the course classification from presential to distance. Assuming that the information in section 4.2 is correct, it would be helpful to understand the option of holding the 32-hour seminar in a face-to-face model, indicated in the Dissertation and Research Project courses, as it is not justified and does not align with the stated objective of having students residing in other regions or countries.

Additionally, there is some overlap between some of the courses, namely between Fundamentals of Cybersecurity and Resilience Management and Cyber-risk Management for Resilience (concerning Risk Management); and System Security and Resilience Verification, Software and Applications Security and Resilience, and Cybersecurity and Resilience Incidents (concerning Software Security and Testing, and Incident Response).

Concerning the section 4.5.2.1.1, the HEI includes a list of possible pedagogical methodologies teachers may adopt in the different curricular units. However, it does not include any recommendations or reflections about what is adequate to the learning objectives of the various curricular units of the program under evaluation.

Concerning 4.5.2.1.3, the teaching-learning methodology is exactly the same in all courses in the CS area. However, given the nature of some courses, a more adapted methodology would be expected. For example, "Security and Resilience of Infrastructure and Communication Networks" should require more effective methods for an experimental component.

4.6.2. Pontos fortes (PT)

Um dos pontos fortes da oferta educativa é procurar responder a uma necessidade evidente no mercado de trabalho, ilustrada por diversos relatórios da especialidade.

É ainda de salientar que a proposta é submetida por uma IES com prestígio e experiência, reunindo condições para ser um programa com sucesso.

Adicionalmente, o programa cobre de forma abrangente as diferentes áreas de segurança. A aplicação cobre eficazmente as áreas humana, social, organizacional, de sistema, ligação, componente, software e segurança de dados, que são essenciais para um programa de cibersegurança robusto.

4.6.2. Pontos fortes (EN)

One of the strengths of the educational offer is that it seeks to meet an evident need in the job market, as illustrated by several speciality reports.

It is also worth noting that the proposal is submitted by an HEI with prestige and experience, meeting the conditions to be a successful program.

Additionally, the program covers the different security areas comprehensively. The application effectively covers human, societal, organizational, system, connection, component, software, and data security areas, which are essential for a robust cybersecurity program.

4.6.3. Pontos fracos (PT)

O uso do termo resiliência, ao longo do plano de estudos, quer no nome das unidades curriculares, quer na respetiva descrição, devia ser mais coerente. Por vezes parece que se refere à resiliência da cibersegurança (o que seria a interpretação correta), mas por vezes aparece como conceito isolado e, portante, muito mais abrangente.

Apesar do plano de estudos evidenciar alguma robustez, era de esperar uma maior identificação com os referenciais existentes, em particular da ENISA e do NIST. Isto sobretudo no que respeita às competências e aos perfis de formação.

Em linha com a observação anterior, estranhamos a não inclusão de alguns controlos de segurança fundamentais, principalmente, do Controlo de Acessos, e a abordagem ligeira à Deteção de Intrusões, misturada com vários outros tópicos, limitando a profundidade esperada, numa única UC que aborda deteção de ameaças, deteção de incidentes, recuperação, resiliência e até aspetos éticos, legais e SOCs (Security Operations Center). O mesmo se pode afirmar no que respeita à segurança em redes. Este é um tópico bastante denso e que aparece diluido numa única UC com vários outros tópicos, também complexos, como segurança em sistemas operativos, segurança em IoT e segurança de sistemas distribuídos. Todos estes assuntos são essenciais em cibersegurança e, neste programa, só podem ser tratados de forma superficial.

4.6.3. Pontos fracos (EN)

The use of the term resilience throughout the study plan, whether in the name of the curricular units or the respective description, should be more coherent. Sometimes, it seems to refer to the resilience of cybersecurity (which would be the correct interpretation), but sometimes, it appears as an isolated concept and, therefore, much more comprehensive.

While the study plan demonstrates some robustness, it could benefit from a stronger alignment with existing references, particularly ENISA and NIST. This is especially important in the context of skills and training profiles.

In line with the previous observation, we found it strange that some fundamental security controls were not included, mainly Access Control, and the lightweight approach to Intrusion Detection, mixed with several other topics, limiting the expected depth, in a single UC that addresses threat detection, incident detection, recovery, resilience and even ethical, legal and SOCs (Security Operations Center) aspects. The same can be said regarding network security. This is a very dense topic that appears diluted in a single UC with several other complex subjects, such as security in operating systems, security in IoT, and security in distributed systems. All of these subjects are essential in cybersecurity and, in this program, can only be covered superficially.

5. Corpo docente.

5.1.1. Coordenação do ciclo de estudos.

[X] Sim [ ] Não [ ] Em parte

5.1.2. Adequação da carga horária.

[ ] Sim [ ] Não [X] Em parte

5.2.1. Cumprimento de requisitos legais.

[ ] Sim [ ] Não [X] Em parte

5.2.2. Estabilidade do corpo docente.

[X] Sim [ ] Não [ ] Em parte

5.2.3. Dinâmica de formação do corpo docente.

[ ] Sim [X] Não [ ] Em parte

5.3. Avaliação do pessoal docente.

[X] Sim [ ] Não [ ] Em parte

5.4.1. Apreciação global (PT)

Esta comissão entende que a instituição não cumpre com os requisitos do nº 2, do Artigo 16º, do DL 74/2006, na sua redação do DL 65/2018, não dispondo de um corpo docente suficientemente especializado na área de Cibersegurança. A CAE entende que apenas 2 ETI cumprem esse requisito.

A maioria dos docentes é responsável por muitas UCs (mais de 5). Dada a natureza prática do programa e o número de alunos esperado, este pode ser um fator limitativo. Esta evidência é particularmente relevante para o coordenador, que tem demasiadas horas atribuídas em outros programas.

De uma forma geral, o corpo docente está bem qualificado em computação e áreas relacionadas, tais como ciências da computação. No entanto o seu grau de especialização, conhecimento e competências em cibersegurança moderna precisa de ser melhorado. A instituição devia proativamente procurar especialistas de elevada qualidade em cibersegurança com conhecimento de base em mineração de dados, inteligência artificial, LLMs e outras atividades emergentes relacionadas com cibersegurança. Só assim a instituição poderá oferecer um programa de mestrado em cibersegurança alinhado com as exigências da era moderna digital.

No caso particular da UC Criptografia para Cibersegurança e Resiliência, dada o grau de complexidade e exigência num programa deste tipo, será recomendado um docente com bastante mais experiência e conhecimento neste tópico do que o que é demonstrado na ficha da docente indicada.

Não obstante a classificação do programa como Presencial, a maioria das UCs têm uma componente predominantemente à distância. Atendendo ainda ao número máximo de alunos, seria de esperar que a preparação de todo o corpo docente para esse regime fosse mais explicitamente assumida. Apesar da existência na IES de uma equipa de apoio especializada para este efeito deixar antever uma forma de mitigação adequada, não é claro como esse apoio, para cada UC, se refletiu no desenho curricular ou nas metodologias de ensino/aprendizagem.

5.4.1. Apreciação global (EN)

This committee understands that the institution does not comply with the requirements of number 2, Article 16, of DL 74/2006, in its wording of DL 65/2018, not having a teaching staff sufficiently specialized in Cybersecurity. The EAT understands that only 2 FTEs meet this requirement.

Most teaching staff members are responsible for many courses (over 5). Given the practical nature of the programme and the expected number of students, this can be a limiting factor. This evidence is particularly relevant for the coordinator, who has too many hours allocated to other programmes.

While the current faculty members are qualified in computing and related fields such as computer science, their expertise in modern cybersecurity knowledge and skills needs improvement. More effort was required to seek out and hire new cybersecurity faculty members. The program seems content with the people it has. The program should proactively seek high-quality cybersecurity specialists with backgrounds in data mining, artificial intelligence, large language models, and other cybersecurity-related activities. The institution must offer a cybersecurity master's program designed and delivered for the modern digital era.

In the particular case of the UC Cryptography for Cybersecurity and Resilience, given the degree of complexity and demand in a program of this type, it is recommended a teacher with much more experience and knowledge in this topic than what is demonstrated in the indicated teacher's file.

Despite the program's classification as In-person, most Curricular Units have a predominantly distance learning component. Given the maximum number of students, it would be expected that the preparation of the entire teaching staff for this regime would be more explicitly assumed. Although a specialized support team at the IES for this purpose suggests an adequate form of mitigation, it needs to be clarified how this support for each UC was reflected in the curricular design or teaching/learning methodologies.

5.4.2. Pontos fortes (PT)

O coordenador do ciclo de estudos demonstra ter elevada experiência pedagógica e científica, bem como um nível de conhecimento adequado a um programa de mestrado em Cibersegurança, permitindo antever uma liderança efetiva e de sucesso.

A equipa docente tem docentes de diversas áreas, o que contribui positivamente para uma visão alargada, em linha com a multidisciplinaridade da cibersegurança (Psicologia, Matemática, e Ciências da Computação e Tecnologias).

5.4.2. Pontos fortes (EN)

The coordinator of the study cycle demonstrates high pedagogical and scientific experience, as well as a level of knowledge appropriate to a master's program in cybersecurity, allowing for effective and successful leadership to be anticipated.

The teaching staff has professors from different areas, contributing positively to a broad vision in line with the multidisciplinarity of cybersecurity (Psychology, Mathematics, and Computer Science and Technologies).

5.4.3. Pontos fracos (PT)

A distribuição de serviço docente parece claramente desbalanceada e adversa à qualidade do ensino e à prossecução dos objetivos.

A equipe docente, de uma forma geral, devia demonstrar mais trabalho científico focado em cibersegurança. Isto coloca em causa a prossecução dos objetivos subjacentes à estratégia para integração com atividades de investigação, descrita no ponto 4.5.2.1.7, na área da cibersegurança.

A cibersegurança é atualmente reconhecida pela sua multidisciplinaridade. Apesar do esforço em incluir no programa docentes de outras áreas relevantes, dada a característica genérica do programa, seria de esperar que outras áreas fossem também incluídas, tais como Direito e Gestão. Isso exige ter docentes com formação nessas áreas, aplicadas à cibersegurança, embora se compreenda que neste caso, face à dimensão reduzida do corpo docente, a tarefa fosse difícil.

5.4.3. Pontos fracos (EN)

The distribution of teaching services seems clearly unbalanced and adverse to the quality of teaching and the pursuit of objectives.
The teaching team should demonstrate more scientific work focused on cybersecurity. This calls into question the pursuit of objectives underlying the strategy for integration with research activities, described in item 4.5.2.1.7, in the cybersecurity area.
Cybersecurity is currently recognized for its multidisciplinary nature. Despite the effort to include teachers from other relevant areas in the program, given the generic nature of the program, it would be expected that other areas would also be included, such as Law and Management. This requires having teachers with training in those areas applied to cybersecurity, although it is understood that, in this case, given the small size of the teaching staff, the task would be difficult.

6. Pessoal técnico, administrativo e de gestão.

6.1. Adequação em número.

[X] Sim [ ] Não [ ] Em parte

6.2. Qualificação profissional e técnica.

[X] Sim [ ] Não [ ] Em parte

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

[X] Sim [ ] Não [ ] Em parte

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

6.4.1. Apreciação global (PT)

O pessoal técnico, administrativo e de gestão é apresentado para a instituição e não em função do ciclo de estudos em particular, à exceção da referência de um indicador geral do valor em ETI (1,62). Sem um enquadramento adequado não é fácil depreender o nível de adequação. De qualquer forma, a maioria desses colaboradores tem formação adequada para o funcionamento expetável de uma instituição de ensino superior, não sendo perceptível qualquer limitação.
Realça-se ainda a existência de uma equipa dedicada ao apoio a docentes no desenho e implementação de componentes para ensino à distância, o que é relevante para o programa em avaliação.

6.4.1. Apreciação global (EN)

The technical, administrative and management staff are presented for the institution and not according to the particular study cycle, except for the reference to a general indicator of the value in FTE (1.62). With an adequate framework, it would be easier to understand the level of adequacy. In any case, the majority of these employees have sufficient training for the expected functioning of a higher education institution, with no noticeable limitations.
It is also worth highlighting the existence of a team dedicated to supporting teachers in designing and implementing components for distance learning that are relevant to the program under evaluation.

6.4.2. Pontos fortes (PT)

O pessoal técnico, administrativo e de gestão tem o nível de preparação adequado e com experiência relevante para o sucesso do programa.

6.4.2. Pontos fortes (EN)

The technical, administrative and management staff have the appropriate level of preparation and relevant experience for the program's success.

6.4.3. Pontos fracos (PT)

Não é clara a forma como o sistema de avaliação do pessoal técnico, administrativo e de gestão valoriza a progressão nas carreiras (para além das formações) ou se compara com outros sistemas.

6.4.3. Pontos fracos (EN)

It is not clear how the evaluation system for technical, administrative and management personnel values career progression (beyond training) or how it compares with other systems,

7. Instalações e equipamentos.

7.1. Instalações.

[X] Sim [ ] Não [ ] Em parte [ ] Não Aplicável

7.2. Sistemas tecnológicos e recursos digitais.

[X] Sim [ ] Não [ ] Em parte

7.3. Equipamentos.

[ ] Sim [ ] Não [X] Em parte

7.4. Apreciação global das instalações e equipamentos.

7.4.1. Apreciação global (PT)

Os equipamentos e recursos disponíveis são apresentado para toda a instituição, e não necessariamente em função do ciclo de estudos aqui em avaliação. A descrição não inclui detalhes que ligam os recursos e equipamentos à proposta. Ainda assim, são mencionados recursos importantes sobretudo no apoio ao ensino à distância, já que este programa revela a sua utilização intensiva. Atendendo às características da área em causa (cibersegurança), era desejável que a instituição promovesse a criação de um laboratório dedicado, assente em recursos de virtualização, onde os alunos do mestrado em cibersegurança poderiam explorar o uso de equipamento e tecnologias modernas relevantes para a área e os exercícios práticos sugeridos pelos curriculos de várias UCs. Sem esse tipo de infraestrutura e ainda mais dada a componente intensa de ensino à distância, os alunos deste mestrado irão sofrer as consequências de uma preparação limitada e até mesmo heterogénea, assumindo que terão que realizar os trabalhos práticos com os recursos pessoais que tenham ao dispor.

7.4.1. Apreciação global (EN)

The equipment and resources available are presented for the entire institution, not necessarily depending on the study cycle under evaluation. The description does not include details linking resources and equipment to the proposal. Even so, essential resources are mentioned, especially in support of distance learning, as this program reveals its intensive use.

Given the characteristics of the area in question (cybersecurity), the institution should have promoted the creation of a dedicated laboratory based on virtualization resources, where master's students in cybersecurity could explore the use of modern equipment and technologies relevant to the area and the practical exercises suggested by the curricula of various courses. Without this type of infrastructure and even more so given the intense distance learning component, students in this master's degree will suffer the consequences of limited and even heterogeneous practical preparation, assuming that they will have to carry out practical work with the personal resources they have.

7.4.2. Pontos fortes (PT)

A descrição geral indica infraestruturas e recursos adequados ao ensino superior e em particular a um programa de segundo nível, com uma componente substancial de ensino à distância.

7.4.2. Pontos fortes (EN)

The general description indicates adequate infrastructure and resources for higher education, particularly for a second-level program with a substantial distance learning component.

7.4.3. Pontos fracos (PT)

Aparte os laboratórios de informática e multimédia, bem como tecnologias de mediação gerais, nenhum elemento descrito na proposta está especialmente orientado para o curso proposto. Dadas as suas especificidades, este aspeto é relevante (e.g., a proposta devia elaborar em como é que os laboratórios ou tecnologias de virtualização dão suporte ao curso, por exemplo, em termos de simulação de ataques em ambiente controlado).

7.4.3. Pontos fracos (EN)

Apart from computer and multimedia laboratories and general mediation technologies, no element described in the proposal is primarily aimed at the proposed course. Given its specificities, this aspect is relevant (e.g., the proposal should elaborate on how laboratories or virtualization technologies support the course, for example, in terms of simulating attacks in a controlled environment).

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.

[X] Sim [ ] Não [ ] Em parte

8.2. Integração em projetos e parcerias nacionais e internacionais.

[ ] Sim [ ] Não [X] Em parte

8.3. Produção científica.

[ ] Sim [ ] Não [X] Em parte

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

[ ] Sim [ ] Não [X] Em parte

8.5. Apreciação global das investigação e desenvolvimento e/ou de formação avançada e desenvolvimento

8.5.1. Apreciação global (PT)

Relativamente a 8.2, a maioria das unidades de investigação enunciadas na Tabela 8.1 não são focadas na área nuclear do ciclo de estudos proposto, e apesar da reconhecida multidisciplinaridade da cibersegurança, só dificilmente estas unidades constituirão o substrato ideal para a investigação associada ao programa em causa. Acresce que os docentes indicados como ligados a dois dos centros de investigação não demonstram essa ligação - através das próprias páginas institucionais ou as páginas dos centros.
Relativamente a 8.3, na área da cibersegurança, são evidentes alguns contributos relevantes de dois dos elementos do corpo docente. Para os restantes, essas contribuições são residuais ou mesmo inexistentes.
No que respeita ao ponto 8.4 e tendo em conta os projetos e participações referidos na proposta (secção 8.2), que é necessariamente vago, não resulta claro que exista uma dinâmica capaz de alavancar as atividades do programa. Salientam-se algumas colaborações que revelam a preocupação de um acompanhamento da área, mas era desejável ter aqui parcerias que permitissem, por exemplo, enquadrar adequadamente os trabalhos de dissertação.

8.5.1. Apreciação global (EN)

Regarding 8.2, most of the research units listed in Table 8.1 are not focused on the core area of the proposed study cycle. Despite the recognized multidisciplinary nature of cybersecurity, these units are unlikely to constitute the ideal substrate for research activities associated with the program in question. Furthermore, professors indicated as linked to two of the listed research centres do not demonstrate this connection - through their institutional home pages or the centres' sites.
Concerning 8.3 and considering cybersecurity, some relevant contributions from two of the faculty members are evident. For others, these contributions are residual or even non-existent.
With regard to point 8.4 and taking into account the projects and participations referred to in the proposal (section 8.2), which is necessarily vague, it is not clear that there is a dynamic capable of leveraging the program's activities. Some collaborations stand out that reveal the concern for monitoring the area, but it was desirable to have partnerships here that would allow, for example, adequate framing of dissertation work.

8.5.2. Pontos fortes (PT)

Os projetos e parcerias enunciados em 8.2 evidenciam colaborações nacionais e internacionais com potencial impacto e propensão para parcerias relevantes. É claro o esforço de afirmação na área da cibersegurança.

8.5.2. Pontos fortes (EN)

The projects and partnerships listed in 8.2 show national and international collaborations with potential impact and a propensity for relevant partnerships. The effort to assert itself in the area of cybersecurity is apparent.

8.5.3. Pontos fracos (PT)

A ligação do programa a atividade de investigação dinâmica e impactante devia ser mais marcante, sobretudo para um programa de segundo ciclo. Atendendo ao limitado foco das unidade de investigação mais fortemente ligada à instituição proponente, seria de esperar um esforço na procura de parcerias.
O programa não se configura como um projeto de treino avançado e desenvolvimento profissional de alto nível. Em vez disso, redireciona as instalações e recursos existentes para um produto que pode mesmo não ser alcançado. Essa falta de realização pode ter um reflexo negativo na reputação do programa e da instituição.

8.5.3. Pontos fracos (EN)

The program's connection to dynamic and impactful research activity should be more striking, especially for a second-cycle program. Given the limited focus on cybersecurity of the research units most closely linked to the proposing institution, one would expect an effort to search for partnerships.
The program is not configured as an advanced training and high-level professional development project. Instead, it redirects existing facilities and resources to a product that may not even be achievable. This lack of achievement can have a negative impact on the reputation of the program and the institution.

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 [ ] Não [X] Em parte

10. Comparação com ciclos de estudos de referência no Espaço Europeu de Ensino Superior (EEES).

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

[X] Sim [ ] Não [ ] Em parte

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

[ ] Sim [ ] Não [X] Em parte

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

10.3.1. Apreciação global (PT)

A Comissão de Avaliaçao entende que a comparação realizada pela instituição podia ser mais abrangente e ambiciosa. Excetua-se a referência aos quatro programas nacionais e às fontes usadas para encontrar essa informação, que indicam um esforço positivo. No entanto, a proposta realça a limitada oferta em "Cibersegurança e Resiliência", como se essa fosse uma área substancialmente diferente da de Cibersegurança. Este critério serve para deixar de fora muitos programas internacionais (de cibersegurança), mas não é usado da mesma forma a nível nacional.

Outro aspeto que merece atenção é a comparação dos resultados de aprendizagem. É evidente apenas um esforço para caracterizar a natureza do programa (mais ou menos tecnológico), mas sem demonstrar como essas opções foram assumidas. É ainda indicada a intenção de cobrir as competências incluídas em referenciais como o da NIST (CSF), mas, mais uma vez, sem evidências claras da aplicação dessa intenção.

Olhando para os resultados de aprendizagem listados nas UCs da proposta e os das UCs equivalentes em outros ciclos de estudo, as diferenças não são assim tão evidentes. Nesta perspetiva, esta proposta de mestrado em Cibersegurança revela algumas lacunas nomeadamente ao nível de competências transversais e competências práticas (saber fazer) em tópicos essenciais com a segurança em redes de computadores.

Relativamente ao uso do termo "resiliencia", a proposta identifica apenas um programa que o usa. Na verdade é possível encontrar mais alguns (e.e., MSc in Homeland Security and Cyber Resilience, da Seton Hall University, ou o MSc in Cyber Security, Risk and Resilience). Uma característica desses programas é uma maior ênfase em tópicos de gestão, incluindo gestão de crises e de conflitos, legislação e direito, inteligência artificial, por vezes em percursos optativos.

10.3.1. Apreciação global (EN)

The Evaluation Committee understands that the comparison carried out by the institution could be more comprehensive and ambitious. Except for referencing the four national programs and the sources used to find this information, which indicates a positive effort. However, the proposal highlights the limited offering in "Cybersecurity and Resilience", as if this were a substantially different area to Cybersecurity. This criterion leaves out many international (cybersecurity) programs but is not used in the same way at the national level.

Another area that requires attention is the comparison with learning results. The proposal characterizes the program's nature (more or less technological) without demonstrating how these options were chosen. The intention to cover the competencies included in references such as the NIST (CSF) is indicated, but it is crucial to provide clear evidence of the application of this intention.

When comparing the learning outcomes listed in the proposal's courses with those of the equivalent courses in other study cycles, the differences are not immediately apparent. However, this master's degree proposal in Cybersecurity does reveal some gaps, particularly in transversal skills and practical skills (know-how) in essential topics related to security in computer networks. This underlines the need for a more hands-on approach to the program.

Regarding using the term "resilience", the proposal identifies only one program that uses it. It is possible to find a few more (e.g., an MSc in Homeland Security and Cyber Resilience from Seton Hall University or an MSc in Cyber Security, Risk and Resilience). A feature of these programs is a greater emphasis on management topics, including crisis and conflict management, legislation and law, artificial intelligence, sometimes in optional pathways.

10.3.2. Pontos fortes (PT)

Em termos gerais, o programa de estudos proposto cobre áreas complementares consideradas relevantes em cibresegurança, na perpetiva do EEES.

10.3.2. Pontos fortes (EN)

In general terms, the proposed study program covers complementary areas considered relevant in cybersecurity from the perspective of the EHEA.

10.3.3. Pontos fracos (PT)

Olhando para ofertas educativas comparáveis no espaço Europeu, é evidente uma falta de profundidade em alguns tópicos abordados e ausência de UCs em algumas áreas tecnológicas atuais e mais relevantes (por exemplo, Internet das Coisas).

É ainda evidente uma ausência de preocupação objetiva em explorar relacionamentos mais fortes com empresas e profissionais de cibersegurança, possivelmente por meio de estágios ou palestras feitas por especialistas do setor (deveria estar mais claramente inserido nos planos curriculares).

Limitada ligação objetiva com os padrões e diretrizes estabelecidos por instituições e organizações relevantes, como ENISA, NIST e ACM, em termos de áreas de conhecimento, resultados de aprendizagem e competências.

O uso to termo "Resiliência" não parece ser usado com o alinhamento devido relativamente a outras propostas de programas similares.

10.3.3. Pontos fracos (EN)

Looking at comparable educational offers in the European space, a lack of depth in some topics covered and an absence of courses in some recent and most relevant technological areas (e.g. Internet of Things) is evident.

It is also evident that there is an absence of objective concern in exploring stronger relationships with companies and cybersecurity professionals, possibly through internships or lessons from area experts (should be more clearly included in curriculum plans).

The objective link with standards and guidelines established by relevant institutions and organizations, such as ENISA, NIST and ACM, regarding knowledge areas, learning outcomes and skills is also limited.

The term "Resilience" does not appear to be used in alignment with other similar program proposals.

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

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

[ ] Sim [X] Não [ ] Em parte [ ] Não Aplicável

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 [X] Não [ ] Em parte [ ] Não Aplicável

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

[ ] Sim [X] Não [ ] Em parte [ ] Não Aplicável

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

[ ] Sim [X] Não [ ] Em parte [ ] Não Aplicável

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

11.6.1. Apreciação global (PT)

A proposta deste CE não inclui a realização de estágios, ou de formação no local de trabalho.

11.6.1. Apreciação global (EN)

This SC proposal does not include internships or on-the-job training.

11.6.2. Pontos fortes (PT)

Nada a saliantar.

11.6.2. Pontos fortes (EN)

Nothing to highlight.

11.6.3. Pontos fracos (PT)

Nada a saliantar.

11.6.3. Pontos fracos (EN)

Nothing to highlight.

12. Observações finais.

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

A CAE compreende o contexto e reconhece o esforço desenvolvido pela IES para responder às questões centrais, procurando nomeadamente contratar docentes mais especializados em cibersegurança. Entendemos que essa é a estratégia adequada, pese embora a formação e o estímulo para a criação de núcleos de saber na área seja igualmente pertinente. No entanto, estas alterações não são consideradas para processos de avaliação em curso, uma vez que não fazem parte da documentação formal.

No que diz respeito aos problemas de carga de trabalho identificados pela CAE, convém esclarecer que as observações baseiam-se na carga de trabalho global e não apenas no programa em avaliação. Reconhecemos que as optativas, não estando instanciadas, poderão ser alocadas a outros docentes, mas também poderão não o ser.

Sobre o equipamento especializado, a explicação apresentada pela IES refere alguns componentes que habitualmente são encontrados em laboratórios para a educação em cibersegurança. No entanto, a arquitetura destes laboratórios apresenta desafios consideráveis, não só na sua implementação e manutenção, mas também no desenho de trabalhos que os podem usar para desenvolver as competências desejadas. É a ausência dessa preocupação em estabelecer tais laboratórios que a CAE identifica como limitação, na proposta submetida. No entanto, a estratégia descrita de colaborações com organizações relevantes nessa matéria é promissora e poderá ser explorada com exito numa proposta de programa subsequente.

Relativamente ao alinhamento com referenciais internacionais, a CAE reconhece o esforço da síntese e o mapeamento feito ao nível dos tópicos, para as UC propostas no programa. É, sem dúvida, um contributo relevante que, infelizmente, não é visível na candidatura. No etanto, tão ou mais importante que os tópicos, são as competências a desenvolver pelas diversas UCs. Neste caso, o mapeamento não é tão visível ou evidente.

Relativamente ao comentário sobre o uso do termo "resiliência" no título do mestrado, a CAE entendeu que na forma apresentada (Cibersegurança e Resiliência) o programa sugere a abordagem aos dois domínios e não apenas sobre os aspetos da resiliência no contexto da cibersegurança. Como sugestão, um título mais adequado poderia ser Cibersegurança Resiliente.

Atendendo ao conteúdo da pronuncia e com base nas observações anteriores, a CAE reconhece o esforço da clarificação de alguns detalhes, mas lamenta informar que não encontra fundamentos suficientes para alterar a posição anteriormente assumida de não acreditação do programa, tal como se apresenta.

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

The EAT understands the context and recognizes the effort made by the HEI to respond to the central questions, seeking, in particular, to hire more specialized professors in cybersecurity. We understand that this is the appropriate strategy, although training and encouragement for creating knowledge centres in the area are equally pertinent. However, these changes are not considered for ongoing assessment processes as they are outside the formal documentation.

About the workload issues identified by the EAT, it should be clarified that the observations are based on the overall workload and not just the program under evaluation. We recognize that electives, if not instantiated, can be allocated to other teachers, but they may not be.

Regarding specialized equipment, the explanation presented by the HEI mentions some components usually found in cybersecurity education laboratories. However, the architecture of these labs presents considerable challenges, not only in their implementation and maintenance but also in the design of assignments that can be used to develop desired skills. The EAT identifies the absence of this concern in establishing such laboratories as a limitation in the submitted proposal. However, the described strategy of collaborations with relevant organizations in this area is promising and could be successfully explored in a subsequent program proposal.

In relation to alignment with international frameworks, the EAT recognizes the effort of synthesis and mapping made at the topic level for the courses proposed in the program. It is, without a doubt, a relevant contribution that, unfortunately, is not visible in the application. However, as important or more important than the topics are the skills to be developed by the different UCs. In this case, the mapping should be more visible.

Regarding the comment on using the term "resilience" in the master's degree, CAE understood that in the form presented (Cybersecurity and Resilience), the program suggests an approach to both domains and not just the aspects of resilience in the cybersecurity context. As a suggestion, a more appropriate title could be "Resilient Cybersecurity".

Considering the content of the HEI response and based on previous observations, the EAT recognizes the effort to clarify some details but regrets to inform that it does not find sufficient grounds to change the previously assumed position of non-accreditation of the program as it stands.

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)

A cibersegurança é uma área relativamente recente e com um impacto crescente dada a acelerada adoção das TIC, em todos os setores de atividade. Em alguns desses setores há já pessoal especializado, mas em muitos é evidente uma lacuna assinalável. Gerir o risco de cibersegurança em qualquer organização deixou de ser uma opção, para ter que ser encarada como um objetivo primário. A natureza abrangente dos domínios de aplicação, o desenvolvimento de tecologias como a Internet das Coisas e a Inteligência Artificial, bem como o âmbito das ameaças e até o enquadramento legal, fazem da cibersegurança uma das áreas de saber mais multidisciplinares, tornando-se um desafio a preparação de qualquer programa de estudo nesta área.

O programa apresentado nesta proposta procura endereçar alguns desses desafios. Tem o mérito, antes de tudo, de procurar colmatar a enorme lacuna de educação e treino nesta área, identificada por diversas instituições nacionais e internacionais, que inclusive deram origem a diversos documentos estratégicos e recomendações relevantes. Tem ainda o mérito de procurar agregar competências de áreas tecnológicas, de gestão e de psicologia, respondendo ao desafio da multidisciplinaridade.

No entanto, para cumprir integralmente o propósito de formação de segundo nível, nesta área, a CAE identifica algumas limitações, em particular:

1) No que respeita ao corpo docente são várias as preocupações que surgiram:

a) de uma forma geral, o nível de especialização em cibersegurança do corpo docente é muito baixo, não satisfazendo os requisitos impostos pelo artigo 16º, do DL 74/2006, na sua redação do DL 65/2018;

b) a carga horário de alguns docentes é claramente exagerada, considerando o serviço docente global indicado; em particular, um dos docentes aparece responsável por cinco UCs do plano de estudos, três das quais no primeiro semestre, sem considerar o acompanhamento em Trabalho de Projeto ou Dissertação; este nível de esforço compromete claramente os resultados que se pretende atingir num segundo ciclo;

c) a dimensão do corpo docente é limitada, não estando garantido o cumprimento da alínea b) do número 1 do artigo 57º do Decreto-lei 74/2006, de 24 de março, com a redação atual pelo Decreto-lei 65/2018, de 16 de agosto. Considerando o número máximo de alunos indicado (35), as tarefas de supervisão e acompanhamento, em particular nas UCs Dissertação e Trabalho de Projeto, correm o risco de não serem efetivas afetando negativamente a imagem do programa;

d) num segundo ciclo de formação, a atividade de investigação assume um papel bastante importante. A limitada atividade de investigação da maioria do corpo docente na área da cibersegurança, pode facilmente comprometer esse objetivo, não estando cumprido o requisito da alínea c) do número 2, do artigo 16º do Decreto-lei 74/2006, de 24 de março, com a redação atual pelo Decreto-lei 65/2018, de 16 de agosto.

2) Uma área significativa para a melhoria da proposta é a necessidade de um maior compromisso institucional para investir em equipamento especializado (em conjunto com o corpo docente) para lançar um programa competitivo de cibersegurança. A falta de equipamentos específicos para o funcionamento do ciclo de estudos, não garante o cumprimento da alínea b) do número 2, do artigo 16º do Decreto-lei 74/2006, de 24 de março, com a redação atual pelo Decreto-lei 65/2018, de 16 de agosto.

3) Existem diversas referências internacionais para orientar a preparação de programas educativos em cibersegurança, assim como diversos programas com elevada reputação. Na proposta aqui em apreciação não existem evidências claras sobre essa desejável influência. Há referências à sua existência, mas não relativamente à forma como foram usadas na preparação da proposta.

4) A descrição de diversas UCs revelam também importantes limitações, conforme referido em detalhe na secção 4.6.1 deste relatório. Em particular a coerência entre os conteúdos e os resultados de aprendizagem, a metodologia de ensino-aprendizagem que é igual para todas as UCs independentemente da sua natureza e ainda clarificações sobre o regimo de funcionamento, principalmente para a UC final (Dissertação ou Trabalho de Projeto).

5) O termo "Resiliência" no título do programa parece ser um artifício sem fundamento e mina a credibilidade da proposta.

6) No que diz respeito à protecção de dados, o Plano de Gestão de Dados não inclui uma indicação da política que abrange a disponibilidade de dados para fins de publicação (particularmente relevante para uma Universidade). Frequentemente, as revistas científicas solicitam dados para efeitos de reprodutibilidade, devendo a Universidade mencionar a política para estes pedidos.

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

Cybersecurity is a relatively recent area with a growing impact, given the accelerated adoption of ICT in all sectors of activity. There are already specialised personnel in some of these sectors, but a notable gap is evident in many. Managing cybersecurity risk in any organization is no longer an option but rather a primary objective. The comprehensive nature of application domains, the development of technologies such as the Internet of Things and Artificial Intelligence, as well as the scope of threats and even the legal framework, make cybersecurity one of the most multidisciplinary areas of knowledge, making it a challenge to prepare any study program in this area.

The program presented in this proposal seeks to address some of these challenges. It has the merit, first of all, of seeking to fill the enormous gap in education and training in this area, identified by several national and international institutions, which have even given rise to several strategic documents and relevant recommendations. It also has the merit of seeking to add skills from technological, management and psychology areas, responding to the challenge of multidisciplinarity.

However, to fully satisfy the purpose of second-level training in this area, CAE identifies some limitations, in particular:

1) Concerning teaching staff, several concerns arose:

a) in general, the level of cybersecurity specialization of the teaching staff is limited, not meeting the requirements imposed by article 16 of DL 74/2006, in its wording of DL 65/2018;

b) the workload of some teachers is clearly exaggerated, considering the overall teaching service indicated; in particular, one of the professors appears responsible for five courses in the study plan, three in the first semester, without considering monitoring in Project Work or Dissertation; this level of effort clearly compromises the results intended to be achieved in a second cycle program;

c) The number of faculty members is limited, and compliance with paragraph b) of number 1 of article 57th of Decree-Law no. 74/2006, March 24th, in the current wording of Decree-Law no. 65/2018, August 16th, is not fulfilled. Considering the maximum number of students indicated (35), supervision and monitoring tasks, especially in the Dissertation and Research Project courses, run the risk of not being effective, negatively affecting the image of the program;

d) research activity plays a significant role in a second-cycle education program. The limited research activity of most faculty in cybersecurity can easily compromise this objective, not being fulfilled the requirement indicated in paragraph c), number 2 of article 16th of Decree-Law no. 74/2006, March 24th, in the current wording of Decree-Law no. 65/2018, August 16th.

2) A significant area for improvement of the proposal is the need for more institutional commitment to investing in specialized equipment (along with faculty) to launch a competitive cybersecurity program. The lack of specific equipment for the operation of the study programme does not guarantee compliance with paragraph b), number 2 of article 16th of Decree-Law no. 74/2006, March 24th, in the current wording of Decree-Law no. 65/2018, August 16th.

3) There are several international references to guide the preparation of educational programs in cybersecurity, as well as several programs with a high reputation. There must be clear evidence of this desirable influence in a proposal like this one. There are references to their existence but no evidence concerning how they were used in preparing the proposal.

4) The description of several courses also reveals important limitations, as detailed in section 4.6.1 of this report. In particular, the coherence between the contents and learning results, the teaching-learning methodology that is the same for all courses regardless of their nature, and clarifications on the operating regime, mainly for the final course (Dissertation or Research Project).

5) The term "Resilience" in the program title seems to be a gimmick without foundation and undermines the proposal's credibility.

6) Regarding data protection, the Data Management Plan does not include a pointer to the policy covering data availability for publication purposes (particularly relevant for a University). Several times, scientific journals have asked for data for reproducibility purposes, and the university should mention the policy for these requests.

13.2. Recomendação final.

[ ] A acreditação do ciclo de estudos [ ] A acreditação condicional do ciclo de estudos [X] A não acreditação do ciclo de estudos

13.3. Período de acreditação

[sem resposta]

13.4. Condições (se aplicável) (PT)

[sem resposta]

13.4. Condições (se aplicável) (EN)

[sem resposta]