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

1.3. Designação do ciclo de estudos. (EN)

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 Science 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

*[0523] Eletrónica e Automação
Engenharia e Técnicas Afins
Engenharia, Indústrias Transformadoras e Construção*

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

25.0

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

Podem-se candidatar ao acesso ao ciclo de estudos conducente ao grau de mestre:
a) Titulares do grau de licenciado ou equivalente legal, na área de Engenharia Informática ou áreas afins;
b) Titulares de um grau académico superior estrangeiro conferido na sequência de um 1.º ciclo de estudos organizado, de acordo com os princípios do Processo de Bolonha, por um Estado aderente a este Processo, na área de Engenharia Informática ou áreas afins;
c) Titulares de um grau académico superior estrangeiro, que seja reconhecido, como satisfazendo os objetivos do grau de licenciado, na área de Engenharia Informática ou áreas afins, pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão;
d) Detentores de um currículo escolar, científico ou profissional que seja reconhecido, como atestando a capacidade para realização deste ciclo de estudos, pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão.

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

The following candidates can apply for access to the cycle of studies leading to the master's degree:
a) Holders of a bachelor's degree or legal equivalent, in the area of Computer Science Engineering or similar areas;
b) Holders of a foreign higher academic degree awarded following a 1st cycle of studies organized, in accordance with the principles of the Bologna Process, by a State adhering to this Process, in the area of Computer Engineering or similar areas;
c) Holders of a foreign higher academic degree, which is recognised as satisfying the objectives of the Bachelor's degree, in the area of Computer Science Engineering or similar areas, by the Technical-Scientific Council of the Escola Superior de Tecnologia e Gestão;
d) Holders of an academic, scientific or professional curriculum that is recognized, as attesting to the ability to carry out this study cycle, by the Technical-Scientific Council of the Escola Superior de Tecnologia e Gestão.

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)

As condições especifica de ingresso são:
a) Titulares do grau de licenciado ou equivalente legal, na área de Engenharia Informática ou áreas afins;
b) Titulares de um grau académico superior estrangeiro conferido na sequência de um 1.º ciclo de estudos organizado, de acordo com os princípios do Processo de Bolonha, por um Estado aderente a este Processo, na área de Engenharia Informática ou áreas afins;
c) Titulares de um grau académico superior estrangeiro, que seja reconhecido, como satisfazendo os objetivos do grau de licenciado, na área de Engenharia Informática ou áreas afins, pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão;
d) Detentores de um currículo escolar, científico ou profissional que seja reconhecido, como atestando a capacidade para realização deste ciclo de estudos, pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão.

Cumprem os requisitos legais.

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

The specific conditions of entry are:
a) Holders of a bachelor's degree or legal equivalent in the area of Computer Engineering or related areas;
b) Holders of a foreign higher academic degree conferred following a 1st cycle of studies organized, in accordance with the principles of the Bologna Process, by a State adhering to this Process, in the area of Computer Engineering or related areas;
c) Holders of a foreign higher academic degree, which is recognized as meeting the objectives of the bachelor's degree, in the area of Computer Engineering or related areas, by the Technical-Scientific Council of the Higher School of Technology and Management;
d) Holders of an academic, scientific or professional curriculum that is recognized, as attesting the ability to carry out this cycle of studies, by the Technical-Scientific Council of the Higher School of Technology and Management.

Comply with legal requirements.

1.11. Modalidade do ensino

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

1.11.1. Regime de funcionamento, se presencial

Diurno

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)

Instituto Politécnico da Guarda (IPG)
Escola Superior de Tecnologia e Gestão (ESTG)
Avenida Dr. Francisco Sá carneiro, 50
6300-559 Guarda

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

Polytechnic Institute of Guarda (IPG)
School of Technology and Management (ESTG)
Avenida Dr. Francisco Sá carneiro, 50
6300-559 Guarda

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

Regulamento de Creditação de Competências_14022020 reduzido.pdf | *PDF* | *430.1 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 encontra-se publicado em D.R. Regulamento n.º 26/2020 de 6 de Fevereiro de 2020, 2ª série Parte E. É adequado e cumpre os requisitos legais.

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

The crediting regulation is published in D.R. Regulation No. 26/2020 of February 6, 2020, 2nd series Part E. It is adequate and complies with legal requirements.

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)

São apresentadas a ata n.º 2/2022 do Conselho Pedagógico e a ata N.º 10/2022 do Conselho Técnico Científico com as deliberações favoráveis para a criação do ciclo de estudos em Cibersegurança. Também é apresentado parecer favorável da Unidade Técnico Científica de Informática sobre a criação do ciclo de estudos de Mestrado em Cibersegurança.

2.1.1. Evidências que fundamentam a apreciação expressa (EN)

Minutes No. 2/2022 of the Pedagogical Council and Minutes No. 10/2022 of the Technical-Scientific Council are presented with favorable resolutions for the creation of the study programme in Cybersecurity. A favorable opinion of the Technical Scientific Unit of Informatics on the creation of the Master's study programme in Cybersecurity is also presented.

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)

O ciclo de estudos tem como objetivos gerais a formação de técnicos especializados capazes de mitigar o risco das ciberameaças nas organizações, ajudando-as a atingir os requisitos mínimos de segurança tanto das redes de dados como dos seus sistemas de informação.

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 objeto e os objetivos do ciclo de estudos são adequados para a modalidade de ensino presencial.

O instituto Politécnico da Guarda (IPG) têm como missão: formar profissionais qualificados, com o objetivo principal de garantir a qualidade das aprendizagens dos estudantes e potenciar o seu sucesso numa carreira profissional; a promoção de novos ciclos de estudo de acordo com as especialidades de formação do IPG e de os articular com as novas necessidades formativas identificadas a nível regional e nacional. O ciclo de estudos proposto insere-se na estratégia institucional de oferta formativa.

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

3.6.1. Apreciação global (EN)

The study programme has the general objectives of training specialized technicians capable of mitigating the risk of cyber threats in organizations, helping them to achieve the minimum security requirements of both data networks and their information systems.

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.

The object and objectives of the study programme are suitable for face-to-face teaching.

The Polytechnic Institute of Guarda (IPG) has the following mission: to train qualified professionals, with the main objective of guaranteeing the quality of student learning and enhancing their success in a professional career; the promotion of new study programmes according to the IPG training specialties and to articulate them with the new training needs identified at a regional and national level. The proposed study programme is part of the institutional strategy of training offer.

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

3.6.2. Pontos fortes (PT)

Ciclo de estudos numa área de demanda crescente por técnicos especializados na área abordada.

3.6.2. Pontos fortes (EN)

Study programme in an area of growing demand for specialist technicians in the area addressed.

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.

Sim

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 o 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 suportado num conjunto de objetivos gerais e num conjunto de objetivos de aprendizagem bem definidos, complementares e com uma boa completude no âmbito da Cibersegurança. Os conteúdos programáticos das unidades curriculares são coerentes com os objetivos de aprendizagem definidos e no seu todo, enquadrados com os objetivos de aprendizagem definidos para o ciclo de estudos. O número de ECTS está em conformidade com o necessário, assim como as restantes exigências. Existem, contudo, três aspetos que devem ser corrigidos, estando o primeiro relacionado com os domínios a abordar nos objetivos de aprendizagem, o segundo relacionado com o equilíbrio das áreas científicas no percurso curricular derivado da existências de unidades curriculares opcionais, e, o terceiro relacionado com os conteúdos programáticos de algumas unidades curriculares:

1.
Os objetivos de aprendizagem definidos para o ciclo de estudos pretendem capacitar os alunos de um conhecimento sustentado teoricamente, mas com uma competência prática efetiva, nomeadamente em seis domínios: (i) "proteção e privacidade dos dados e o seu enquadramento legal"; (ii) "segurança e defesa de redes e sistemas"; (iii) "ameaças e ataques"; (iv) "criptologia"; (v) "risco"; (vi) "processo de investigação científica na área da segurança informática".

Das nove unidades curriculares obrigatórias: duas enquadram-se no domínio da "segurança e defesa de redes e sistemas", nomeadamente "Segurança e Defesa de Redes" e "Administração e Segurança de Sistemas"; duas enquadram-se no domínio das "ameaças e ataques", nomeadamente "Análise de Ameaças" e "Segurança Ofensiva"; uma enquadra-se no domínio da "criptologia", nomeadamente "Criptologia Aplicada"; uma enquadra-se no domínio da "proteção e privacidade dos dados e o seu enquadramento legal", nomeadamente "Fundamentos de Cibersegurança"; e duas enquadram-se no domínio do "processo de investigação científica na área da segurança informática", nomeadamente "Metodologias de Investigação" e "Proposta de Investigação". A unidade curricular de Dissertação/Projeto/Estágio não se considerou enquadrada especificamente em nenhum dos domínios elencados nos objetivos de aprendizagem.

Considerando que existem catorze unidades curriculares opcionais que devem ser selecionadas pelos alunos para preencher quatro opções no primeiro ano, duas no primeiro semestre e duas no segundo semestre, existe a possibilidade do percurso conducente ao grau de mestre não incluir o domínio do "risco" enunciado nos objetivos de aprendizagem, pois existem apenas duas unidades curriculares que focam este domínio, nomeadamente "Administração de Segurança Empresarial" e "Avaliação do Risco em Cibersegurança", sendo ambas opcionais.

2.
Apresentam-se quatro áreas científicas, nomeadamente: Programação e Multimédia (PM); Engenharia de Software e Sistemas de Informação (ESSI); Redes e Sistemas Informáticos (RSI); e Direito (D). Contudo, nas unidades curriculares obrigatórias, as áreas científicas de ESSI e de D, apenas estão presentes nas unidades curriculares no domínio do "processo de investigação científica na área da segurança informática" juntamente com as outras duas áreas científicas, portanto, as áreas científicas de ESSI e de D podem não ser abordadas ao longo do ciclo de estudos, dependendo das escolhas dos alunos nas unidades curriculares opcionais.

3.
Na unidade curricular "Contextualização e História da Cibersegurança" apresenta-se como objetivo "Conhecer os diversos tipos de grupos de ciber atacantes, a sua constituição e motivações", nos conteúdos programáticos existe um tópico de "Análise de grupos de ciber atacantes", mas na bibliografia não se refere o maior referencial sobre esta matéria que é o Projeto Attack do Mitre (https://attack.mitre.org).

Verifica-se uma sobreposição evidente da matéria relativa ao "Regulamento Geral de Proteção de Dados" nas unidades curriculares "Fundamentos de Cibersegurança" e "Direito da Cibersegurança". Sugere-se que na unidade curricular opcional, a de "Direito da Cibersegurança", esta matéria possa ser substituída por outra no domínio do Direito, ou que se foque em maior profundidade as questões das Leis da Cibersegurança e do Cibercrime.
A tabela "4.1.2. Áreas científicas e créditos necessários à obtenção do grau", encontra-se incompleta pois apenas totaliza 96 créditos ECTS quando o ciclo de estudos está organizado para 120. É necessário que esta explicite de forma inequívoca o número de créditos ECTS que é necessário realizar para cada área cientifica e que perfaçam o total de 120 créditos ECTS em que o ciclo de estudos está organizado.

A tabela "4.1.2. Áreas científicas e créditos necessários à obtenção do grau", encontra-se incompleta pois apenas totaliza 96 créditos ECTS quando o ciclo de estudos está organizado para 120. É necessário que esta explicite de forma inequívoca o número de créditos ECTS, obrigatórios e opcionais, que é necessário realizar para cada área cientifica e que perfaçam o total de 120 créditos ECTS em que o ciclo de estudos está organizado.

4.6.1. Apreciação global (EN)

Curriculum development is supported by a set of general objectives and a set of well-defined, complementary learning objectives with good completeness in the context of Cybersecurity. The syllabus of the curricular units are coherent with the defined learning objectives and, as a whole, framed with the defined learning objectives for the study programme. The number of ECTS complies with what is necessary, as well as the other requirements. There are, however, three aspects that must be corrected, the first being related to the domains to be addressed in the learning objectives, the second related to the balance of scientific areas in the curricular path derived from the existence of optional curricular units, and the third related with the syllabus of some curricular units:

1.
The learning objectives defined for the study programme intend to enable students with a theoretically sustained knowledge, but with an effective practical competence, namely in six domains: (i) "protection and privacy of data and its legal framework"; (ii) "security and defense of networks and systems"; (iii) "threats and attacks"; (iv) "cryptology"; (v) "risk"; (vi) "scientific research process in the area of computer security".

Of the nine compulsory curricular units: two fall within the domain of "security and defense of networks and systems", namely "Security and Defense of Networks" and "Administration and Security of Systems"; two fall within the domain of "threats and attacks", namely "Threat Analysis" and "Offensive Security"; one falls within the domain of "cryptology", namely "Applied Cryptology"; one falls within the domain of "data protection and privacy and its legal framework", namely "Fundamentals of Cybersecurity"; and two fall within the scope of the "scientific research process in the area of computer security", namely "Research Methodologies" and "Research Proposal". The Dissertation/Project/Internship curricular unit was not considered to fall specifically into any of the domains listed in the learning objectives.

Considering that there are fourteen optional curricular units that must be selected by students to complete four options in the first year, two in the first semester and two in the second semester, there is a possibility that the path leading to the master's degree does not include the domain of the "risk" mentioned in the learning objectives, as there are only two curricular units that focus on this domain, namely "Corporate Security Administration" and "Risk Assessment in Cybersecurity", both of which are optional.

2.
Four scientific areas are presented, namely: Programming and Multimedia (PM); Software Engineering and Information Systems (ESSI); Networks and Computer Systems (RSI); and Right (D). However, in the compulsory curricular units, the scientific areas of ESSI and D, are only present in the curricular units in the field of "scientific research process in the area of computer security" together with the other two scientific areas, therefore, the scientific areas of ESSI and D may not be addressed throughout the study programme, depending on students' choices in optional course units.

3.
In the curricular unit "Contextualization and History of Cybersecurity", the objective is "To know the different types of groups of cyber attackers, their constitution and motivations", in the syllabus there is a topic of "Analysis of groups of cyber attackers", but the bibliography does not refer to the main reference on this matter, which is the Miter Attack Project (https://attack.mitre.org).

There is an evident overlap of the matter relating to the "General Data Protection Regulation" in the curricular units "Fundamentals of Cybersecurity" and "Cybersecurity Law". It is suggested that in the optional curricular unit, "Cybersecurity Law", this subject could be replaced by another one in the field of Law, or that the issues of Cybersecurity and Cybercrime Laws be focused in greater depth. The table "4.1.2. Scientific areas and credits required to obtain the degree", is incomplete as it only totals 96 ECTS credits when the study cycle is organized for 120. ECTS must be completed for each scientific area and that makes up the total of 120 ECTS credits in which the study program is organized.

4.6.2. Pontos fortes (PT)

A complementaridade dos objetivos de aprendizagem do ciclo de estudos.

4.6.2. Pontos fortes (EN)

The complementarity of the learning objectives of the study programme.

4.6.3. Pontos fracos (PT)

O elevado número de unidades curriculares opcionais.

4.6.3. Pontos fracos (EN)

The high number of optional course units.

5. Corpo Docente

5.1.1. Coordenação do ciclo de estudos.

Sim

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.

Em parte

5.3. Avaliação do pessoal docente.

Sim

5.4.1. Apreciação global (PT)

A coordenação do ciclo de estudos é assegurada por um docente doutor em informática e com publicações cientificas na área cientifica principal do ciclo de estudos.

Da análise às fichas curriculares dos docentes, verifica-se que o serviço docente atribuído é adequado, contendo alguma margem para a realização de outras atividades. Em média, considerando a distribuição máxima de 12 horas/semana, obtém-se uma percentagem de cerca de 75% deste valor, ou seja uma média de 9 horas/semana.

O corpo docente cumpre os requisitos legais: corpo docente próprio (85%), academicamente qualificado(62,8% sete doutores) e especializado (53,8% 5 doutores e dois especialistas).

Existe estabilidade do corpo docente por um período superior a três anos (77,92%).
Não existem docentes inscritos em programas de doutoramento há mais de um ano, porém seria conveniente reforçar o corpo doente com docentes doutorados na área da cibersegurança .

A avaliação de desempenho dos docentes encontra-se regulada pelo Regulamento n.º 521/2015, de 7 de agosto publicado em D.R. Cumpre os requisitos legais e prevê medidas conducentes à atualização permanente e desenvolvimento profissional.

Existe um docente apenas com o grau de licenciado obtido em 2014, a lecionar num ciclo de estudos de nível de mestrado e não é detentor do Título de Especialista (Art. 3.º alínea g do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto). A proposta, no campo de observações, resume a experiência profissional deste docente. Porém o mecanismo legal disponível é através da certificação dessa experiência profissional por meio da obtenção do Título de Especialista atrás referido.

A proposta indica zero docentes filiados Unidades de Investigação da Instituição acreditadas pela FCT, mas nas fichas de docentes apresentadas contam-se cinco (43,3%) ligados a centros acreditados pela FCT pertencentes a outras instituições.

5.4.1. Apreciação global (EN)

Coordination of the study programme is ensured by a professor with a Ph.D. in informatics and scientific publications in the main scientific area of the study programme.

From the analysis of the professors' CVs, it appears that the assigned teaching service is adequate, with some margin for carrying out other activities. On average, considering the maximum distribution of 12 hours/week, a percentage of around 75% of this value is obtained, i.e. an average of 9 hours/week.

The teaching staff complies with the legal requirements: own teaching staff (85%), academically qualified (62.8% seven doctors) and specialized (53.8% 5 doctors and two specialists).

There is stability of the teaching staff for a period of more than three years (77.92%).

There are no professors enrolled in doctoral programs for more than a year, but it would be convenient to reinforce the faculty with professors who have a doctorate in the area of cybersecurity.

The performance evaluation of teachers is regulated by Regulation n.º 521/2015, of 7 August published in D.R. It complies with legal requirements and provides for measures conducive to permanent updating and professional development.

There is one teacher with a bachelor's degree obtained in 2014, teaching in a master's level study programme and does not hold the Title of Specialist (Art. 3.º line g of DL n.º 74/2006, of 24 March in the wording of DL n.º 65/2018, August 16th). The proposal, in the field of observations, summarizes this teacher's professional experience. However, the legal mechanism available is through the certification of this professional experience by obtaining the aforementioned Specialist Title.

The proposal indicates zero professors affiliated to the Institution's Research Units accredited by the FCT, but in the professors' files presented there are five (43.3%) linked to centers accredited by the FCT belonging to other institutions.

5.4.2. Pontos fortes (PT)

Nada a reportar.

5.4.2. Pontos fortes (EN)

Nothing to report.

5.4.3. Pontos fracos (PT)

Docente apenas com o grau de licenciado obtido em 2014, e não é detentor Título de Especialista (Art. 3.º alínea g do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto). Recomenda-se vivamente a equacionar o procedimento para obtenção deste Título.

Dada a natureza do ciclo de estudos, requer atualização permanente, recomendam-se esforços no sentido de aumentar o número de docentes filiados em centros de investigação acreditados pela FCT.

5.4.3. Pontos fracos (EN)

Teacher with only a bachelor's degree obtained in 2014 and does not hold the Title of Specialist (Art. 3.º line g of DL n.º 74/2006, of March 24 in the wording of DL n.º 65/2018, August 16th). It is strongly recommended to consider the procedure for obtaining this Title.

Given the nature of the study programme, which requires permanent updating, efforts are recommended to increase the number of professors linked to research centers accredited by FCT.

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)

A ESTG conta com 18 funcionários contratados a 100% com as seguintes qualificações: Mestrado cinco, Licenciatura três, Ensino secundário quatro, 3.º ciclo de ensino básico três, 2.º ciclo de ensino básico um e 1.º ciclo de ensino básico dois.

A avaliação do desempenho do pessoal não docente realiza-se cumprindo o previsto no Sistema Integrado de Gestão e Avaliação do Desempenho na Administração Pública (SIADAP) e estão implementadas medidas conducentes à sua permanente atualização e desenvolvimento profissional.

6.4.1. Apreciação global (EN)

ESTG has 18 employees hired 100% with the following qualifications: Master's five, Bachelor's degree three, Secondary education four, 3rd cycle of basic education three, 2nd cycle of basic education one and 1st cycle of basic education two.

The performance assessment of non-teaching staff is carried out in compliance with the Integrated Management and Performance Assessment System in Public Administration (SIADAP) and measures leading to their permanent updating and professional development are implemented.

6.4.2. Pontos fortes (PT)

Corpo de pessoal técnico e administrativo adequado.

6.4.2. Pontos fortes (EN)

Adequate technical and administrative staff.

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)

Dispõem de 9 salas de informática equipadas com PC e software, cerca de 40 salas de aula e diversos laboratórios nomeadamente: Robótica, Redes e Sistemas Informáticos, Programação e Multimédia,
Engenharia de Software e Sistemas de Informação. Dispõem também de outras instalações de utilização transversal, como sala de Informática (alunos), sala de reuniões e de videoconferência, auditório, biblioteca (1651 m2) e diversas salas mais pequenas para os alunos e gabinetes onde os docentes prestam atendimento aos alunos.

Encontram-se disponíveis duas plataformas de eLearning: o Sistema Integrado de Gestão Académica (Sigarra) e o Modular Object Oriented Dynamic Learning Environment (Moodle). Também disponível uma infraestrutura de rede sem fios Eduroam e apossibilidade de professores, funcionários e alunos estabelecerem uma ligação VPN para poderem aceder a diversos serviços internos. Também se dispõe de acesso ao COLIBRI que disponibiliza ferramentas para a realização de aulas, reuniões ou trabalhos de grupo para professores e alunos através da Internet.

A proposta apresenta uma extensa lista de equipamentos e softwares disponíveis nos laboratórios nomeadamente: 319 computadores, 21 kits didaticos, principais ferramentas de desenvolvimento Microsoft, 13 Routers Cisco e Enterasys , um Sistema de videoconferência, oito Switchs Cisco e Enterasys e 42 Softwares Packet Tracer 5.0.

7.4.1. Apreciação global (EN)

They have 9 computer rooms equipped with PC and software, about 40 classrooms and several laboratories, namely: Robotics, Computer Networks and Systems, Programming and Multimedia,
Software Engineering and Information Systems. They also have other facilities for transversal use, such as the IT room (students), meeting and videoconferencing room, auditorium, library (1651 m2) and several smaller rooms for students and offices where teachers provide assistance to students.

Two eLearning platforms are available: the Integrated Academic Management System (Sigarra) and the Modular Object Oriented Dynamic Learning Environment (Moodle). Also available is an Eduroam wireless network infrastructure and the possibility for teachers, staff and students to establish a VPN connection in order to access various internal services. They also have access to COLIBRI, which provides tools for conducting classes, meetings or group work for teachers and students via the Internet.

The proposal presents an extensive list of equipment and software available in the laboratories namely: 319 computers, 21 teaching kits, main Microsoft development tools, 13 Cisco and Enterasys Routers, a videoconference system, eight Cisco and Enterasys Switches and 42 Packet Tracer 5.0 Software.

7.4.2. Pontos fortes (PT)

Infraestrutura de suporte à atividade letiva adequada.

7.4.2. Pontos fortes (EN)

Support infrastructure adequate for 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 para ver reconhecida a sua autoria em projectos ou artigos, esta análise considerou 3 indicadores: produção científica, bolsas de projeto e formação (cursos) ou qualificações nos últimos 5 anos. Em geral, há publicações científicas em revistas ou conferências com revisão por pares. Este facto é observado em cerca de 69,23% dos casos dos docentes. No entanto, do ponto de vista da investigação de impacto (publicações indexadas de renome), tal foi observado em apenas 7,69% dos casos dos docentes (apenas 1 docente tem 1+ publicações no Q1 - ocupado pelos 25% melhores periódicos, no Scimago Journal & Country Rank); este docente é da área da física. No entanto, 76,92% dos docentes não têm publicações indexadas ao impacto (4 professores com publicações em revistas não revistas por pares, 2 com a última publicação em 2018 e um em coautoria do outro, e 4 professores sem publicações). Estes números indicam pouca atividade na área da investigação, o que é uma preocupação para um programa de mestrado. Atualmente, nenhum dos membros do corpo docente tem uma bolsa de projeto comunicada. A maior parte dos projectos comunicados são antigos (cerca de 10 anos) ou estão fora do domínio da cibersegurança, ou ambos. Não foram comunicadas quaisquer parcerias nacionais ou internacionais de intercâmbio de estudantes ou de professores. Não foi identificada qualquer ação de docentes na procura de qualificações.

8.5.1. Apreciação global (EN)

In order to evaluate everything that the lecturers do to show that they are up to date in the field or to have their authorship recognized in projects or articles, 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. This is observed in about 69.23% of the cases of the lecturers. However, from the point of view of impact research (reputable indexed publications), this was observed in only 7.69% of cases for the lecturers (only 1 lecturers have 1+ publications in Q1 - occupied by the top 25% of journals, in Scimago Journal & Country Rank); this lecturer is from the field of physics. However, 76.92% of the lecturers have no impact-indexed publications (4 professors with publications in non-peer-reviewed journals, 2 with last publication in 2018 and one co-authoring the other, and 4 professors with no publications).These numbers indicate little activity in the area of research, which is a concern for an M.S. program. Currently, none of the faculty members has a reported project grant. Most of the reported projects are old (approximately 10 years old) or outside the field of cybersecurity, or both. No national or international student or faculty exchange partnerships have been reported. No lecturers action has been identified in searching for qualifications.

8.5.2. Pontos fortes (PT)

A maioria (69,23%) dos membros do corpo docente considera necessário manter-se atualizado no domínio da cibersegurança através da publicação em conferências, revistas e mídia não científica. No entanto, 38,46% dos docentes distinguiram-se por terem escrito pelo menos um artigo científico publicado no estrato Q1 da Scimago a partir de 2018.

8.5.2. Pontos fortes (EN)

The majority (69.23%) of lecturers consider it necessary to stay up-to-date in the cybersecurity domain by publishing in conferences, journals, and non-scientific media. However, 38.46% of faculty members distinguished themselves by having written at least one scientific paper published in Scimago's Q1 stratum as of 2018.

8.5.3. Pontos fracos (PT)

É preocupante que 76,92% dos docentes não sejam protagonistas de qualquer produção autoral significativa (artigos científicos indexados de renome ou bolsas de projecto) nos ultimos 5 anos. Este facto levanta a preocupação de que os docentes se tornem meros duplicadores do que outros produzem em termos de materiais didácticos de qualidade. Claro que os docentes podem escrever livros ou capítulos de livros, mas a área em que trabalhamos é tão dinâmica que estes tendem a ficar desactualizados rapidamente. Por isso, para orientar alunos de mestrado, o docente não pode se isentar da responsabilidade de ser um autor de material de qualidade e revisto por pares, porque, no que diz respeito à cibersegurança, se não inovarmos, seremos sempre vítimas dos atacantes. É necessário reforçar a cooperação internacional, que não tem sido desenvolvida da forma esperada para um curso de sucesso. É também urgente fazer com que os professores estudem, os 30,76% que nem sequer se actualizaram com cursos de reciclagem nos últimos 5 anos. Não são referidos projectos significativos de cibersegurança na secção 8.2.

8.5.3. Pontos fracos (EN)

It is worrying that 76,92% of lecturers are not protagonists of any significant authorial production (renowned indexed scientific papers or project grants) in the last 5 years. This raises the concern that lecturers become mere duplicators of what others produce in terms of quality teaching materials. Of course, lecturers may write books or book chapters, but the area we work in is so dynamic that these tend to become outdated very fast. Therefore, to advise master's students, the lecturer cannot escape the responsibility of authoring quality, peer-reviewed material, because when it comes to cybersecurity, if we do not innovate we will always be attackers' victims. There is a need to strengthen international cooperation, which has not been developed in the way expected for a successful course. It is also urgent to get the teachers (30,76%) who have not even updated with refresher courses in the last 5 years to study. No significant cybersecurity projects are mentioned in section 8.2.

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 (eees).

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.

Sim

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

10.3.1. Apreciação global (PT)

De um modo geral, o curso segue o que se observa noutras propostas de EEES. No entanto, na proposta do IPG, as AC de Engenharia de Software e Sistemas de Informação (ESSI) e Direito (D) são contempladas de forma comum a outras UC, uma vez que tem 5 AC e 6 UC obrigatórias. É aconselhável analisar mais de perto o Mestrado em Cibersegurança proposto pela Università degli Studi di Milano. Analisando a proposta da Ecole Polytechnique Fédérale de Lausanne, podemos constatar que o Mestrado em Cibersegurança é um programa conjunto EPFL-ETHZ, o que constitui um ponto fraco na proposta do IPG, uma vez que a colaboração na investigação e o intercâmbio de estudantes e professores são altamente recomendados. A internacionalização é também muito desejável num programa de investigação. No entanto, não é abordada na proposta do IPG, tal como acontece no mestrado EURECOM em segurança digital.

10.3.1. Apreciação global (EN)

Generally, the course follows what is observed in other EEES proposals. However, in the IPG proposal, the CA of Software Engineering and Information Systems (ESSI) and Law (D) are covered in a common way in the CUn, as it has 5 scientific fields (SF) and 6 mandatory curriculum units (CUn). It is advisable to take a closer look at the Master in Cybersecurity proposed by the Università degli Studi di Milano. Looking at the proposal of the Ecole Polytechnique Fédérale de Lausanne, we can see that the Master in CyberSecurity is a joint EPFL-ETHZ programme, which is a weakness in the IPG proposal, as collaborating on research and exchanging students and professors is highly recommended. Internationalization is also very desirable in a research program. However, it is not addressed in the IPG proposal, as it is in the EURECOM master's in digital security

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 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 course 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)

São apresentados apenas três protocolos com entidades recetoras de estágios. Para um total de 25 alunos, deveriam estabelecer-se mais protocolos com entidades recetoras de estágios.

11.6.1. Apreciação global (EN)

Only three protocols with entities receiving internships are presented. For a total of 25 students, more protocols should be established with entities that receive 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)

Poucos protocolos com entidades recetoras de estágios.

11.6.3. Pontos fracos (EN)

Few protocols for entities receiving internships.

12. Observações finais.

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

A CAE concorda com as propostas de alteração propostas na pronúncia.

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

CAE agrees with the proposed changes in the response.

12.2. Observações (PT)

Na pronuncia, a Instituição aceita o cumprimento das condições apresentadas e assume o compromisso de as cumprir na íntegra. A proposta deverá ser corrigida em conformidade.

A CAE considera que as condições pedidas se encontram satisfeitas, sendo de propor a acreditação incondicional do ciclo de estudos.

12.2. Observações (EN)

In the response, the Institution accepts compliance with the conditions presented and assumes the commitment to comply with them in full. The proposal should be amended accordingly.

The EAC considers that the requested conditions are satisfied, and proposes the unconditional accreditation of the study programme..

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, pretende formar técnicos especializados capazes de mitigar o risco das ciberameaças nas organizações, ajudando-as a atingir os requisitos de segurança tanto das redes de dados como dos seus sistemas de informação, apresentando-se como uma oferta inovadora na região de influência do Instituto Politécnico da Guarda.

Está em consonância com a missão do Instituto Politécnico de Guarda, 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 (84,6%), academicamente qualificado (62,8%) e especializado (51,9%) com afetação de serviço docente adequada. Verifica-se uma percentagem baixa de docentes envolvidos em unidades de investigação acreditadas e consequentemente um número baixo de publicações em revistas internacionais na área principal do ciclo de estudos.

O ciclo de estudos apresenta uma perspetiva de uma procura razoável por parte de potenciais estudantes.

O nível de empregabilidade dos graduados deverá ser bom.

O plano de estudos tal como se encontra apresenta alguns aspetos que necessitam de ser revistos (ver 4.61 deste relatório):

- A tabela "4.1.2. Áreas científicas e créditos necessários à obtenção do grau", encontra-se incompleta pois apenas totaliza 96 créditos ECTS quando o ciclo de estudos está organizado para 120. É necessário que esta explicite de forma inequívoca o número de créditos ECTS, obrigatórios e opcionais, que é necessário realizar para cada área cientifica e que perfaçam o total de 120 créditos ECTS em que o ciclo de estudos está organizado.

- Considerando que existem catorze unidades curriculares opcionais que devem ser selecionadas pelos alunos para preencher quatro opções no primeiro ano, duas no primeiro semestre e duas no segundo semestre, existe a possibilidade do percurso conducente ao grau de mestre não incluir o domínio do "risco" enunciado nos objetivos de aprendizagem, pois existem apenas duas unidades curriculares que focam este domínio, nomeadamente "Administração de Segurança Empresarial" e "Avaliação do Risco em Cibersegurança", sendo ambas opcionais.

- Apresentam-se quatro áreas científicas, nomeadamente: Programação e Multimédia (PM); Engenharia de Software e Sistemas de Informação (ESSI); Redes e Sistemas Informáticos (RSI); e Direito (D). Contudo, nas unidades curriculares obrigatórias, as áreas científicas de ESSI e de D, apenas estão presentes nas unidades curriculares no domínio do "processo de investigação científica na área da segurança informática" juntamente com as outras duas áreas científicas, portanto, as áreas científicas de ESSI e de D podem não ser abordadas ao longo do ciclo de estudos, dependendo das escolhas dos alunos nas unidades curriculares opcionais.

- Na unidade curricular "Contextualização e História da Cibersegurança" apresenta-se como objetivo "Conhecer os diversos tipos de grupos de ciber atacantes, a sua constituição e motivações", nos conteúdos programáticos existe um tópico de "Análise de grupos de ciber atacantes", mas na bibliografia não se refere o maior referencial sobre esta matéria que é o Projeto Attack do Mitre (https://attack.mitre.org).

- Verifica-se uma sobreposição evidente da matéria relativa ao "Regulamento Geral de Proteção de Dados" nas unidades curriculares "Fundamentos de Cibersegurança" e "Direito da Cibersegurança". Sugere-se que na unidade curricular opcional, a de "Direito da Cibersegurança", esta matéria possa ser substituída por outra no domínio do Direito, ou que se foque em maior profundidade as questões das Leis da Cibersegurança e do Cibercrime.

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

Na pronuncia, a Instituição aceita o cumprimento das condições apresentadas e assume o compromisso de as cumprir na íntegra.
A CAE considera que as condições pedidas se encontram satisfeitas, sendo de propor a acreditação incondicional do ciclo de estudos.

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

The study programme in Cybersecurity aims to train specialized technicians capable of mitigating the risk of cyberthreats in organizations, helping them to meet the security requirements of both data networks and their information systems, presenting itself as an innovative offer in region of influence of the Polytechnic Institute of Guarda.

It is in line with the mission of the Polytechnic Institute of Guarda, complies with the legal requirements in terms of curriculum structure, study plan, ECTS and workload involved and fits in with the educational, scientific and cultural project of the institution. 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 study programme is associated with a teaching staff that meets the legal requirements: its own teaching staff (84.6%), academically qualified (62.8%) and specialized (51.9%) with adequate allocation of teaching service. There is a low percentage of professors involved in accredited research units and consequently a low number of publications in international journals in the main area of the study cycle.

The study cycle presents a perspective of reasonable demand from potential students.

The employability level of graduates should be good.

The study plan as it stands presents some aspects that need to be reviewed (see 4.61 of this report):

- The table "4.1.2. Scientific areas and credits necessary to obtain the degree", is incomplete as it only totals 96 ECTS credits when the study programme is organized for 120, it is necessary to carry out for each scientific area and that they make up the total of 120 ECTS credits in which the study programme organized.

- Considering that there are fourteen optional curricular units that must be selected by students to complete four options in the first year, two in the first semester and two in the second semester, there is a possibility that the path leading to the master's degree does not include the domain of "risk" stated in the learning objectives, as there are only two curricular units that focus on this domain, namely "Corporate Security Administration" and "Risk Assessment in Cybersecurity", both of which are optional.

- Four scientific areas are presented, namely: Programming and Multimedia (PM); Software Engineering and Information Systems (ESSI); Networks and Computer Systems (RSI); and Right (D). However, in the compulsory curricular units, the scientific areas of ESSI and D, are only present in the curricular units in the field of "scientific research process in the area of computer security" together with the other two scientific areas, therefore, the scientific areas of ESSI and D may not be addressed throughout the study programme, depending on students' choices in optional course units.

- In the curricular unit "Contextualization and History of Cybersecurity", the objective is "To know the different types of groups of cyber attackers, their constitution and motivations", in the syllabus there is a topic of "Analysis of groups of cyber attackers", but the bibliography does not refer to the main reference on this matter, which is the Miter Attack Project (https://attack.mitre.org).

- There is an evident overlap of the matter relating to the "General Data Protection Regulation" in the curricular units "Fundamentals of Cybersecurity" and "Cybersecurity Law". It is suggested that in the optional curricular unit, "Cybersecurity Law", this subject could be replaced by another one in the field of Law, or that the issues of Cybersecurity and Cybercrime Laws be focused in greater depth.

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

In the response, the Institution accepts compliance with the conditions presented and assumes the commitment to comply with them in full. The EAC considers that the requested conditions are satisfied, and proposes the unconditional accreditation of the study programme.

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]