COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS

COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS

Ana Margarida Seixas Costa

Principais Riscos e Práticas de Controlo em Cibersegurança – Perceções dos Intervenientes e Estratégias Implementadas em Instituições de Ensino Superior em Portugal

Coimbra, abril de 2025

Principais Riscos e Práticas de Controlo em Cibersegurança

Ana Margarida Seixas Costa

ISCAC | 2025

Ana Margarida Seixas Costa

Título

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Auditoria Empresarial e Pública,** realizada sob a orientação da Professora Isabel Pedrosa.

Coimbra, abril de 2025

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

AGRADECIMENTOS

Em primeiro lugar, expresso a minha mais sincera gratidão à Professora Isabel Pedrosa, pela confiança depositada, pela proximidade e amizade demonstradas, pelos valiosos ensinamentos partilhados ao longo deste percurso, bem como pela constante disponibilidade e orientação, desde o início da dissertação. As suas correções e sugestões revelaram-se determinantes para a concretização deste trabalho.

Aos meus pais, deixo o meu mais profundo reconhecimento, pelo apoio incondicional, pela força partilhada nos momentos mais difíceis, pela persistência com que enfrentaram comigo cada obstáculo, pelo estímulo constante para não desistir e pela resiliência que tornou possível a realização deste objetivo de vida.

Aos entrevistados, pela participação e contributo sem o qual não teria sido possível realizar o estudo empírico.

Por último, ao meu namorado, por ser o meu pilar e me incentivar sempre a não desistir nos momentos mais difíceis.

RESUMO

Atualmente as Instituições de Ensino Superior enfrentam desafios cada vez mais complexos no domínio da cibersegurança, resultantes da sua estrutura organizacional aberta e da crescente dependência das tecnologias digitais. Estas instituições armazenam e processam volumes significativos de dados sensíveis, incluindo informações pessoais, académicas e financeiras de alunos e colaboradores, bem como dados relacionados com investigação académica e propriedade intelectual. Dada a natureza crítica desta informação, torna-se fundamental garantir que as IES implementam medidas de segurança da informação capazes de mitigar riscos. A globalização e a expansão das tecnologias de informação trouxeram inúmeras vantagens para o ensino e para a investigação, no entanto permitiram também o uso indevido por parte de agentes maliciosos (*hackers*). Assim, torna-se essencial prevenir potenciais comportamentos deste tipo, que podem ter consequências catastróficas para as instituições. A cibersegurança, surge como uma forma de prevenir ataques informáticos, permitindo assim a salvaguarda das redes e computadores, bem como a integridade da informação. Para tal, torna essencial fomentar uma cultura de segurança digital junto de toda comunidade académica, promovendo a formação e sensibilização contínua dos utilizadores. O presente estudo tem como principal objetivo sensibilizar para a necessidade de uma abordagem estratégica e robusta de cibersegurança nas IES, promovendo a segurança e a integridade da informação num contexto cada vez mais vulnerável a ataques de cibersegurança. Para tal foram realizadas duas entrevistas com responsáveis da área de Cibersegurança em duas IES distintas, uma pertencente ao Subsistema de Ensino Superior Público Politécnico e outra ao Subsistema de Ensino Superior Público Universitário. As entrevistas permitiam concluir que ambas as Instituições demonstram um compromisso claro com a cibersegurança, ainda que se encontrem em fases distintas de maturidade organizacional. Enquanto a primeira apresenta uma estrutura mais consolidada, com políticas formais e práticas regulares de sensibilização e auditoria, a segunda já implementou várias medidas de segurança, no entanto ainda não se encontram formalizadas num único documento estratégico.

Palavras-chave: Cibersegurança; Instituições de Ensino Superior; IES; Segurança da Informação; Medidas de Segurança da Informação

ABSTRACT

Higher education institutions are currently facing increasingly complex challenges in the field of cybersecurity, arising from their open organizational structure and growing dependence on digital technologies. These institutions store and process significant volumes of sensitive data, including personal, academic, and financial information of students and staff, as well as data related to academic research and intellectual property. Given the critical nature of this information, it is essential that the IES implement measures capable of mitigating risks. Globalization and the expansion of information technologies have brought numerous advantages to education and research; however, they have also enabled misuse by malicious actors (hackers). Therefore, it is crucial to prevent such behaviors that may lead to catastrophic consequences for these institutions. Cybersecurity emerges as a means of preventing cyberattacks, thereby safeguarding networks and computers, as well as the integrity of information. To achieve this, it is essential to foster a culture of digital security throughout institutions and the academic community, promoting continuous training and awareness among users. Thus, this study aims to raise awareness of the need for a strategic and robust cybersecurity approach in higher education institutions, promoting the security and integrity of information in a context increasingly vulnerable to cyberattacks. In order to achieve this, two interviews were conducted with Cybersecurity officers from two distinct higher education institutions, one from Public Polytechnic Higher Education Subsystem and the other from the blic University Higher Education Subsystem. The interviews revealed that both institutions demonstrate a clear commitment to cybersecurity, even though they are at different stages of organizational maturity. While the first has a more consolidated structure, with formal policies and regular awareness and audit practices, the second has already implemented several security measures, although these have not yet been formalized in a single strategic document.

Keywords: Cybersecurity; Higher Education Institutions; HEI; Information Security; Information Security Measures

ÍNDICE GERAL

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

Lista de abreviaturas, acrónimos e siglas

AMA I.P. - Agência para a Modernização Administrativa, I. P.

AUP - Política de Uso Aceitável

CERT - Computer Emergency Response Team

CIS - Center for Internet Security

CMMC - Cybersecurity Maturity Model Certification

CNCS – Centro Nacional de Cibersegurança de Portugal

CNPD - Comissão Nacional de Proteção de Dados

COBIT - Control Objectives for Information and Related Technologies

CSF - Cyber Security Framework

CSIRT - Computer Security Incident Response Team

DGES - Direção Geral do Ensino Superior

DHS - Departamento de Segurança Interna dos EUA

EDN - Estratégia Digital Nacional

ENISA - Agência da União Europeia para a Cibersegurança

EPD – Encarregado de Proteção de Dados

IA – Inteligência Artificial

IAR - *Information Asset Register*

IEC - International Electrotechnical Commission

IES – Instituições de Ensino Superior

INCoDe.2030 - Iniciativa Nacional Competências Digitais e.2030

INE – Instituto Nacional de Estatística

ISACA - Information Systems Audit and Control Association

ISO - International Organization for Standardization

IUTICAP - Inquérito à Utilização de Tecnologias da Informação e da Comunicação - Administração Pública Central e Regional

MCTES - Ministério da Ciência, Tecnologia e Ensino Superior

MRR - Mecanismo de Recuperação e Resiliência

NIST – National Institute of Standards and Technology

PATD - Plano de Ação para a Transição Digital

PRR - Plano de Recuperação e Resiliência

QACC - Quadro de Avaliação de Capacidades de Cibersegurança

QNRCS - Quadro Nacional de Referência para a Cibersegurança

QUT - *Queensland University of Technology*

RGPD - Regime Geral de Proteção de Dados

SGSI - Sistema de Gestão de Segurança da Informação

SISO - Sistema de Informação de Segurança da Organização

TD – Transformação Digital

TI – Tecnologias de Informação

TIC - Tecnologias da Informação e Comunicação

VPN - Redes Privadas Virtuais

UE – União Europeia

INTRODUÇÃO

A Internet está hoje profundamente integrada em praticamente todos os aspetos da vida quotidiana. No entanto, aquando do seu aparecimento, em meados da década de 1960, destinava-se a um grupo restrito de utilizadores, sobretudo investigadores e cientistas. Nesta fase inicial, a execução de crimes informáticos exigia, na maioria dos casos, o acesso físico ao equipamento. No entanto, atualmente, este cenário alterou-se drasticamente, sendo possível executar este tipo de crime, remotamente, a partir de qualquer parte do mundo, o que aumenta exponencialmente o risco. Além disso, a evolução das ameaças digitais tem sido marcada por uma crescente sofisticação dos métodos utilizados pelos cibercriminosos, o que exige respostas cada vez mais robustas e eficazes por parte das instituições.

Neste contexto, a gestão do risco de cibersegurança, tradicionalmente, associada à aquisição de tecnologia adequada, deve, segundo Serres (2018) assumir uma abordagem integrada que envolva que envolva não apenas a tecnologia, mas também o capital humano, os processos internos e os modelos operacionais e de gestão. O autor sublinha ainda que, quanto maior é a organização, maior será a complexidade associada à implementação de mecanismos eficazes de segurança, pelo que não existe uma solução universal de segurança da informação. Cada instituição deverá desenvolver a sua própria estratégia de proteção, com base no autoconhecimento, na compreensão do setor em que se encontra inserida e na avaliação dos riscos que o mesmo acarreta.

No caso específico das Instituições de Ensino Superior, tem-se verificado, nos últimos anos, a crescente preocupação com o reforço de medidas de segurança da informação. As medidas de segurança visam, não só a proteção de dados sensíveis e informações, mas também a salvaguarda da reputação institucional e o cumprimento das exigências legais em vigor, como o Regime Geral de Proteção de Dados (RGPD), a legislação nacional em matéria de cibercrime e as orientações definidas pelo Centro Nacional de Cibersegurança (CNCS), no âmbito da Estratégia Nacional de Segurança do Ciberespaço.

O principal objetivo deste estudo é sensibilizar para a necessidade de uma abordagem estratégica e robusta de cibersegurança nas IES, promovendo a segurança e a integridade da informação num contexto cada vez mais vulnerável a ataques de cibersegurança.

Para tal foram realizadas duas entrevistas com responsáveis da área de Cibersegurança em duas IES distintas, uma pertencente ao Subsistema de Ensino Superior Público Politécnico e outra ao Subsistema de Ensino Superior Público Universitário de forma a permitir: (i) avaliar o nível de preparação existente nas IES em Portugal e a sua capacidade para prevenir, detetar e responder a incidentes de cibersegurança; (ii) identificar os principais desafios e vulnerabilidades enfrentados pelas IES em Portugal; (iii) analisar a existência e a eficácia de políticas e práticas de cibersegurança; (iv) avaliar a existência de um plano de resposta a ataques e a sua eficácia na mitigação de danos; e, por fim, (v) recolher perspetivas sobre oportunidades de melhoria e necessidades futuras.

O presente estudo encontra-se estruturado de forma a abordar de maneira abrangente o tema da cibersegurança nas IES. O primeiro capítulo, intitulado Estado de Arte, faz uma revisão detalhada da literatura, dividindo-se em diversas seções que contextualizam as IES no cenário da globalização e da transformação digital, além de explorar os conceitos fundamentais de cibersegurança, as vulnerabilidades específicas das IES e a evolução da cibersegurança no setor educativo. A parte normativa também é abordada, com foco nos regulamentos e frameworks internacionais, bem como na legislação portuguesa. Além disso, são descritas as principais medidas de segurança da informação e boas práticas recomendadas para a implementação de estratégias eficazes de cibersegurança nessas organizações.

No segundo capítulo, Estudo Empírico, apresenta-se a metodologia adotada para a investigação, detalhando a caracterização da população alvo, o processo de seleção dos entrevistados e a técnica de recolha de dados utilizada. A análise dos resultados das entrevistas, juntamente com a discussão dos principais contributos, é feita de forma detalhada.

1 Estado de Arte

1.1 Instituições de Ensino Superior e a Globalização

Neste capítulo, será realizada uma análise aprofundada da literatura relevante, baseada em livros, artigos científicos, dissertações, bem como na consulta de diplomas legais e fontes noticiosas. O objetivo é proporcionar uma compreensão detalhada da evolução histórica e das definições chave relacionadas com o sistema de ensino superior e a cibersegurança, bem como analisar as políticas de segurança, tanto a nível europeu como nacional, que foram implementadas nestas Instituições para prevenir ataques no ciberespaço.

Esta revisão servirá como base para a discussão apresentada no ponto 2, que pretende aferir, através de entrevistas realizadas a intervenientes de Instituições de Ensino Superior (IES) em Portugal, quais os principais riscos e práticas de controlo em cibersegurança nestas Instituições, bem como as estratégias já implementadas para mitigar riscos.

1.1.1 Enquadramento histórico do Sistema de Ensino Superior

Desde a antiguidade é possível identificar formas de educação e transmissão de conhecimento cultural entre os povos primitivos. No entanto, foi na Grécia Antiga que surgiu o conceito de educação como existe na atualidade. Segundo Luzuriaga (1985), foi nessa região que apareceram os sofistas, considerados os primeiros educadores conscientes da história e que se assemelham, na atualidade, à figura do professor.

Ao longo do século XX, o conceito da educação foi sendo desenvolvido e, simultaneamente, sofrendo diversas alterações. Segundo Newman (1919) uma universidade era vista como "*um lugar onde a investigação é impulsionada, as descobertas verificadas e aperfeiçoadas, a imprudência tornada inócua e o erro, pela colisão de mente com mente e conhecimento com conhecimento. É o lugar onde o professor se torna eloquente e é um missionário e um pregador, mostrando a sua ciência na sua forma mais completa e vitoriosa, derramando-a com o zelo do entusiasmo e acende o seu próprio amor por ela nos corações dos seus ouvintes*".

Segundo Meyer e Schofer (2005) "*para explicar o crescimento do ensino superior, precisamos de mudar a nossa atenção para uma perspetiva global (...) as mudanças histórias na sociedade mundial entre 1930 e 1960 inauguram um novo modelo de sociedade*", o qual estava associado à criação de uma estrutura social mais escolarizada e exclusiva. Assim, antes da Segunda Guerra Mundial, o ensino superior, especialmente na Europa, era geralmente destinado a uma elite nacional, o que, segundo os autores, poderia resultar numa ineficiência social, já que ao restringir o acesso à educação superior, grandes segmentos da população eram privados da oportunidade de contribuir para o progresso social e económico, limitando o desenvolvimento mais amplo da sociedade.

O período pós-Segunda Guerra Mundial testemunhou profundas mudanças económicas em todo o mundo, com muitos países a transitarem para economias pós-industriais que exigiam profissionais altamente especializados (Altbach *et all, 2010).* Especialmente nos países desenvolvidos, o crescimento das indústrias de serviços e a economia do conhecimento, juntamente com as transformações sociais, contribuíram significativamente para o aumento da procura pelo ensino superior (Altbach *et all, 2010).*

Segundo Meyer (2004) a educação tem o potencial de ser um meio para a construção de uma sociedade mundial mais justa e virtuosa. Para o autor, a educação não é apenas um instrumento de transmissão de conhecimento, mas também uma ferramenta fundamental para promover valores e princípios que contribuam para o desenvolvimento de uma sociedade global mais ética e equilibrada.

A expansão do acesso ao ensino superior em massa verificou-se inicialmente nos Estados Unidos da América, onde, na década de 1960, cerca de 40% da população frequentava o ensino superior, e também na União Soviética, sendo estas duas novas superpotências que emergiram da guerra. Ambas as nações tinham razões políticas claras para promover o intercâmbio e a cooperação educacional internacional, com o objetivo de obter uma maior compreensão por parte do resto do mundo, assim como manter e expandir a sua influência (De Wit, 1995). Nesse contexto, De Wit (1995) argumenta que, à data, os objetivos da internacionalização do ensino superior estavam mais relacionados com a diplomacia do que com a cooperação académica e cultural, uma vez que as

superpotências viam a educação como uma ferramenta estratégica para reforçar o seu poder político e influência global.

1.1.2 A Internacionalização e a Transformação Digital nas IES

1.1.2.1 A Internacionalização das IES na Era da Globalização

Ao longo das últimas décadas, o sistema de ensino superior tem vindo a sofrer profundas transformações, adaptando-se de forma contínua às diferentes realidades globais. Essas mudanças têm sido impulsionadas pela globalização e pelos seus efeitos nos domínios económicos, sociais e tecnológicos.

O conceito de globalização foi introduzido, embora não da forma como é amplamente compreendido atualmente, por Wallerstein em 1974 na sua obra *The Modern World-System*, que começou por abordar o conceito de *capitalist world-economy* e como este unifica as diversas regiões num sistema global de troca e exploração, referindo ainda uma interdependência entre regiões centrais e periféricas (Cap I).

O termo tem sido amplamente debatido, tornando-se um dos conceitos mais controversos dos finais do século XX e inícios do século XXI, uma vez que cada autor apresenta a sua própria definição (Guillén, 2001)

Santos (2001:32) refere que o mundo se encontra "*perante um fenómeno multifacetado com dimensões económicas, sociais, políticas, culturais, religiosas e jurídicas interligadas de modo complexo*". O sociólogo Roland Robertson (1992) argumenta que a globalização "*se refere tanto à compressão do mundo quanto à intensificação da consciência do mundo como um todo*", por sua vez o sociólogo Martin Albrow (1997) define a globalização como a "*difusão de práticas, valores e tecnologias que influenciam a vida das pessoas em todo o mundo*".

Os autores Hirst *et all* (2015) sugerem que o conceito pode ter várias interpretações, entre elas:

i. Globalização refere-se ao crescimento da interdependência e interligação de recursos económicos e atividades, ultrapassando distâncias, espaços e

fronteiras. Os mesmos autores consideram que esta é a abordagem mais tradicional de comércio internacional, investimentos e padrões de migração.

ii. Globalização refere-se ao aumento na sensibilidade de importantes variáveis de economia, tais como, preços de bens, serviços e ativos, taxas de alteração de variáveis, assim como outputs e emprego, e fatores como preferências e tecnologias podem tornar-se cada vez mais uniformizados em territórios territorialmente distantes.

iii. Globalização refere-se ainda ao crescimento de processos sem uma localização territorial fixa. Nesta definição são integradas as tecnologias de informação (TI), que se materializam, particularmente, pela *Worl Wide Web (WWW)* e pela *Internet*, mas também englobam os telefones e rádios.

iv. Por último, os mesmos autores referem-se ao conceito da globalização como o crescimento da interdependência e integração por meio da adoção ou harmonização de normas comuns.

Com base nos vários contributos de diversos autores entende-se como a globalização, inserida num contexto mais abrangente e multidimensional, como um fenómeno de ampla complexidade, sendo possível defini-la como o processo de interdependência económica, política, cultural e tecnológica entre as várias regiões do mundo, que resulta na criação de uma rede global sem fronteiras físicas e mais homogénea relativamente a normas, políticas, aspetos económicos e educação.

No contexto específico das IES, e de acordo com Altbach e Knight (2007:291) a globalização é o conjunto de "*forças económicas, políticas e sociais que empurram o ensino superior do século XXI para um maior envolvimento internacional", uma "realidade moldada por uma economia mundial cada vez mais integrada pelas novas tecnologias de informação e comunicação, pela emergência de uma rede internacional de conhecimento, pelo papel da língua inglesa e por outras forças fora do controlo das instituições académicas*".

Sendo as Instituições de Ensino Superior parte integrante do mundo cada vez mais globalizado, surge o conceito de internacionalização, que, segundo Altbach (2004) é muitas vezes confundido com a globalização e frequentemente vista como uma resposta à globalização (Altbach & Knight,2007; Altbach et al.,2009; de Wit & Altbach,2021; de Wit & Knight,1996). O autor Peter Scott (2006:14) acrescenta ainda, que tanto a internacionalização como a globalização são fenómenos complexos com muitas vertentes e conclui que "*a distinção entre os dois conceitos, embora sugestiva, não pode ser considerada como categórica. Os dois conceitos sobrepõem-se e estão interligados de todas as maneiras*".

Nesta Dissertação, será dada especial atenção à aplicação e ao impacto da internacionalização no ensino superior em Portugal, analisando as suas principais iniciativas, desafios e oportunidades ao longo das últimas décadas.

Segundo Knight (2004) a internacionalização está a mudar o mundo do ensino superior, e a globalização está a mudar o mundo da internacionalização. Neste seguimento, Knight (2004) refere que no final da década de 1980, a internacionalização era frequentemente definida a nível institucional e em termos de um conjunto de atividades, promovendo a cooperação internacional, as relações académicas internacionais e a mobilidade de estudantes estrangeiros. A partir de meados da década de 1990, e à medida que as atividades das IES se expandem, tanto em termos quantitativos como qualitativos, no contexto internacional, foi introduzida uma abordagem processual ou organizacional por Knight (1994) para demonstrar a internacionalização como um processo de integração de uma dimensão internacional nas funções de ensino/aprendizagem, pesquisa e serviço de uma universidade ou faculdade. Esta abordagem visa integrar a dimensão internacional, intercultural ou global nas funções tradicionais da universidade – ensino, investigação e serviços –, incluindo a oferta de programas de ensino superior adaptados a este contexto (Knight, 2004). Em 1989 foi fundada a Associação Europeia para a Educação Internacional (EAIE) que afirmou que a internacionalização é toda a gama de processos pelos quais o ensino superior se torna menos nacional e mais internacionalmente orientado.

Mais recentemente, Knight (2004) refere que Soderqvist (2002) introduziu outra definição que se foca no processo de mudança educacional e numa visão holística da gestão a nível institucional. Sendo assim, a internacionalização de uma instituição de ensino superior, definida como um processo de transformação de uma instituição de ensino superior nacional para uma instituição de ensino superior internacional, levando à inclusão de uma dimensão internacional em todos os aspetos da sua gestão holística, com o objetivo de melhorar a qualidade do ensino e da aprendizagem e alcançar as competências desejadas. (Soderqvist, 2002)

Segundo os autores Altbach e Knight (2007) entende-se a internacionalização como o conjunto de políticas e práticas desenvolvidas por sistemas académicos e instituições – e até mesmo indivíduos – para lidar com o ambiente académico global.

Como resultado da globalização e internacionalização das IES, os autores Altbach e Knight (2007) referem algumas alterações nas IES como a integração da pesquisa, o uso do inglês como língua franca para a comunicação científica, o crescente mercado internacional de trabalho para académicos e cientistas, o crescimento das empresas de comunicação e das publicações multinacionais e tecnológicas e a utilização da tecnologia de informação. A globalização impulsionou a mobilidade de estudantes em grande escala através de uma maior consciência da informação, oportunidades e maior propensão para viajar, promovendo um maior intercâmbio entre países e culturas. Nem a educação nem o conhecimento são restringidos pelas fronteiras dos estados-nação e/ou culturas regionais (Ge, 2022). A mobilidade de estudantes e académicos torna-se assim num fator importante no ensino superior em todo o mundo. (Altbach et al. 2009).

Considerando que a internacionalização das Instituições de Ensino Superior se configura como um conjunto práticas e políticas aplicadas por estas em resposta aos desafios da globalização, é fundamental aprofundar a compreensão dos principais fatores e incentivos que impulsionam o processo de internacionalização académica.

1.1.2.2 Estímulos à Internacionalização do Ensino Superior

A internacionalização do Ensino Superior é impulsionada por um conjunto de estímulos, que podem variar conforme as particularidades de cada instituição e o contexto

global em que se inserem. Inicialmente estes estímulos à internacionalização eram classificados em duas grandes categorias: razões políticas e económicas e razões culturais e educacionais (Knight e De Wit, 1995). No entanto, em estudos posteriores, estes estímulos encontram-se agrupados em quatro categorias: socioculturais, políticas, académicas e económicas (Knight & de Wit, 1999). Embora essas categorias gerais continuem a ser uma estrutura útil para analisar as motivações da internacionalização, é fundamental destacar as mudanças significativas na natureza e na prioridade de cada uma delas (Knight, 2004).

De acordo com a autora Knight (2008), e tal como se apresenta na Tabela 1, são categorizados quatro racionais, que, por sua vez se dividem em existentes e emergentes tanto o nível nacional como o institucional.

Tabela 1 - Estímulos à Internacionalização das Instituições de Ensino Superior

Rationales	***Existing Rationales***	***Of Emerging Importance***
Social/cultural	National cultural identity Intercultural understanding Citizenship development Social and community development	**National level** Human resources development Strategic alliances Income generation/commercial trade Nation building/institution building Social/cultural development and mutual understanding
Political	Foreign policy National security Technical assistance Peace and mutual understanding National identity Regional identity	**Institutional Level** International branding and profile Quality enhancement/international standards Income generation Student and staff development Strategic alliances Knowledge production
Economic	Economic growth and competitiveness Labor market Financial incentives	
Academic	Extension of academic horizon Institution building Profile and status Enhancement of quality International academic standards International dimension to research and teaching	

Fonte: Knight, 2008:25, conforme originalmente apresentado em Knight, 2005

No que respeita aos incentivos socioculturais à internacionalização da educação, destacam-se os estímulos à promoção e difusão da identidade e dos valores culturais de

um país (De Wit & Knight, 1995). De acordo com Mayor (1989), "*a universidade é uma instituição na qual a produção, a transmissão e a reprodução da cultura se encontram harmoniosamente e na qual estas últimas são complementadas pela reflexão sobre o papel e a função da cultura na vida das nações e dos indivíduos*".

Além deste fator, segundo De Wit e Knight (1995), a internacionalização tem desempenhado um papel fundamental na promoção do conhecimento e da compreensão intercultural, bem como no desenvolvimento da cidadania global, preparando indivíduos mais conscientes das dinâmicas internacionais. Por fim, a internacionalização das IES tem igualmente contribuído para o fortalecimento das comunidades locais, através do intercâmbio internacional de estudantes e docentes.

No âmbito dos incentivos políticos à internacionalização da educação, destaca-se o reforço das relações políticas e diplomáticas de um país. Além deste fator, salientam-se ainda outros estímulos, nomeadamente o fortalecimento da posição geopolítica e da segurança nacional, o aumento da capacidade de fornecer apoio educativo e técnico a países em desenvolvimento, a promoção da paz através da intensificação da colaboração internacional e intercultural, bem como o reforço da identidade nacional e regional através de acordos e parcerias internacionais.

Quanto aos incentivos económicos, destacam-se o crescimento da economia e o investimento futuro, dado que se prevê que a internacionalização da educação contribua positivamente para o desenvolvimento tecnológico e, consequentemente, para o aumento da competitividade económica de um país.

Adicionalmente, verifica-se um aumento da concorrência no mercado de trabalho, uma vez que os diplomados passam a competir não apenas a nível nacional, mas também com candidatos de outros países num ambiente globalizado.

Por último, importa salientar o impacto financeiro da internacionalização do ensino superior, que pode gerar receitas significativas. O aumento do número de estudantes estrangeiros, sujeitos a propinas mais elevadas, representa o aumento do retorno financeiro tanto para as instituições de ensino como para o próprio Estado, ajudando a mitigar os custos públicos com o setor. Além disso, os estudantes

internacionais de pós-graduação prestam frequentemente serviços de investigação e ensino por uma remuneração reduzida, enquanto o seu consumo e despesas no país de acolhimento geram um impacto económico significativo (Altbach & Knight, 2011).

No que respeita aos incentivos educacionais, destacam-se a expansão da investigação e do ensino, integrando a perspetiva de uma sociedade global, bem como a ampliação do horizonte académico, contribuindo para a melhoria da qualidade do ensino e da investigação (De Wit, 1995). Estes objetivos são alcançados, entre outros meios, através do recrutamento internacional de estudantes e docentes, promovendo uma maior diversidade e intercâmbio de conhecimento. Além disso, a internacionalização confere uma dimensão global à investigação e ao ensino das IES, estimulando o pensamento crítico de estudantes e da sociedade em geral (De Wit, 1995).

Adicionalmente, salienta-se o fortalecimento da posição e da infraestrutura das instituições, permitindo a adoção de decisões e iniciativas que, de outra forma, não seriam viáveis com base apenas em recursos e conhecimentos locais. A colaboração internacional possibilita a ampliação das fronteiras do conhecimento, abrindo portas para novas oportunidades e desafios que impulsionam o seu desenvolvimento.

Por fim, destaca-se ainda o reforço da imagem e reputação de uma instituição no contexto internacional, a melhoria da qualidade académica ao nível internacional e a adoção de normas académicas globais, promovendo a uniformização de práticas de ensino e investigação, alinhadas com padrões internacionais de excelência.

Para a autora Knight (2004), embora as instituições de ensino superior tenham sempre sido competitivas em alcançar elevados padrões académicos, reconhece que existe o desenvolvimento de uma estratégia ativa e comercial de forma a posicionar a instituição num mercado internacional e cada vez mais competitivo, pelo que é possível identificar uma quinta categoria, o *branding* e reputação da IES, que prevê a procura de prestígio, reconhecimento e reputação internacional para a instituição.

Knight (2004) propõe ainda uma nova classificação das motivações à internacionalização do ensino, adotando uma perspetiva distinta, na qual distingue entre motivações de carácter nacional e institucional. De acordo com a autora, nos países onde

a internacionalização não é uma prioridade a nível nacional – o que ainda é comum em várias regiões do mundo – os racionais institucionais ganham maior relevância e podem variar significativamente entre instituições, aliado ao facto de que diversos fatores influenciam os racionais institucionais, incluindo a missão da instituição, o perfil dos estudantes e docentes, a localização geográfica, as fontes de financiamento, o nível de recursos disponíveis e a orientação para interesses locais, nacionais ou internacionais

A crescente internacionalização do Ensino Superior, motivada por fatores socioculturais, políticos, económicos e educacionais, tem desempenhado um papel fundamental na forma como as IES se posicionam no cenário global. Esta abertura ao mundo, além de ampliar horizontes e oportunidades, tem vindo a transformar profundamente o modo como as instituições funcionam. A transformação digital tornou-se, assim, uma aliada incontornável deste processo, proporcionando, não apenas inovação e eficiência, mas também novos desafios, especialmente no que diz respeito à segurança da informação.

1.2 A Segurança da informação e cibersegurança

1.2.1 A transformação digital nas IES

A par da globalização e internacionalização emergiram também outros desafios, designadamente a *Internet* e a *World Wide Web* que vieram revolucionar o mundo, impactando a forma de comunicar, o acesso à informação e a transformação dos negócios.

A *Internet* surgiu, no final da década de 60, e, ainda designada por ARPANET, esta era apenas destinada ao Departamento de Defesa (DoD) e tinha como principal objetivo responder às necessidades de troca de informações entre militares. A designação de *"Internet"*, como é conhecida atualmente, surge no ano de 1983, através da crescente interligação entre várias universidades nos EUA e mais tarde com organismos europeus (Antunes & Rodrigues, 2018). A década de 80 foi marcada pela sua expansão, com o envolvimento de cada vez mais organismos, desde operadores de telecomunicações, universidades a governos e instituições públicas. No entanto, em Portugal o domínio ".pt" só foi introduzido em 1991. Na década de 90, a *Internet* atingiu um elevado nível de globalização através da interligação de redes de vários países e continentes. Foi também

nesse período que surgiu um dos principais serviços de *internet*: *o World Wide Web* (Antunes & Rodrigues, 2018).

Com a globalização, a capacidade de propagação da informação tornou-se cada vez maior e, como resultado, a sociedade criou uma dependência da *Internet*, passando a viver com o sentimento de satisfação imediata e com grandes expectativas através do serviço *just-in-time*. - Desde o seu aparecimento até aos dias de hoje, a *Internet* evoluiu consideravelmente, aumentando a importância na vida quotidiana de pessoas, empresas, estados e instituições, constituindo uma vantagem o acesso imediato a informação e a conectividade global. Para além destes aspetos, o aparecimento da *Internet* veio possibilitar o desenvolvimento de novos negócios e a inovação tecnológica de muitos outros.

O conceito da transformação digital surge como resposta organizada e estratégica ao crescente uso da internet na sociedade. Enquanto a disseminação da *Internet* proporcionou uma expansão rápida e muitas vezes desordenada, a transformação digital visa corrigir e orientar o uso dessas tecnologias, promovendo a adaptabilidade, segurança e eficiência nas organizações e processos.

O conceito de "transformação digital" tem sido largamente debatido ao longo dos últimos anos. Schwab (2016) introduziu o conceito de uma Quarta Revolução Industrial, que segundo este autor se baseia nas outras três revoluções, mas que utiliza as novas tecnologias com máxima força, pelo que, tanto o desenvolvimento e a difusão das inovações são muito mais rápidos do que até então.

Revolution		Year	Information
	1	1784	Steam, water, mechanical production equipment
	2	1870	Division of labour, electricity, mass production
	3	1969	Electronics, IT, automated production
	4	?	Cyber-physical systems

Figura 1 - Revoluções passadas e o futuro

Fonte: WeForum (2025) https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

De acordo com o mesmo autor, se por um lado, "a Primeira Revolução Industrial utilizou a energia da água e do vapor para mecanizar a produção, a Segunda usou a energia elétrica para criar a produção em massa e a Terceira utilizou a eletrónica e a TI para automatizar a produção". Por outro lado, "a Quarta Revolução Industrial está a construir-se sobre a terceira", ou seja, esta é caraterizada por uma fusão de tecnologias que tornam invisíveis as fronteiras físicas, digitais e biológicas". No entanto, Schwab (2016) refere três razões pelas quais as transformações não representavam apenas um prolongamento da Terceira Revolução Industrial, mas antes o aparecimento de uma Quarta: a velocidade dos avanços, que quando comparada com as revoluções anteriores, esta última evoluiu de uma forma exponencial e não linear; o âmbito e impacto nos sistemas, estas mudanças anunciam a transformação de sistemas inteiros de produção, gestão e governação.

A *The Enterprises Project*[1] define o processo de transformação digital como *"a integração da tecnologia digital em todas as áreas de um negócio, mudando, fundamentalmente, a forma como opera e entrega valor aos clientes (...) e representa*

[1] Comunidade e publicação online, parceira da Harvard Business Review, que ajuda CEO e líderes de Tecnologias de Informação a resolver problemas e gerar valor comercial. Consultado a 21 de janeiro de 2025 em https://enterprisersproject.com/about-this-project. Citação consultada em https://enterprisersproject.com/what-is-digital-transformation.

uma mudança cultural que exige que as organizações desafiem continuamente o status quo, experimentem e se sintam confortáveis com o fracasso".

Através de uma revisão de literatura elaborada pelos autores Ismael *et all* (2018) é possível analisar as várias perspetivas de transformação digital debatidas na Literatura ao longo dos últimos anos, tal como se apresenta na Figura 2.

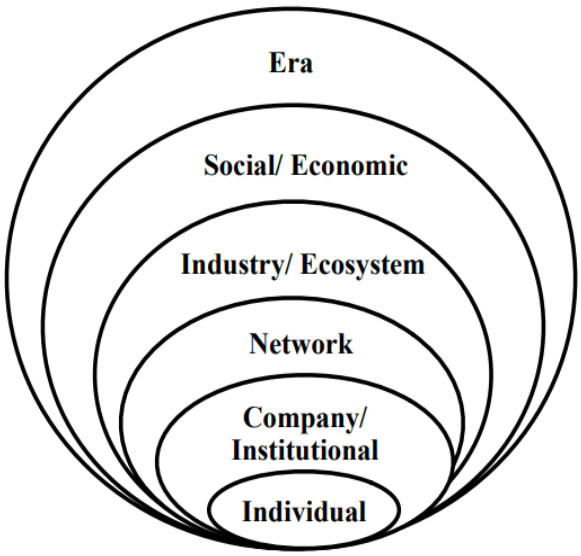

Figura 2 - Perspetivas sobre a transformação digital na Literatura

Fonte: Ismail, M. H., Khater, M., & Zaki, M. (2018). *Digital Business Transformation and Strategy: What Do We Know So Far?* Pp. 2-3

A síntese elaborada por estes autores, visa várias perspetivas sobre o conceito transformação digital. Se por um lado, alguns autores reconhecem a TD como uma nova era digital devido à sua natureza omnipresente e proliferação (Anderson & Lanzolla, 2010), outros autores acreditam que estava a emergir uma nova economia global (Schwab, 2016). A perspetiva industrial evidencia como a TD revolucionou o funcionamento das indústrias. No que respeita ao *network*, as novas tecnologias acentuaram mudanças nos negócios tradicionais, passando a abranger, por exemplo, mais clientes digitais e criando um ecossistema digital (Gray et al., 2013). A TD também pode ser entendida do ponto de vista dos negócios, uma vez que era visto como um fator estratégico essencial, com muitas organizações a transformares os seus departamentos de TI em catalisadores de inovação e crescimento (Hess et al., 2016). Do ponto de vista do

individuo, "as tecnologias digitais criam novas formas de experimentação e expressão pessoa, permitindo construir múltiplas versões de um individuo online" (Turkle, 2011) e de acordo com Belk (2014), "a partilha digital é agora uma parte fundamental da nossa vida, transformando o modo como experimentamos a propriedade e, em última análise, quem somos, já que possuímos cada vez menos, mas partilhamos mais".

Esta dissertação irá dar mais enfase à perspetiva da TD nas organizações, com particular atenção às Instituições de Ensino Superior.

No contexto mais amplo de uma organização, segundo Seres (2018), a transformação digital possui seis dimensões:

1. Estratégia digital organizacional e abordagem para aplicação da inovação definidas e aceites
2. Processos colaborativos ágeis, adaptáveis ajustáveis considerando modelos de negócio e desafios atuais;
3. Automatização dos processos;
4. Análise detalhada do processo de tomada de decisão dos clientes;
5. Tecnologias a apoiar os processos empresariais da organização;
6. Dados no centro da tomada de decisão, com base em informações relevantes, alinhadas com objetivos e estratégia da organização.

A maioria dos autores reconhece a transformação digital como uma das formas mais complexos de mudança organizacional, uma vez que envolve não apenas a integração de novas tecnologias, mas também a reestruturação de processos e estratégias e a transformação cultural em todos os níveis da organização (Westerman, Bonnet & McAfee, 2014; Vial, 2019; Kane *et al.*, 2015).

1.2.2 Definição de segurança da informação

A relação entre os conceitos de internacionalização, transformação digital e segurança da informação nas IES é significativa, já que a expansão das atividades

internacionais está intrinsecamente ligada ao aumento do volume de informação e consequentemente à necessidade de proteger a mesma.

Altbach, et al (2009:7) no relatório à UNESCO Nota da Conferência Mundial sobre Ensino Superior referem que as tecnologias de informação e comunicação criaram um meio universal de contacto instantâneo e comunicação científica mais simplificada.

Com a expansão global das IES, a segurança da informação desempenha um papel fundamental na garantia da proteção, integridade e confidencialidade dos dados e sistemas, e ao mesmo tempo enfrenta desafios associados à diversidade cultural, conformidade regulatória e complexidade tecnológica. Esta relação destaca a importância de estratégias de segurança da informação adaptadas a um contexto de globalização, uma vez que a necessidade de partilha de informação entre Instituições e parceiros exige protocolos rigorosos de segurança, bem como o uso de tecnologias avançadas de forma a prevenir acessos não autorizados.

Segundo Stallings (2020) a proteção da informação está interligada com o conceito de segurança informática e define este último conceito como "*a proteção conferida a um sistema de informação automatizado a fim de atingir os objetivos aplicáveis de preservar a integridade, a disponibilidade e confidencialidade dos recursos do sistema de informação (inclui hardware, software, informações/dados e telecomunicações)*". O NIST define a segurança da informação como "a proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer confidencialidade, integridade e disponibilidade"

De acordo com Stallings (2020) e em linha com a norma FIPS 199 do NIST *(Standards for Security Categorization of Federal Information and Information Systems*), os três objetivos fundamentais de segurança da informação são:

a) A *confidencialidade* abrange dois conceitos relacionados entre si: (i) confidencialidade dos dados, em que é assegurado que a informação privada ou confidencial não é disponibilizada ou divulgada a indivíduos não autorizados; (ii) privacidade em que é assegurado que os indivíduos controlam

a informação que lhes diz respeito, e podem escolher que informação pode ser recolhida ou armazenada e por quem, e a quem essa informação pode ser divulgada.

b) A *integridade* abrange dois conceitos relacionados entre si: (i) integridade dos dados, em que é garantido que as informações sejam alteradas apenas com autorização para tal e (ii) integridade dos sistemas em que é assegurado que um sistema desempenha a função pretendida de forma irrepreensível, livre de qualquer manipulação não autorizada no sistema.

c) A *disponibilidade* em que é assegurado que os sistemas funcionam prontamente e que o serviço não é negado a utilizadores autorizados.

De acordo com KPMG LLP. (2023), um sistema de gestão de segurança de informação é uma estrutura de políticas e procedimentos para gestão sistemática de dados sensíveis de uma organização. Este inclui as pessoas, processos e tecnologias responsáveis por proteger contra o acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição da informação. Desta forma, a segurança da informação é sustentada por três pilares fundamentais – Pessoas, Tecnologia e Processos. Para que a segurança da informação seja eficazmente implementada, é essencial que esses pilares estejam bem definidos e integrados dentro da organização.

A primeira linha de proteção da informação são as **Pessoas,** é necessário garantir que os colaboradores estão conscientes dos riscos e que são responsáveis por proteger a informação da organização.

Uma organização deve determinar a competência necessária das pessoas que realizam um determinado trabalho que pode afetar a segurança da informação; assegurar que essas pessoas são competentes e têm o conhecimento, a formação e a experiência necessária para a função; se for caso disso tomar medidas para a aquisição das competências necessárias e avaliar a eficácia das ações tomadas; arquivar a informação como prova da competência (ISO/IEC 27001, 2022).

Assim, a ISO/IEC 27001 estabelece que as pessoas que trabalham numa determinada organização devem ter conhecimento da política de segurança da

informação, da sua contribuição para a eficácia do sistema de gestão da segurança da informação e das implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação, sendo que, para tal, a organização deve determinar a necessidade de comunicações internas e externas (Secção 7.2 a 7.4 da ISO/IEC 27001, 2022).

A segunda linha de proteção é a **Tecnologia**, onde o objetivo é criar barreiras lógicas que impeçam que as ameaças afetem a informação (antivírus, firewall, proxy, VPN, …). A estratégia recomendada pela NSA, no seu artigo "Defense in Depth" refere que é recomendável para as organizações adotarem vários princípios de garantia da informação, incluindo:

- Defesa em múltiplos pontos – implementar mecanismos de proteção da informação em diferentes locais para resistir a todos os tipos de ataques, internos ou externos. As áreas de defesa devem incluir: a defesa das redes e infraestruturas, utilizando criptografia e medidas de segurança para proteger contra a monitorização passiva; a defesa das fronteiras do sistema, através da implementação de *firewalls* e sistemas de deteção de intrusão; e a defesa do ambiente computacional, aplicando controlos de acesso em todos os dispositivos, de modo a garantir que apenas utilizadores ou dispositivos autorizados estão autorizados a aceder, prevenindo, assim, ataques internos, invasões físicas ou manipulações não autorizadas.
- Defesa em camadas – implementação de múltiplos mecanismos de defesa entre o atacante e o seu alvo. Um exemplo de defesa em camadas é a implementação de *firewalls* em diferentes níveis da rede, cada um com funções específicas e deteção de intrusão integrada.
- Especificação da robustez da segurança - A força e garantia de cada componente de segurança devem ser proporcionais ao valor do bem ou sistema protegido e à ameaça. Por exemplo, pode ser mais eficaz e operacionalmente adequado implementar mecanismos mais robustos nas fronteiras da rede do que nos dispositivos finais dos utilizadores.

- Gestão robusta de infraestruturas públicas chave - Criar infraestruturas robustas que suportem as tecnologias de segurança da informação e sejam altamente resistentes a ataques, pois são alvos estratégicos para os adversários.
- Deteção e resposta a intrusões - Desenvolvimento de infraestruturas que permitam detetar, analisar, correlacionar e reagir a ataques.

No entanto, de forma a garantir que as tecnologias sejam adquiridas e implementadas nas organizações corretamente, esta deve estabelecer políticas e processos eficazes para aquisição da mesma (NSA)

A terceira linha de proteção são os **Processos**, sendo o seu objetivo desenvolver um modelo integrado de segurança que contemple os aspetos estratégicos e de gestão de segurança da informação (políticas de segurança, procedimentos, ações internas, etc.).

De acordo com a organização NSA, é necessário:

a) Manter políticas de segurança do sistema acessíveis e atualizadas
b) Certificação de alterações na base da Tecnologia da Informação
c) Gestão dos mecanismos de segurança tecnológica, através da instalação *patches* de segurança, da atualização de antivírus e controlo de acessos.
d) Oferecer serviços de gestão e proteção da infraestrutura.
e) Realizar avaliações de segurança no sistema.
f) Monitorizar e reagir a ameaças atuais.
g) Detetar, alertar e responder a ataques.
h) Realizar processos de recuperação e reconstituição após incidentes.

Em suma, uma organização deve determinar as questões externas e internas mais relevantes e que afetam a sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação - SGSI (ISO 27001, 2022, Secção 4.1). Ao planear o SGSI uma organização tem de considerar planear, implementar e controlar os processos necessários para cumprir os requisitos.

1.2.3 Conceitos Fundamentais de Cibersegurança

1.2.3.1 A Cibersegurança

A crescente necessidade de proteger a informação e de promover o desenvolvimento sustentável das redes através da sensibilização para a segurança tem gerado intensos debates sobre a proteção e salvaguarda da informação, uma vez que o modelo de comunicação da Internet é vulnerável a diferentes tipos de exploração, geralmente realizadas por indivíduos mal-intencionados, cujo objetivo é causar danos aos alvos ou obter, de forma indevida, acesso a informação privilegiada (Antunes & Rodrigues, 2018).

De acordo com Christos K. Dimitriadis a importância cibersegurança tem vindo a crescer rapidamente, impulsionada pela evolução constante das ameaças e pela crescente dependência de tecnologias de informação cada vez mais complexas, interconectadas e globalizadas.

Assim, é fundamental estabelecer uma distinção entre dois conceitos frequentemente interligados e, por vezes, confundidos: segurança da informação e cibersegurança.

Segundo o Centro Nacional de Cibersegurança (CNCS), a segurança da informação é a "*proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças*". Por sua vez, o mesmo organismo, em consonância com a Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, descreve a cibersegurança como um "*conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem*".

O relatório The Joint Task Force on Cybersecurity Education (2017:18) define cibersegurança como:

> *A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.*

Com base na análise etimológica, é possível distinguir dois conceitos fundamentais: "ciberespaço" e "segurança". Conforme definido no Dicionário de Língua Portuguesa Priberam (2024), o prefixo "ciber" exprime a noção de Internet ou de comunicação entre redes de computadores. Por sua vez, o conceito de "ciberespaço", diretamente associado ao prefixo supracitado, é definido pelo mesmo organismo como "espaço ou conjunto das comunidades de redes de comunicação entre computadores, nomeadamente a *Internet"*. No que diz respeito ao termo "segurança", este dicionário carateriza-o como o "conjunto das ações e dos recursos utilizados para proteger algo ou alguém" tendo como principal objetivo "diminuir riscos e perigos".

De acordo com o Public Safety Canada (2010), o "ciberespaço" é o mundo eletrónico criado por redes interrelacionadas de tecnologia de informação e as suas respetivas informações, correspondendo a um ecossistema dinâmico e em constante evolução, caraterizado pelas inovações contantes (Deibert & Rohozinski, 2010).

Segundo Kemmerer (2003), a cibersegurança consiste, em grande medida, na aplicação de métodos defensivos destinados a detetar e prevenir intrusões. Por outras palavras, envolve a proteção de redes e computadores, assim como das informações neles armazenadas (Lewis, 2006). Este conceito também inclui a mitigação do risco de ataques informáticos a *software*, computadores e redes, podendo envolver o uso de ferramentas específicas para detetar intrusos num sistema, programas capazes de bloquear vírus ou acessos mal-intencionados, além de soluções que permitem comunicações criptografadas (Amoroso, 2006).

De forma geral, a cibersegurança pode ser entendida como a prática de assegurar a existência e a continuidade de uma organização, sociedade ou país, garantindo a proteção das informações no ciberespaço (Canongia & Mandarino, 2014).

Um outro contributo relevante é o de Antunes e Rodrigues (2018) que definem a cibersegurança como o conjunto de tecnologias, processos e práticas desenvolvidos para proteger redes, computadores e outros dispositivos eletrónicos, programas e dados contra potenciais ataques ou ameaças. Neste sentido, os mesmos autores, destacam que a cibersegurança envolve ações de monitorização, prevenção e neutralização de ameaças que possam comprometer a liberdade dos cidadãos e das empresas, assim como o bem-estar socioeconómico das nações.

Segundo o Committee on National Security Systems (2015), a cibersegurança é definida como a prevenção de danos, a proteção dos computadores, de sistemas e serviços de comunicações eletrónicas, incluindo as informações neles contidas, com o objetivo de garantir a sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio.

Desta forma, a cibersegurança pode ser definida como o conjunto de práticas, políticas e tecnologias utilizadas para proteger sistemas informáticos, dados e informações relevantes, que permitem mitigar os riscos e responder eficazmente a incidentes de segurança. Esta visa igualmente garantir a integridade, confidencialidade e disponibilidade da informação, assegurando que as infraestruturas permaneçam seguras, tanto em ambientes pessoais quanto organizacionais.

No âmbito da cibersegurança, é importante compreender a existência de alguns conceitos interligados, mas distintos: ciberameaça, ciberataque e cibercrime, os quais representam diferentes aspetos dos riscos e da segurança nos sistemas digitais.

1.2.3.2 Cibermeaça, Ciberataque e Cibercrime

Uma ciberameaça é uma causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque (CNCS, 2024). Um ciberataque é qualquer tipo de atividade maliciosa que tenta recolher, perturbar, negar, degradar ou destruir recursos de um sistema de informação ou a informação em si (CNCS, 2024).

Os ciberataques podem assumir variadas formas, desde o acesso remoto indevido através da instalação de programas maliciosos (*malware*), à usurpação de credenciais de

acesso (Antunes e Rodrigues, 2018). Segundo os mesmos autores, os ciberataques podem ser classificados em dois grandes grupos:

i. os que exploram vulnerabilidades já conhecidas e para as quais já foi disponibilizada uma medida corretiva;
ii. os *zero days attacks*, que ocorrem pela primeira vez e não se sabe muito sobre a sua ação e os danos que poderão causar.

Ao abordar a distinção entre "ciberameaça" e "ciberataque" no âmbito da cibersegurança, é fundamental compreender que as ciberameaças representam potenciais riscos que podem comprometer a integridade dos sistemas, enquanto os ciberataques correspondem a ações concretas e maliciosas que visam explorar vulnerabilidades de sistemas para atingir objetivos específicos.

Neste contexto, torna-se crucial analisar os tipos de ataques mais frequentes, à data de hoje, com base no relatório da CNCS. O relatório permite identificar as principais ameaças enfrentadas pelas organizações em 2023, bem como algumas recomendações a levar em conta, tal como se evidencia na Tabela 2.

Tabela 2 - Definição e recomendações de segurança das principais ameaças

Tipo de Ataque	Definição	Recomendações de Segurança
Phishing/Smishing/ Vishing	Mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de emails ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas [*pharming*], façam transferências de dinheiro, etc. *Fonte:* ENISA, Threat Landscape 2018	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores; realizar simulações de *phishing* e aplicar as melhores práticas e standards de segurança ao nível da configuração do email organizacional.
Tipo de Ataque	**Definição**	**Recomendações de Segurança**

Ransomware	Tipo de *malware* que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas." *Fonte:* ENISA, Threat Landscape 2018	Formação dos colaboradores relativamente às recomendações relativas ao *phishing* e email; salvaguardar cópias de segurança numa localização secundária e desconectada da rede; manter os sistemas, as aplicações e o antivírus atualizados; ter as redes da organização segmentadas; evitar navegar em websites sem garantias de segurança; não utilizar dispositivos USB de origem desconhecida.
Engenharia Social	Ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança. *Fonte:* NIST, Digital Identity Guidelines	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores; realizar simulações de ataques de engenharia social.
Burla *Online*	Uma das formas de cibercrime mais frequentes, frequentemente associada ao comércio eletrónico e às transações monetárias e pode envolver técnicas como *phishing*, smishing e outras formas de manipulação do fator humano. *Fonte: CNCS*	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores; garantir que os colaboradores confirmam o destino e a necessidade das transferências bancárias solicitadas; utilizar carteiras virtuais ou cartões temporários nos pagamentos online a fornecedores; verificar a veracidade dos websites de fornecedores e privilegiar aqueles que utilizam HTTPS.

Tipo de Ataque	**Definição**	**Recomendações de Segurança**

Comprometimento de Contas	Comprometimento de um sistema em que o atacante ganhou privilégios de administração ou usando uma conta (utilizador/serviço) não privilegiada. Fonte: Taxonomia Comum da Rede Nacional de CSIRT[2].	Aplicar de forma contínua as políticas de segurança definidas quanto às palavras-passe em particular, promovendo o cumprimento de requisitos mínimos de dimensão e complexidade; monitorizar e bloquear ataques de força-bruta; registar os eventos; aplicar o múltiplo fator de autenticação.

Fonte: CNCS e Taxonomia Comum da Rede Nacional CSIRT

No que diz respeito às recomendações é importante manter estas ações monitorizadas por políticas de segurança definidas.

Com o crescimento exponencial do ciberespaço e o aumento das ameaças e ataques que podem perpetrados, surgiu, ainda na década 90, o conceito de cibercrime como uma forma de definir as novas formas de delitos que emergiram em ambiente digital.

O conceito, que inicialmente se restringia aos crimes cometidos por meio do uso de tecnologias eletrónicas ou através da Internet, evoluiu ao longo dos anos, passando a englobar uma categoria mais ampla de crimes praticados nas redes de comunicação em geral, incluído a Internet (Antunes e Rodrigues, 2018). Estes crimes incluem os crimes informáticos, praticados contra sistemas informáticos, dados e informações alojadas nos sistemas de informação.

Atualmente, os *hackers* tendem a encontrar padrões cada vez mais sofisticados para aceder a computadores e redes, tornando o combate a esses ataques um desafio não só para as organizações, mas também para a sociedade em geral. Segundo Ishaq (2016), embora o impacto a curto prazo possa ser devastador, as implicações a longo prazo podem ser igualmente bastante graves. Entre elas, destacam-se o pagamento de resgate por extorsão, a recuperação de dados, a localização e correção das vulnerabilidades

[2] A Rede Nacional de CSIRT é uma rede de organizações que cooperam para melhorar a cibersegurança, partilhar informações sobre ameaças e coordenar respostas a incidentes de segurança, no contexto de um país ou região. A Taxonomia Comum da Rede Nacional de CSIRT é uma classificação padronizada usada para categorizar e descrever diferentes tipos de incidentes de cibersegurança, facilitando a comunicação e colaboração entre os membros da rede e outras entidades relacionadas com a cibersegurança. https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

exploradas, a perda de clientes, lucros ou até empregos e, em casos extremos, a continuidade da própria empresa pode estar em causa.

No contexto específico das empresas, um ataque informático pode levar as empresas a considerar que a melhor forma de evitar tais incidentes seria realizar todas as atividades de forma manual, o que, no entanto, se tornaria insustentável, especialmente considerando o contexto de globalização atual. Assim, de forma a mitigar e diminuir o risco e, consequentemente, aumentar a cibersegurança de uma organização, é essencial proteger o perímetro de redes com *firewalls* e ter um sistema de prevenção de intrusão. Além disso, é fundamental realizar análises periódicas às vulnerabilidades, procedendo às respetivas correções (Ishaq, 2016).

1.2.4 Organismos de Cibersegurança nacionais e internacionais

Atualmente, vivemos num mundo onde os sistemas informáticos das instituições operam em rede e estão interligados. A possibilidade destes sistemas serem atacados ou, até, desligados levanta problemas significativos tanto para o bem-estar das populações quanto para a segurança global. Assim, a implementação de estratégias de ciberdefesa deve ocorrer tanto a nível nacional como internacional, garantindo uma resposta eficaz às crescentes ameaças no espaço digital.

No contexto nacional, destaca-se o Centro Nacional de Cibersegurança (CNCS), entidade responsável pela coordenação da estratégia de cibersegurança em Portugal. Criado para garantir a proteção dos sistemas e infraestruturas críticas do país, o CNCS atua de forma preventiva e reativa, promovendo a consciencialização sobre riscos e coordenando respostas a incidentes em todo o território nacional.

A nível internacional, a União Europeia tem sido proativa na promoção de uma abordagem coordenada para a cibersegurança. Em 1999, foi desenvolvida pela Comissão Europeia a iniciativa *eEurope*, que desempenhou um papel fundamental ao estabelecer bases para uma sociedade digital mais segura e confiável, tanto para cidadãos como para empresas. Esta iniciativa abordou a necessidade de adotar medidas regulatórias para

mitigar riscos, tais como o combate a conteúdos prejudiciais ou ilícitos na web e a promoção de práticas seguras de utilização da Internet.

Em 2004, foi criada a ENISA (Agência da União Europeia para a Cibersegurança), pelo Regulamento (CE) n.º 460/2004, pelo Parlamento Europeu e pelo Conselho da União Europeia, que fornece apoio técnico e estratégico à implementação de políticas de segurança digital na União Europeia. O seu principal objetivo é reforçar a cibersegurança na União Europeia, apoiando os Estados-Membros na prevenção e resposta a incidentes de cibersegurança, promovendo boas práticas e facilitando a cooperação entre os diferentes organismos nacionais e internacionais.

O CNCS, enquanto Autoridade Nacional de Certificação da Cibersegurança, representa Portugal no Grupo Europeu de Certificação da Cibersegurança, fórum estratégico da certificação da cibersegurança na UE que tem, entre outras, as missões de aconselhar e apoiar a Comissão no domínio da certificação da cibersegurança e da implementação e aplicação coerentes do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019, em particular no que diz respeito ao programa de trabalho evolutivo da União, às questões de política de certificação de cibersegurança, à coordenação das abordagens políticas e à elaboração de esquemas europeus de certificação da cibersegurança; apoiar, aconselhar e cooperar com a ENISA em relação à elaboração de esquemas candidatos; elaborar e adotar pareceres sobre os esquemas candidatos preparados pela ENISA; solicitar à ENISA a elaboração de esquemas candidatos.

No plano operacional, o CERT (Computer Emergency Response Team) é um dos principais intervenientes a nível internacional na prevenção e resposta a incidentes. Em vários países da UE, existem os CERT's nacionais que desempenham um papel essencial na identificação de vulnerabilidades, na partilha de informações sobre ameaças e na coordenação de respostas rápidas a ataques informáticos. Estes centros operam num modelo de cooperação global, mantendo uma comunicação estreita entre si e com organismos internacionais.

1.2.5 Evolução Histórica da Cibersegurança nas IES

A cibersegurança tem vindo a ganhar uma enorme relevância nas últimas décadas, devido ao aumento dos números associados ao fenómeno do cibercrime nas organizações. Segundo o CNCS (2024:22), no seu relatório "*80% das empresas consideram que a cibersegurança é uma prioridade bastante alta ou muito elevada*", referindo ainda que "*a percentagem de organismos da Administração Pública com uma estratégia para a segurança da informação definida aumentou de 59% em 2022 para 67% em 2023*" (CNCS 2024:24).

O setor da educação tem se tornado um alvo cada vez mais atraente para este tipo de crimes, impulsionado pela quantidade e sensibilidade dos dados geridos nas instituições. De acordo com a Microsoft (2024), *"o setor da educação apresenta-se como um alvo particularmente interessante para cibercriminosos, uma vez que as instituições de ensino são responsáveis por gerar dados que podem incluir registos de saúde, informação financeira e outros dados confidenciais. Além disso, nas suas plataformas podem alojar sistemas de processamento de pagamentos, redes que funcionam como fornecedores de serviços de internet e outras soluções digitais. (...)*, referindo ainda que no que respeita às IES estas "*são os principais alvos de malware, phishing e vulnerabilidades de IoT*".

Esta vulnerabilidade é algo que vem sendo observado desde os primeiros estudos sobre a cibersegurança nas IES. Um estudo desenvolvido por Caruso (2003), baseado em inquéritos a 435 IES, revelou que, naquela época, as primeiras abordagens de segurança aplicadas eram, em grande parte, centradas em medidas reativas e de baixo custo, como o *backup* centralizado de dados e o uso de *firewalls* de perímetro. Embora estas práticas ainda sejam valiosas, revelam-se insuficientes face ao atual panorama de ciberameaças em constante evolução, especialmente em virtude da transição digital nas últimas décadas.

A evolução das ciberameaças no setor da educação é corroborada por relatórios mais recentes, como o estudo "*University Challenge: Cyber Attacks in Higher Education*", desenvolvido por VMware em 2016. Este relatório, que incluiu IES do Reino Unido, revelou que cerca de 87% das IES já tinham sido alvos de ataques informáticos bem-

sucedidos, e uma em cada três universidades era atacada a cada hora. Além disso, 83% das instituições participantes no estudo acreditavam que a sofisticação dos ataques estava a aumentar, assim como a sua frequência. Estes dados destacam não só a evolução das ciberameaças nas IES, mas também o agravamento da sua complexidade e da frequência com que ocorrem. Os ataques são agora muito mais sofisticados do que os observados nos primeiros estudos, o que reflete a crescente sofisticação das táticas e técnicas utilizadas pelos atacantes.

Um exemplo ilustrativo dessa evolução pode ser observado no ataque informático ocorrido em 2022, que afetou 76 universidades, provenientes de 14 países diferentes, e foi perpetrado por um grupo de hackers iranianos. Durante este ataque, cerca de 31 terabytes de informação privilegiada foram expostos, a maioria dos quais envolvendo dados académicos, informação relacionada com projetos de investigação e dados pessoais dos estudantes e professores. Este ataque destacou-se não apenas pela sua escala, mas também pela sua natureza altamente sofisticada, fazendo parte de uma campanha de espionagem.

Um outro exemplo mais recente, que sublinha ainda mais a evolução das ameaças, ocorreu em agosto de 2024, quando a Universidade Paris-Saclay, na França, foi alvo de um ataque de *ransomware* perpetrado pelo grupo RansomHouse. Este ataque resultou na paralisação do sistema informático da Universidade e afetou gravemente os seus sistemas centrais. Além disso, levou à exposição de informações sensíveis, com o grupo de *ransomware* a afirmar ter roubado 1 terabyte de dados e ameaçando divulgar 193 arquivos em formato PDF contendo, maioritariamente, currículos, transcrições, cartas de motivação/recomendação, diplomas e até documentos de identidade provenientes de 44 candidaturas ao nível de mestrado.

De acordo com o jornal francês *Le Monde,* a Universidade Paris-Saclay, em resposta ao ataque, manteve-se fiel aos princípios governamentais, não entrando em contacto com os atacantes e recusando o pagamento de qualquer resgate. A Universidade também apresentou queixa às autoridades francesas.

Estes dois exemplos no panorama internacional ilustram de forma clara a evolução das ciberameaças no Ensino Superior, evidenciando a transição de ataques simples para

estratégias cada vez mais sofisticadas, direcionadas não só para o roubo de dados, mas também para a exploração de sistemas críticos e a extorsão de organizações através de *ransomwares*. A crescente complexidade e a escala desses ataques sublinham a necessidade de medidas de segurança mais robustas e de uma gestão proativa da cibersegurança nas IES.

1.2.6 Panorama da Cibersegurança em Portugal no setor educativo

A nível nacional, o impacto das ciberameaças no ensino superior reflete-se nos dados apresentados pelo CNCS. De acordo com o "Relatório Cibersegurança em Portugal", o número de incidentes registados pelo CERT.PT tem vindo a aumentar ao longo dos anos, demonstrando, no entanto, uma tendência de estabilização a partir de 2022, tal como é possível verificar na Figura 3.

Figura 3 - Número de incidentes registados pelo CERT.PT por ano

Fonte: "Relatório Cibersegurança em Portugal" do CNCS

Com base nos dados apresentados pelo CERT.PT, o setor da Educação, Ciência, Tecnologia e Ensino Superior manteve-se entre os cinco setores mais afetados por ciberataques em 2023, ocupando a quinta posição no *ranking* nacional. Este posicionamento evidencia que as IES continuam a ser alvos estratégicos para ataques informáticos.

No entanto, verificou-se uma redução face ao ano anterior, com menos 26 ataques em 2023 do que em 2022 (tal como se destaca na Figura 4) o que poderá estar associado

a melhorias na implementação de medidas de cibersegurança, a uma maior sensibilização para as ameaças e ataques digitais e a possíveis avanços tecnológicos na proteção de infraestruturas digitais das instituições.

2022				2023				Ordenação	
RK	Setor e Área Governativa[5]	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Outros	1055	37	1º	Outros	1503	74	+42	=
2º	Banca	542	19	2º	Prestadores de Serviços de Internet	517	26	+249	+
3º	Infraestruturas Digitais	205	7	3º	Banca	197	10	-64	-
4º	Educação e Ciência, Tecnologia e Ensino Superior	202	7	4º	Saúde	171	8	+106	+
5º	Prestadores de Serviços de Internet	148	5	5º	Educação, Ciência, Tecnologia e Ensino Superior	150	7	-26	-
6º	Presidência do Conselho de Ministros	131	5	6º	Infraestruturas Digitais	148	7	-28	-
7º	Administração Pública Local	129	5	7º	Transportes	136	7	+46	+
8º	Transportes	93	3	8º	Administração Pública Local	111	5	-14	-
9º	Saúde	83	3	9º	Serviço de Computação em Nuvem	102	5	+10100	+
10º	Finanças	55	2	10º	Presidência do Conselho de Ministros	70	3	-47	-

Figura 4 - Incidentes por setor e área governativa registados pelo CERT.PT – TOP 10

Fonte: CERT.PT

No que diz respeito aos tipos de ataques mais frequentes em Portugal, os dados apresentados no relatório de Cibersegurança, revelam que o *phishing*/smishing manteve-se como o vetor de ataque predominante em 2023, representando 35% dos incidentes reportados, embora tenha registado uma ligeira redução de 6% face ao ano anterior, continua a ser uma ameaça significativa, explorando táticas de engenharia social para induzir vítimas a revelar credenciais e informações sensíveis.

No entanto, um dos dados mais alarmantes é o aumento significativo das tentativas de login malicioso, que cresceram 2785% face a 2022, tornando-se o segundo tipo de ataque mais frequente. Este crescimento poderá estar associado ao uso de credenciais comprometidas e muitas vezes obtidas através de campanhas de *phishing*, aumentando o risco para instituições que dependem de sistemas autenticados. A engenharia social, que

ocupava a segunda posição em 2022, passou para terceiro lugar em 2023. No entanto, a sua relevância mantém-se elevada, uma vez que continua a ser um vetor de entrada para outras ameaças, como o *phishing* e o comprometimento de contas.

Por outro lado, verificou-se uma redução significativa nos casos de distribuição de *malware* (-42%) e na utilização ilegítima de nomes de terceiros (-18%), o que pode refletir um reforço das medidas de cibersegurança e de consciencialização para a deteção destes ataques.

Entre as ameaças emergentes, destaca-se o aumento de 40% nos casos de sistemas vulneráveis, que passaram a representar 3% dos incidentes, evidenciando a importância de manter infraestruturas atualizadas e protegidas contra explorações de vulnerabilidades, tal como se constata na Figura 5.

2022				2023				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	*Phishing/Smishing*	742	37	1º	*Phishing/Smishing*	700	35	-6	=
2º	Engenharia social	285	14	2º	Tentativa de *login*	375	19	+2785	+
3º	Distribuição de *malware*	214	11	3º	Engenharia Social	205	10	-28	-
4º	Utilização Ilegítima de nome de terceiros	126	6	4º	Comprometimento de conta não privilegiada	139	7	+21	+
5º	Comprometimento de conta não privilegiada	115	6	5º	Distribuição de *malware*	124	6	-42	-
6º	Sistema infetado (*malware*)	84	4	6º	Utilização ilegítima de nome de terceiros	103	5	-18	-
7º	Comprometimento de aplicação	81	4	7º	Sistema infetado (*malware*)	90	4	+7	-
8º	Modificação não autorizada (69 *ransomware*)	74	4	8º	Sistema vulnerável	67	3	+40	+
9º	SPAM	62	3	9º	Modificação não autorizada (57 de *ransomware*)	57	3	-23	+
10º	Sistema vulnerável	48	2	10º	Comprometimento de aplicação	40	2	-51	-

Figura 5 - Incidentes por tipo registados pelo CERT.PT – Top 10

Fonte: CERT.PT

De acordo com o mesmo relatório, o *phishing/smishing* foi o tipo de ataque mais frequente no setor da Educação, Ciência, Tecnologia e Ensino Superior, representando 27% dos incidentes reportados neste setor. Este dado confirma que as IES continuam a ser alvos atrativos para ataques de engenharia social, uma vez que dependem fortemente de plataformas digitais e serviços de email para comunicação interna e externa (em destaque na Figura 6.

	Tipo de incidente	Nº	% no setor	% do total
Educação, Ciência, Tecnologia e Ensino Superior	*Phishing/Smishing*	40	27	1

Figura 6 – Tipo de incidentes mais frequentes no setor da Educação, Ciência, Tecnologia e Ensino Superior registados pelo CERT.PT em 2023

Fonte: CERT.PT

Adicionalmente, o Centro Nacional de Cibersegurança (CNCS), no seu *Guia para a Gestão dos Riscos em Matérias de Segurança da Informação e Cibersegurança* (2022:50), apresenta no Anexo A – *Catálogo de Ameaças Comuns* – um conjunto de exemplos de ameaças comuns que podem afetar as organizações. Estas ameaças são organizadas em três grandes categorias: intencionais, acidentais e de origem natural ou ambiental. Pela sua natureza aberta e pela elevada quantidade de dados sensíveis que gerem, as IES estão particularmente expostas a muitas destas ameaças. Entre elas, o erro humano surge como uma das mais relevantes. O CNCS identifica situações como a divulgação indevida de informação, a introdução de dados provenientes de fontes não confiáveis, a utilização incorreta de equipamentos e software, o acesso não autorizado a sistemas, bem como a violação de leis e regulamentos. Estas ameaças, muitas vezes resultantes de falhas de atenção, desconhecimento ou falta de formação adequada, reforçam a necessidade de promover ações regulares de sensibilização e formação junto dos utilizadores.

Neste sentido, tanto o CERT.PT como o CNCS têm vindo a destacar que o fator humano continua a ser um dos elementos mais vulneráveis no domínio da segurança digital, exigindo uma atenção contínua por parte das organizações. A formação contínua em boas práticas de cibersegurança revela-se essencial, especialmente no contexto das IES, uma vez que desempenham um papel fundamental na formação de profissionais e investigadores. Dado o crescimento das ameaças digitais, a sensibilização e a formação dos utilizadores são aspetos críticos para mitigar riscos e fortalecer a segurança das infraestruturas digitais.

1.2.7 Principais características e vulnerabilidades das IES

Após a análise do panorama da cibersegurança, é essencial identificar as principais características que tornam as Instituições de Ensino Superior particularmente vulneráveis a ameaças neste domínio, sobretudo numa altura em que os problemas de segurança dos sistemas de informação têm vindo a atrair uma atenção crescente nas últimas décadas (Cheng et all, 2022).

Numa perspetiva mais abrangente, as vulnerabilidades mais frequentemente associadas às organizações no setor do ensino superior, no domínio da cibersegurança, podem ser agrupadas em três principais categorias conforme proposto por Wangen et al (2021) e tendo por base a norma ISO 27005:2018:

- **Administrativas e organizacionais**

As vulnerabilidades administrativas e organizacionais incluem a falta de sensibilização e conhecimento acerca da segurança da informação, a gestão inadequada da segurança da informação, o conflito entre a cultura académica e os requisitos de segurança da informação. Segundo Wangen et al (2021), a "*ausência de um compromisso transversal e de uma cultura organizacional centrada na segurança compromete seriamente a eficácia das medidas implementadas*".

Para além dos supramencionados, destaca-se, ainda, a falta de apoio da gestão, recursos e financiamento. De acordo com FireEye, Inc. (2019:4), "*ao estabelecer prioridades de despesa, os administradores tendem a favorecer iniciativas académicas, comparativamente aos investimentos em segurança. Este défice de segurança é agravado pelo elevado número de servidores e dispositivos que as instituições têm de gerir, bem como pela complexidade de cumprir requisitos regulamentares que variam entre programas académicos e de investigação, operações de saúde, segurança do campus, e outras atividades essenciais"*.

Adicionalmente, o CNCS apresenta exemplos das vulnerabilidades administrativas e organizacionais no Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança, publicado em 2022, que se destacam na tabela 2:

Tabela 3 - Exemplos de Vulnerabilidades Organizacionais segundo o CNCS

Tipos	Exemplos de vulnerabilidades
Organização	Inexistência ou ineficácia na sua implementação de um procedimento formal para o registo e a remoção de utilizadores
	Inexistência ou ineficácia na sua implementação de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Inexistência ou ineficácia na sua implementação de procedimento de monitorização das instalações de processamento de informações
	Inexistência de auditorias periódicas (supervisão) regulares
	Inexistência ou ineficácia na sua implementação de procedimentos para a identificação, análise e avaliação dos riscos
	Inexistência ou insuficientes relatórios de falha nos arquivos ("logs") de auditoria das atividades de administradores e operadores
	Resposta inadequada do serviço de manutenção
	Service Level Agreement (SLA) inexistente ou insuficiente
	Inexistência ou ineficácia na sua implementação de procedimento de controlo de mudanças
	Inexistência ou ineficácia na sua implementação de um procedimento formal para o controlo da documentação do SGSI – Sistema de Gestão de Segurança da Informação
	Inexistência ou ineficácia na sua implementação de um procedimento formal para a supervisão dos registos do SGSI
	Inexistência ou ineficácia na sua implementação de um processo formal para a autorização de informações passiveis de disponibilização publica
	Atribuição inadequada das responsabilidades de segurança da informação
	Inexistência, insuficiência ou desatualização de um plano de continuidade
	Inexistência ou ineficácia na sua implementação de política de uso de e-mail
	Inexistência ou ineficácia na sua implementação de procedimentos para a instalação de software em sistemas operativos
	Inexistência ou ineficácia na sua implementação de procedimentos para o manuseamento de informações classificadas
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções
	Insuficiência ou inexistência de cláusulas (relativas à segurança da informação) em contratos com funcionários
	Inexistência ou inadequação de um processo disciplinar no caso de incidentes relacionados com a segurança da informação
	Inexistência ou inadequação de uma política formal sobre o uso de dispositivos móveis
	Insuficiente controlo de ativos fora das instalações
	Política de mesas e ecrãs limpos ("clear desk and clear screen") inexistente ou insuficiente
	Inexistência de, ou falha na autorização para as instalações de processamento de informações.
	Inexistência ou insuficiência dos mecanismos de monitorização de violações da segurança
	Inexistência ou ineficácia na implementação de procedimentos para o reporte de fragilidades ligadas à segurança.
	Inexistência ou ineficácia na implementação de procedimentos para garantir a conformidade com os direitos de propriedade intelectual

Tipos	Exemplos de vulnerabilidades
Pessoas	Ausência de recursos humanos
	Procedimentos de recrutamento inadequados
	Formação insuficiente em segurança
	Uso incorreto de software e hardware
	Falta de consciencialização em segurança
	Inexistência ou insuficiência de mecanismos de monitorização
	Trabalho não supervisionado de pessoal de limpeza ou de terceiros
	Inexistência ou insuficiência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens

Fonte: Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (CNCS, 2022:54)

Segundo Amine et al (2023) um dos principais desafios organizacionais incluem a falta de pessoal especializado em segurança informática, o que compromete a identificação e mitigação atempada de ameaças. No entanto, de acordo com o relatório da Europol (2024), o fator humano continua a ser o elo mais fraco na maior parte dos cenários de ciberataques.

- **Técnicas**

As vulnerabilidades técnicas incluem a utilização de dispositivos pessoais (BYOD – *Bring Your Own Device*), que, de acordo com Wangen et al (2021), podem provocar incidentes quando a rede possui uma arquitetura de segurança inadequada e mecanismos de controlo de acesso implementados incorretamente. A descentralização da informação numa organização, a implementação de controlos de segurança sem ter por base as melhores práticas e a complexidade técnica e da rede podem igualmente comprometer a segurança da informação de uma organização. De acordo com Amine et al (2023) a inexistência de um centro de dados centralizado pode comprometer a manutenção de um ambiente informático seguro e organizado.

Para além das vulnerabilidades técnicas descritas acima, o CNCS aborda as mesmas distinguindo por três categorias, hardware, software e rede, conforme tabela 4:

Tabela 4 - Exemplos de Vulnerabilidades Técninas segundo o CNCS

Tipos	Exemplos de vulnerabilidades
Hardware	Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento
	Falta de uma rotina de substituição periódica
	Suscetibilidade à humidade, poeira, sujeira
	Sensibilidade à radiação eletromagnética
	Inexistência de um controlo eficiente de mudança de configuração
	Suscetibilidade a variações de voltagem
	Suscetibilidade a variações de temperatura
	Armazenamento não protegido
	Falta de cuidado durante o descarte ou destruição
	Realização não controlada de cópias

Tipos	Exemplos de vulnerabilidades
Software	Procedimentos de teste de software insuficientes ou inexistentes
	Falhas conhecidas no software
	Não execução do término de sessão (logout) ao deixar-se uma estação de trabalho sem assistência / controlo
	Destruição ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados
	Inexistência de um registo de auditoria
	Atribuição indevida de direitos de acesso
	Software amplamente distribuído
	Utilizar programas com um conjunto errado de dados (referentes a um outro período)
	Interface de utilizador complexa
	Documentação inexistente ou insuficiente
	Configuração incorreta de parâmetros
	Datas incorretas
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
	Listas de passwords desprotegidas
	Fraca gestão de passwords
	Serviços desnecessários permanecem habilitados
	Software novo ou imaturo
	Especificações confusas ou incompletas para os programadores
	Inexistência de um controlo eficaz de mudança
	Download e uso não controlado de software
	Falta ou inexistência de cópias de segurança ("backup")
	Inexistência de relatórios de gestão

Tipos	Exemplos de vulnerabilidades
Rede	Inexistência ou insuficientes evidências que comprovem o envio ou receção de mensagens
	Linhas de comunicação desprotegidas
	Tráfego sensível desprotegido
	Junções de cablagem mal feitas
	Ponto único de falha
	Falta ou ineficácia de mecanismos de identificação e autenticação do emissor e do recetor
	Arquitetura insegura da rede
	Transferência de passwords em claro
	Gestão de rede inadequada (quanto à flexibilidade de roteamento)
	Conexões de redes públicas desprotegidas

Fonte: Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (CNCS, 2022:52)

- **Físicas**

Relativamente a vulnerabilidades físicas, tendo em conta a cultura académica aberta e inclusiva, as universidades geralmente têm muito pouca segurança física, A segurança física é um aspeto essencial da segurança da informação, pois pode levar à perda de hardware, espionagem e roubo de dados (Wangen et al, 2021).

No caso concreto das vulnerabilidades físicas, o CNCS destaca as vulnerabilidades presentes na Tabela 5:

Tabela 5 - Exemplos de Vulnerabilidades Físicas segundo o CNCS

Tipos	Exemplos de vulnerabilidades
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e salas
	Localização em área suscetível a inundações
	Fornecimento instável de energia
	Insuficientes mecanismos de proteção física no prédio, portas e janelas

Fonte: Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (CNCS, 2022:53

As ameaças de cibersegurança estão cada vez mais sofisticadas, no entanto as Instituições de Ensino Superior enfrentam desafios únicos que tornam a implementação eficaz de cibersegurança mais difícil do que noutros sectores.

De acordo com o relatório "*Higher Education Roadmap to Building a Sustainable Cybersecurity Management Program*"[3] (EDUCAUSE, 2018) as principais características

[3] O Relatório apresenta um guia estratégico para o desenvolvimento de um programa sustentável de gestão de cibersegurança nas Instituições de Ensino Superior.

das IES que podem impactar a cibersegurança dividem-se em quatro principais categorias:

a) Quantidade e variedade de dados

De acordo com o relatório referido anteriormente, as IES, à semelhança de todas as instituições, têm o dever de assegurar a proteção da informação relativa aos seus funcionários e colaboradores. Contudo, devido à sua natureza, as IES gerem uma vasta tipologia de dados que abrangem diversas áreas da sua atividade. Para além da informação pessoal e profissional de alunos, antigos alunos, docentes e funcionários, as IES tratam igualmente de dados referentes a bolsas de estudo, financiamentos, doações, bem como são ainda responsáveis pela realização de projetos de investigação.

Segundo Giszczak & Paluzzi (2016), as IES armazenam dados — financeiros, médicos e pessoais — incluindo doadores, membros dos conselhos, antigos alunos, estudantes, pais, candidatos, docentes, funcionários, investigadores, pacientes, consumidores e fornecedores, o que torna as IES alvos privilegiados de ciberataques devido à enorme quantidade de dados que recolhem e mantêm a partir destas fontes. No entanto, para além da grande quantidade e variedade de dados, o mesmo autor refere que as instituições de ensino superior são também particularmente vulneráveis devido à natureza aberta.

A Queensland University of Technology (QUT) publicou um registo de todos os seus ativos de informação, conhecido como *Information Asset Register* (IAR), onde são descritos e categorizados por várias áreas funcionais, detalhando, em cada uma, os tipos de dados, a sua finalidade e os sistemas associados. De seguida, são apresentadas as principais categorias de ativos de informação, com base no registo estruturado desenvolvido pela QUT, que podem ser adaptáveis a qualquer IES:

1. Informações sobre Estudantes
2. Informações sobre Ensino e Aprendizagem
3. Informações sobre Investigações
4. Informações sobre Gestão de Instalações
5. Informações sobre Gestão Financeira

6. Informações sobre Governação, Estratégia e Política
7. Informações sobre Inteligência Estratégica e Relatórios
8. Informações sobre Suporte Tecnológico (TI)
9. Informações sobre Recursos Humanos
10. Informações sobre Alumni, Desenvolvimento e Envolvimento
11. Informações sobre Marketing, Media e Comunicações
12. Informações de Dados administrativos e financeiros sobre saúde
13. Dados e Informação Curados
14. Informações disponibilizadas publicamente que não requerem autenticação

b) Descentralização de dados

Segundo o relatório "Higher Education Roadmap to Building a Sustainable Cybersecurity Management Program" (2018), nas IES existe uma maior descentralização de dados, o que dificulta, muitas vezes, a proteção da informação. Esta "descentralização típica das estruturas organizacionais nas IES — onde diferentes departamentos gerem os seus próprios sistemas e dados — contribui para uma maior complexidade e dificulta a implementação de políticas uniformes de segurança", o que compromete a capacidade de resposta coordenada perante incidentes, pela ausência de uma visão integrada da segurança da informação (Wangen et al, 2021).

De acordo com EDUCAUSE (2023), a "*estrutura organizacional, orientada para a partilha aberta de informação e o acesso descentralizado, contribui para que estas instituições sejam alvos mais fáceis*" em matéria de cibersegurança.

c) Regras e Regulamentos:

A grande quantidade de regulamentos e disposições legais às quais as IES estão sujeitas pode dificultar o seguimento de uma única estrutura regulatória.

d) Fundos:

Segundo o relatório "Higher Education Roadmap to Building a Sustainable Cybersecurity Management Program" (2018), nas IES os fundos são controlados muitas

vezes por legisladores e doadores, o que pode dificultar o seu acesso por parte das instituições. As IES enfrentam, igualmente, maiores dificuldades na alocação de fundos quando comparadas com empresas privadas.

Segundo dados da OCDE (2022), em Portugal o total de despesas com instituições públicas de ensino superior, em 2018, representava o equivalente a 0,9% do Produto Interno Bruto (PIB) nacional, comparativamente à média de 1,1% nos países da OCDE.

De acordo com EDUCAUSE (2023), "a falta de orçamento torna difícil reforçar as infraestruturas face ao panorama de ameaças em constante evolução ou competir com empresas privadas na contratação de profissionais de TI qualificados".

1.2.8 O papel do Estado e da UE no contexto da transição digital nas IES

Como resposta ao processo de digitalização e ao crescente risco de ciberataques e cibercrime associado, têm vindo a ser desenvolvidos planos e estratégias relacionadas com a transição digital em Portugal, com destaque para o setor da educação e nas Instituições de Ensino Superior. Nos cronogramas seguintes são enumeradas as várias iniciativas do Estado Português e da União Europeia desde 2018, tal como apresentado na Figura 7.

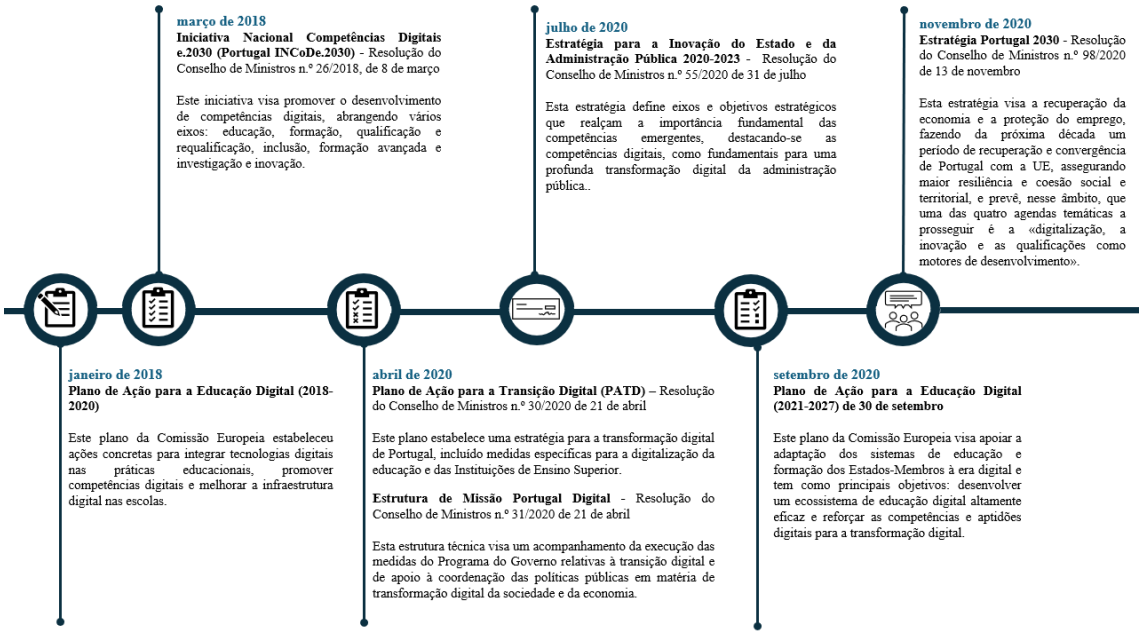

Figura 7 - Cronograma de planos, iniciativas e estratégias adotados para apoiar o processo de TD nas organizações (2018-2020)

Fonte: Elaboração Própria

Os anos de 2018 e 2020, foram determinantes para a aceleração da transformação digital, especialmente impulsionados pela Pandemia Covid-19. Este período forçou muitas empresas e organizações a adotarem novos métodos digitais para garantir a continuidade dos seus negócios. Em Portugal, foram implementados diversos planos e estratégias para promover a transição digital em diferentes setores da sociedade. De seguida apresentam-se as medidas mais significativas relacionadas com as IES, com foco nas iniciativas mais relevantes e com maior impacto:

a) a Iniciativa Nacional Competências Digitais e.2030, aprovada pela Resolução do Conselho de Ministros n.º 26/2018, de 8 de março, que entre outras medidas, visa o desenvolvimento e implementação de competências digitais nas IES e assenta em 5 eixos, entre os quais a educação, através da "*formação das camadas mais jovens através do reforço de competências digitais em todos os ciclos de ensino e de aprendizagem*" (Governo de Portugal, 2018).
b) o Plano de Ação para a Transição Digital, aprovado pela Resolução do Conselho de Ministros n.º 30/2020 de 21 de abril, com o propósito de acelerar o processo de digitalização em Portugal. Este plano reflete a estratégia definida para a

transição digital e condensa a visão do Governo neste domínio, materializada numa estrutura que contempla três principais pilares de atuação: Pilar I - Capacitação e inclusão digital das pessoas; Pilar II - Transformação digital do tecido empresarial; Pilar III - Digitalização do Estado, bem como uma dimensão adicional de catalisação que cria as condições de base a uma acelerada digitalização do País.

c) Plano de Ação para a Educação Digital (2021-2027) de 30 de setembro, iniciativa da União Europeia, "*é um apelo a uma maior cooperação a nível europeu em matéria de educação digital a fim de dar resposta aos desafios e aproveitar as oportunidades ligadas à pandemia de COVID-19 e de oferecer oportunidades à comunidade educativa (professores e estudantes), aos decisores políticos, ao meio académico e aos investigadores a nível nacional, da UE e internacional*" e visa, essencialmente, promover o desenvolvimento de um ecossistema de educação digital altamente eficaz e reforçar as aptidões e competências digitais para a transformação digital. Este plano baseia-se no primeiro Plano de Ação para a Educação Digital (2018-2020).

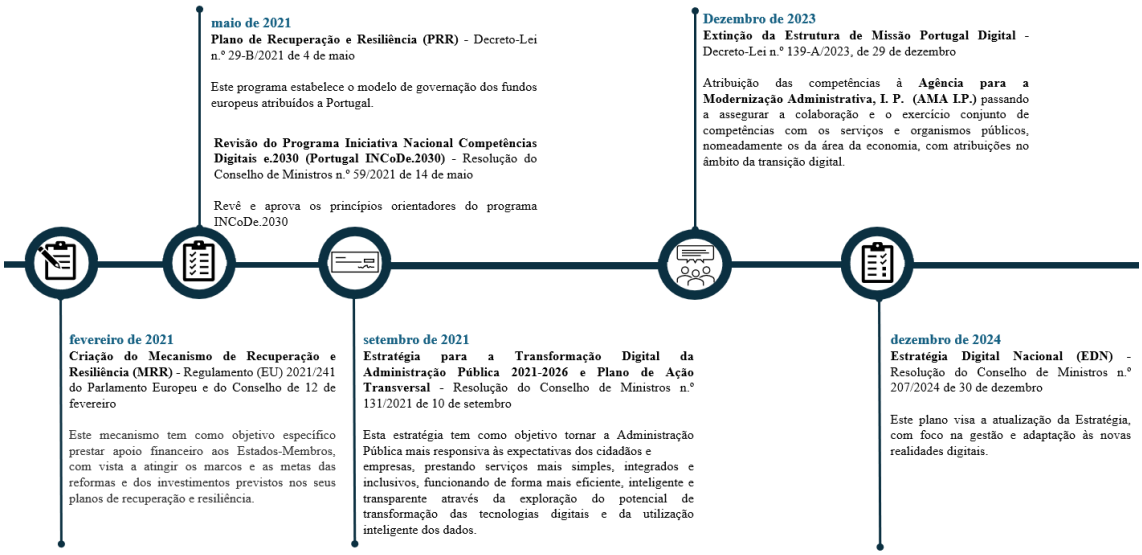

Figura 8 - Cronograma de planos, iniciativas e estratégias adotados para apoiar o processo de TD nas organizações (2021-2024)

Fonte: Elaboração Própria

Entre os anos de 2021 e 2024, foram intensificados os esforços para a transição digital das organizações tendo em conta as novas exigências de uma sociedade cada vez mais digital. Neste período os planos e iniciativas mais relevantes implementados em Portugal foram:

a) O Plano de Recuperação e Resiliência, aprovado pelo Decreto-Lei n.º 29-B/2021 de 4 de maio, após a criação do MRR através do Regulamento (EU) 2021/241 do Parlamento Europeu e do Conselho de 12 de fevereiro. Este plano inclui programas como o "Impulso Jovens STEAM", o "Impulso Adultos" e o "Impulso MAIS Digital". O primeiro tem por objetivo promover e apoiar iniciativas orientadas exclusivamente para aumentar a graduação superior de jovens em áreas de ciências, tecnologias, engenharias, artes e matemática, através da oferta de licenciaturas e outras formações iniciais de âmbito superior (DGES, 2024). O Impulso Adultos tem por objetivo apoiar a conversão e atualização de competências de adultos ativos, através de formações de curta duração no ensino superior, de nível inicial e de pós-graduação, em todas as áreas do conhecimento, assim como a formação ao

longo da vida (DGES, 2024). O programa "Impulso MAIS Digital" tem como objetivos o estímulo à modernização da rede de ensino superior, com ênfase em áreas-chave para a resiliência do país e o aumento das competências na sociedade e nas empresas, nomeadamente nas áreas digitais e tecnológicas, através de um maior número de ofertas formativas por parte das Instituições de Ensino Superior e de um maior número de jovens e adultos formados e requalificados e engloba as seguintes medidas:

i) Reforma e Modernização das Ciências Agrárias - Modernização Tecnológica e Digital das Ciências Agrárias;
ii) Reforma e Modernização da Medicina;
iii) Reforço das Competências digitais;
iv) Inovação e Modernização Pedagógica no Ensino Superior - Criação de Centros de Excelência de inovação pedagógica;
v) Inovação e Modernização Pedagógica no Ensino Superior - Programa de Promoção de Sucesso e Redução de Abandono no Ensino Superior. (DGES, 2024).

b) Estratégia Digital Nacional (EDN) aprovada pela Resolução do Conselho de Ministros n.º 207/2024 de 30 de dezembro, visa a atualização da Estratégia, com foco na gestão e adaptação às novas realidades digitais.

A par das medidas aplicadas por Portugal e pela EU, a Comissão Europeia tem vindo a acompanhar o progresso digital dos Estados-Membros e embora existam sinais de convergência no processo de digitalização, este ainda é desigual (IDES, 2022), conforme se pode observar na Figura 9.

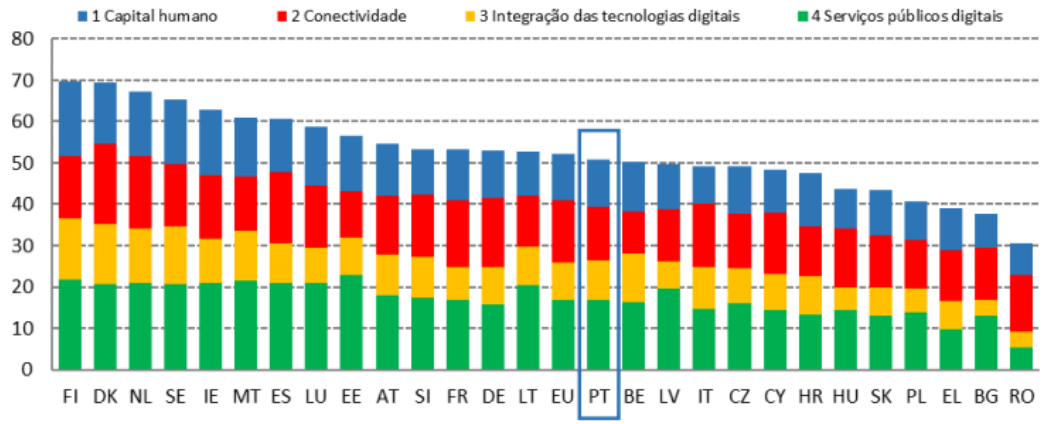

Figura 9 - Classificações do Índice de Digitalidade da Economia e da Sociedade (IDES) de 2022.

Fonte: Comissão Europeia. (2022). Índice de Digitalidade da Economia e da Sociedade (DESI) 2022: Portugal. Consultado em https://digital-strategy.ec.europa.eu/en/policies/desi-portugal

Portugal ocupa o 15º lugar entre os 27 Estados-Membros da EU e segundo o mesmo relatório "os progressos relativos de Portugal são, de modo geral, ligeiramente inferiores aos dos países homólogos, pelo que há margem para o país acelerar os seus esforços de digitalização" (IDES, 2022).

Dado o contínuo crescimento da digitalização das organizações em Portugal é imperativo adotar medidas eficazes para garantir a adequada proteção dos dados, através da implementação e acompanhamento de práticas de segurança da informação, a fim de salvaguardar a privacidade das pessoas e das organizações, bem como assegurar a conformidade com os regulamentos legais aplicáveis.

1.2.9 Normativos e Regulamentos relacionados com a Cibersegurança nas IES

1.2.9.1 Normativos e Frameworks de cibersegurança a nível internacional

Os normativos e as *frameworks* de cibersegurança são estruturas ou conjunto de diretrizes, boas práticas e procedimentos desenvolvidos para ajudar as organizações a gerir a segurança da informação e a proteger os seus sistemas e dados contra qualquer ciberameaça.

O cronograma apresentado sintetiza os principais *frameworks* adotados pelas organizações desde a década de 1990 até ao presente.

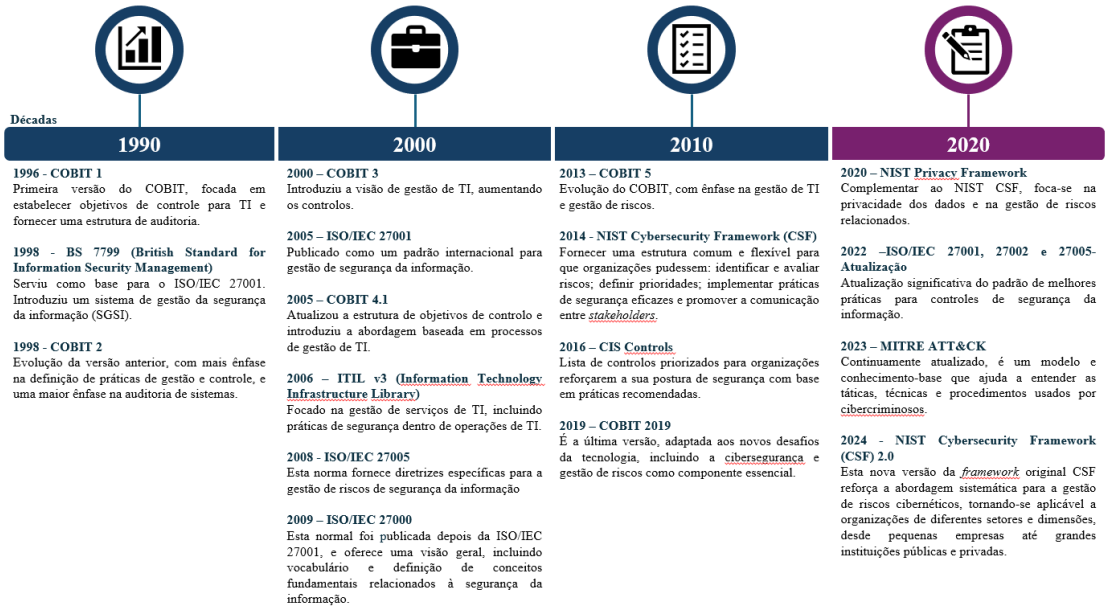

Figura 10 - Cronograma dos frameworks mais utilizados no âmbito da segurança da informação

Fonte: Elaboração Própria

Nas últimas quatro décadas observou-se uma evolução história significativa dos *frameworks* de cibersegurança. Na década de 1990, o foco estava em estabelecer normas e diretrizes iniciais, em resposta ao crescimento exponencial da *internet* e conetividade. A partir da década de 2020, a cibersegurança passou a ser integrada como gestão de riscos e conformidade regulatória. Este período também foi marcado pela expansão do conceito de cibersegurança para contextos digitais cada vez mais complexos, refletindo as mudanças tecnológicas e as novas exigências regulatórias num mundo cada vez mais globalizado.

As *frameworks* de cibersegurança mais amplamente reconhecidas e adotadas no campo da proteção digital incluem as seguintes:

a) Cyber Security *Framework* (CSF 2.0) do National Institute of Standards and Technology (NIST)
b) Normas da International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), designadamente 27000
c) Control Objectives for Information and Related Technologies (COBIT)
d) Center for Internet Security (CIS) Controls

a) NIST Cybersecurity Framework (CSF) 2.0

O *National Institute of Standards and Technology* (NIST) criou uma *framework* de cibersegurança com um conjunto de diretrizes e boas práticas, em forma de controlos e ações, com o objetivo de mitigar os riscos de segurança da informação nas organizações (NIST 2013). Esta *framework* tem sido sujeito a algumas atualizações ao longo das últimas duas décadas, com a sua primeira versão publicada em 2014. De forma a adaptar-se à realidade e necessidades das organizações e do mundo no contexto da cibersegurança foi publicada a mais recente versão em fevereiro de 2024.

O NIST CFS fornece às organizações uma estrutura abrangente para gerir os riscos de cibersegurança de forma eficaz, através de três indicadores:

a) Compreender e Avaliar – O CSF permite às organizações descrever a sua postura atual ou desejada em matéria de cibersegurança, seja em toda a organização ou em áreas específicas. Este processo facilita a identificação de lacunas e apoia a avaliação do progresso na resolução dessas mesmas lacunas.
b) Priorizar – O CSF ajuda a identificar, organizar e priorizar ações destinadas à gestão dos riscos de cibersegurança. Estas ações são alinhadas com a missão da organização, o cumprimento das exigências legais e regulamentares, e os objetivos gerais de gestão de riscos.
c) Comunicar – O CSF oferece uma linguagem padronizada que simplifica a comunicação sobre os riscos, capacidades, necessidades e expectativas em matéria de cibersegurança. (NIST CSF 2.0)

O CSF 2.0 encontra-se organizado em seis funções, governar, identificar, proteger, detetar, responder e recuperar, representadas na Figura 11:

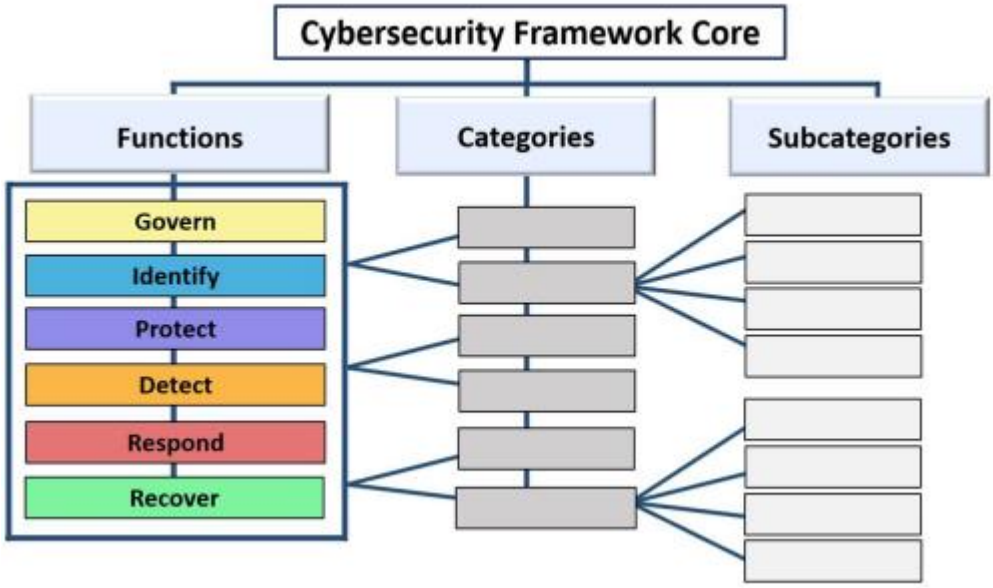

Figura 11 - Estrutura do CSF Core 2.0

Fonte: National Institute of Standards and Technology. (2024:3). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29). https://doi.org/10.6028/NIST.CSWP.29NIST

A estrutura do CSF Core é organizada de forma hierárquica e composta por três níveis principais: funções, categorias e subcategorias.

b) Normas ISO/IEC 27000

O conjunto de normas ISO/IEC 27000 tem como objetivo ajudar as organizações a estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação (SGSI).

Este *framework* é dinâmica, sendo atualizado regularmente e integra, entre outras, as seguintes normas:

a) ISO/IEC 27000: Estrutura Geral - Esta norma oferece uma visão abrangente da série 27000, incluindo vocabulário essencial e definições fundamentais relacionadas à segurança da informação.

b) ISO/IEC 27001: Requisitos para certificação - Principal referencial normativo que estabelece os requisitos para implementar e manter um SGSI. É a norma utilizada para a certificação.
c) ISO/IEC 27002: Controlos de segurança da informação – Esta norma complementa a ISO/IEC 27001, servindo como guia para a implementação detalhada dos controlos de segurança.
d) ISO/IEC 27003: Segurança da informação, cibersegurança e proteção da privacidade - Estabelece uma orientação sobre a implementação de Sistemas de Gestão da Segurança da Informação.
e) ISO/IEC 27004: Métricas e relatórios do SGSI – Esta norma estabelece a forma de medição da eficácia dos sistemas de gestão da segurança da informação.
f) ISO/IEC 27005: Gestão de riscos em segurança da informação – Esta norma fornece as diretrizes para a gestão de riscos de segurança da informação.
g) ISO/IEC 27032: Tecnologias da informação - Oferece diretrizes para a cibersegurança no contexto das tecnologias de informação.

A ISO/IEC 27001:2022 é o referencial global para a certificação de SGSI, e permite às organizações uma eficaz gestão e proteção da informação através da implementação dos controlos de segurança, conferindo um elevado grau de confiança de todas as partes interessadas. Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação no contexto da organização e inclui requisitos para a avaliação e tratamento dos riscos de segurança da informação adaptados às necessidades de cada organização.

A ISO/IEC 27001:2022 não estabelece controlos específicos, no entanto remete para a ISO/IEC 27002 que inclui a lista de práticas recomendadas e funciona como um guia de apoio para implementar os controlos definidos no Anexo A da ISO/IEC 27001. A versão de 2022 da ISO/IEC 27002 trouxe importantes atualizações face à versão de 2013, incluindo a reestruturação dos controlos, agora organizados em quatro categorias (organizacionais, pessoais, tecnológicos e físicos) totalizando 93 controlos.

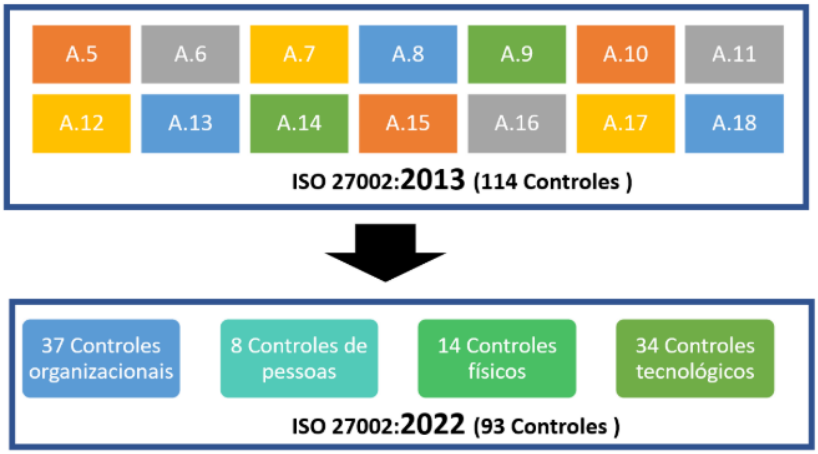

Figura 12 - Ilustração dos controlos segundo a ISO/IEC 27002

Fonte: Bastos (2023)

c) Control Objectives for Information and Related Technologies (COBIT)

O COBIT é uma *framework* desenvolvida pela *Information Systems Audit and Control Association* (ISACA) e é um conjunto de boas práticas e orientações para a gestão das TI nas organizações, fornecendo um modelo de referência para assegurar que os recursos TI sejam utilizados de forma eficiente, eficaz e em conformidade com os objetivos da organização. Esta *framework* foi criada em 1996 e tem vindo a ser atualizada ao longo das últimas décadas. A última versão é a COBIT 2019 que para além da atualização da *framework*, oferece recursos adicionais de implementação, orientações práticas e insights, bem como amplas oportunidades de formação.

O COBIT 2019 foi especificamente concebido para se integrar de forma harmoniosa com outras *frameworks*. A sua implementação tornou-se, com esta versão, mais flexível, permitindo que se adapte a solução de gestão à medida das necessidades da organização utilizando o COBIT. (ISACA, 2024)

O COBIT 2019 trouxe mudanças significativas em relação às versões anteriores, substituindo os quatro domínios clássicos (planeamento e organização, aquisição e implementação, entrega e suporte e monitorização e avaliação) por uma estrutura mais flexível baseada em objetivos de administração e de gestão. Estes objetivos, encontram-se agora distribuídos em cinco domínios principais:

a) Domínio da Administração – Representado por "Avaliar, Dirigir e Monitorizar" (EDM) que inclui atividades de supervisão estratégica;
b) Domínio da Gestão – Representado por cinco pilares: "Alinhar, Planear e Organizar (APO), focado no planeamento estratégico, "Construir, Adquirir e Implementar (BAI) que trata do desenvolvimento e aquisição de soluções, "Entregar, Servir e Suportar" (DSS), relacionado à prestação de serviços e "Monitorizar, Avaliar e Medir (MEA), que assegura a medição de desempenho e a conformidade com normas e regulamentos.

d) Center for Internet Security (CIS) Controls

O CIS é uma organização sem fins lucrativos que fornece orientações, boas práticas e ferramentas para as organizações. Os *CIS Controls* são um conjunto de práticas de segurança da informação recomendadas para ajudar as organizações a protegerem as suas redes e sistemas contra as ameaças. (CIS, 2024)

A estrutura do *CIS Controls* contempla 18 controlos:

1. Controlo e inventário de ativos de *hardware;*
2. Controlo e inventário de ativos de *software;*
3. Proteção de dados.
4. Configuração segura de ativos empresariais e *software*
5. Gestão de contas
6. Gestão de controlo de acessos
7. Gestão contínua de vulnerabilidades
8. Gestão de registos de auditoria
9. Proteções para *email* e navegadores *web*
10. Defesas contra *malware*
11. Recuperação de dados
12. Gestão da infraestrutura de rede
13. Monitorização e defesa de rede
14. Consciencialização e formação em segurança
15. Gestão de fornecedores de serviços

16. Segurança na utilização do software
17. Resposta e gestão de incidentes
18. Testes e exercícios de penetração.

Estas *frameworks* fornecem uma série de procedimentos e boas práticas a serem adotadas na implementação da Segurança da Informação, com base no modelo de negócio e dimensão das organizações.

Contudo, no contexto específico das Instituições de Ensino Superior (IES), torna-se essencial distinguir entre os diferentes *frameworks* disponíveis, atendendo à sua aplicabilidade e adequação às particularidades deste setor.

Tabela 6 - Tabela comparativa dos frameworks

Características	ISO/IEC 27000	NIST-CSF	COBIT	CIS Controls
Principal Objetivo	Segurança da Informação	Cibersegurança	Gestão de TI	Práticas específicas de cibersegurança
Abordagem	Prescritiva	Flexível e adaptável	Baseada em processos e objetivos de negócio	Técnica e Operacional
Certificação	Sim	Não	Não (Apenas é possível a certificação para profissionais e não para organizações)	Não
Público-Alvo	Organizações	Infraestruturas críticas	Gestores e decisores	Equipas Operacionais
Níveis de maturidade	Não definidos	Sim (5 níveis)	Sim (modelo de maturidade COBIT)	Sim (IG1, IG2, IG3 - Implementation Groups)
Aplicabilidade em IES	Elevada, usada como referência estruturante	Elevada, flexível e adaptável	Média, com foco mais forte em alinhamento de TI	Elevada, útil para guias rápidos e técnicos

Fonte: ISO/IEC 27001:2022; ISO/IEC 27002:2022; NIST Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1 (2018); COBIT 2019 Framework: Governance and Management Objectives e CIS Critical Security Controls v8 (2021)

Todos os referenciais elencados neste subcapítulo têm como principal objetivo o reforço da segurança da informação nas organizações, no entanto apresentam diferenças significativas na sua aplicação prática.

As principais diferenças entre a ISO/IEC 27000 e o NIST-CSF, podem ser sintetizadas em quarto principais aspetos: a) ISO/IEC 27000 enfatiza principalmente a segurança da informação, enquanto o NIST-CSF adota uma abordagem mais ampla, abrangendo adicionalmente a cibersegurança; b) A natureza prescritiva do ISO/IEC 27000 envolve requisitos específicos para certificação, enquanto o NIST-CSF oferece

flexibilidade, permitindo programas de cibersegurança personalizados; c) ISO/IEC 27000 fornece certificação por meio de organismos terceiros, enquanto o NIST-CSF não possui um processo formal de certificação e d) em termos de níveis de maturidade, o ISO/IEC 27000 não define níveis, enquanto o NIST-CSF descreve cinco níveis, oferecendo uma abordagem mais detalhada para o desenvolvimento de programas (Amine et al, 2023).

De acordo com PrivacyEngine (2023) a ISO/IEC 27001 está mais centrada na criação e implementação de um SGSI e abrange uma vasta gama de controlos de segurança, incluindo segurança física, segurança de recursos humanos, gestão de ativos, controlo de acesso, entre outros. Esta normal exige, igualmente, que as organizações se submetam a auditorias e avaliações regulares para garantir a conformidade com a norma. Por outro lado, e ainda segundo o mesmo organismo, o NIST CSF oferece uma estrutura mais flexível, permitindo que as organizações escolham o nível de maturidade da cibersegurança que se alinha com as suas necessidades específicas e apetência pelo risco.

Relativamente aos CIS Controls, segundo Prey Project (2023), e comparativamente aos restantes *frameworks* estes oferecem uma abordagem prática e direta à cibersegurança, facilitando implementação de medidas eficazes de segurança, uma vez que se focam em passos concretos e boas práticas, o que permite alocar os recursos de forma eficiente e a concentrar os esforços nos controlos mais impactantes, garantindo, assim, proteção máxima contra riscos de cibersegurança. Para além disso, os CIS Controls são atualizados regularmente com base no contributo de uma comunidade diversificada de especialistas, profissionais e organizações de cibersegurança, o que garante que os controlos se mantêm relevantes e eficazes face a novas ameaças e desafios.

De acordo com Advisera (2019), o COBIT é um referencial abrangente que se foca na gestão das TI e não apenas na segurança numa organização. Este referencial abrange todos os controlos, medidas e processos relacionados com as tecnologias da informação. Inclui controlos, métricas e modelos de maturidade, e apoia a definição de responsabilidades e a avaliação do desempenho organizacional. A ISO/IEC 27001, por outro lado, é uma norma internacional e o seu foco está na realização de uma avaliação de riscos e na aplicação de controlos de segurança específicos para proteger os ativos de informação críticos da organização. Deste modo, o referido estudo indica que caso o

principal objetivo da organização seja a proteção dos seus ativos de informação através da implementação de controlos de segurança apropriados e relevantes, a norma ISO/IEC 27001 é a escolha mais indicada. No entanto, se a prioridade da organização for a adoção de um modelo de gestão das TI que auxilie os responsáveis e gestores dos processos de negócio na otimização de processos, potenciando, desta forma, o valor entregue pelas TI e promovendo uma gestão eficaz dos riscos, então o COBIT é o enquadramento mais adequado. (Advisera, 2019)

Apesar das diferenças evidenciadas entre os diferentes referenciais, existem alternativas na sua aplicação nas organizações. Vários autores defendem que a utilização simultânea de dois referenciais pode potenciar a eficácia das medidas de proteção, garantindo, assim, uma maior segurança.

Segundo Leszczyna (2018), de forma a garantir a segurança de uma organização, por vezes, é possível aplicar mais do que uma *framework* na mesma organização ou então a que melhor se adeque à mesma.

Segundo o estudo desenvolvido por Amine et al (2023) a combinação da ISO/IEC 27001 com o NIST-CSF nas IES é considerada a abordagem ideal. Os autores defendem que o NIST-CSF é mais eficaz na estruturação dos domínios de segurança a implementar, enquanto a ISO/IEC 27001 destaca-se no controlo e na conceção de um sistema de gestão da segurança da informação a longo prazo. Ou seja, para os autores a solução mais adequada para a gestão de segurança e risco é adotar a ISO/IEC 27001, definindo simultaneamente os limites com base nas diretrizes do NIST-CSF.

Por outro lado, Prey Project (2023) desenvolveu um estudo em que conclui que para as instituições que têm capacidade para tal, a adoção simultânea de dois referenciais, neste caso concreto NIST-CSF e CIS *Controls* pode oferecer uma proteção mais abrangente.

1.2.9.2 Referenciais e regulamentos aplicados em Portugal no âmbito da cibersegurança

As *frameworks* de cibersegurança são conjuntos de diretrizes e melhores práticas recomendadas para ajudar as organizações a estabelecerem processos eficazes de

segurança e gestão de riscos, sendo voluntárias e flexíveis, podendo ser adaptadas conforme as necessidades específicas de cada entidade. Em contraste, os regulamentos e leis são normas jurídicas obrigatórias, criadas por autoridades governamentais ou entidades reguladoras, que impõem requisitos legais de segurança e proteção, com penalidades previstas para o não cumprimento. Enquanto as *frameworks* orientam a implementação de práticas de segurança, os regulamentos e leis visam garantir a conformidade com padrões legais e a proteção da sociedade e das infraestruturas críticas.

Deste modo, os principais regulamentos e leis relacionados com a cibersegurança em Portugal são:

- *Lei n.º 46/2018 (Lei da Cibersegurança*) – Transposição da Diretiva NIS (Regulamento (UE) 2016/1148), estabelecendo o Regime Jurídico da Cibersegurança em Portugal e criando a Autoridade Nacional de Cibersegurança (CNCS);

A Lei da cibersegurança estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (Diário da República, 2018). Por sua vez, o Decreto-Lei n.º 65/2021 estabelece o regime jurídico da segurança do ciberespaço e define as obrigações relativas à certificação de cibersegurança, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Esta lei estabelece a criação de uma Estratégia Nacional de Segurança do Ciberespaço, definindo o seu enquadramento, os objetivos e as linhas de ação do Estado nesta área, alinhadas com os interesses nacionais, e, por conseguinte, designa a estrutura nacional de segurança do ciberespaço, incluído a criação de:

- Conselho Superior de Segurança do Ciberespaço;
- Centro Nacional de Cibersegurança;
- Equipa de Resposta a Incidentes de Segurança Informática Nacional – CERT.PT;

- Notificação de Incidentes e Notificação Voluntária de Incidentes, para incidentes que podem comprometer a segurança de dados pessoais ou infraestruturas críticas;
- Quadro Nacional de Referência para a Cibersegurança (QNRCS);
- Roteiro para as Capacidades Mínimas de Cibersegurança.

Segundo o CNCS, o Regime Jurídico da Segurança do Ciberespaço aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente, no âmbito da notificação voluntária de incidentes.

Dado que a Lei n.º 46/2018 constitui a base do regime jurídico da cibersegurança em Portugal, importa destacar que esta legislação foi recentemente atualizada para refletir as exigências da nova Diretiva (UE) 2022/2555 — conhecida como NIS 2. Esta diretiva europeia introduz um conjunto reforçado de medidas destinadas a garantir um nível elevado e comum de cibersegurança em todos os Estados-Membros, com especial foco na gestão de riscos, resposta a incidentes e na responsabilização da gestão de topo. Com a entrada em vigor da Lei n.º 55/2022, que altera a Lei n.º 46/2018, o regime jurídico nacional foi atualizado face às exigências da Diretiva NIS 2, de modo a refletir a necessidade de dar resposta ao aumento do número e da gravidade de ciberataques. Nesse sentido, muitas das obrigações previstas na NIS 2 já estão em vigor em Portugal, nomeadamente no que se refere à definição de responsabilidades claras em matéria de cibersegurança, à implementação de medidas de gestão de risco, à obrigatoriedade de notificação de incidentes e ao fortalecimento da capacidade de resposta e recuperação das entidades abrangidas.

Todavia, encontra-se em tramitação na Assembleia da República a Proposta de Lei n.º 50/XVI/1, que tem como objetivo a introdução de obrigações adicionais e mais exigentes para as entidades consideradas essenciais e importantes, incluindo as IES, sempre que estas cumpram os critérios definidos na legislação (como dimensão, impacto no funcionamento da sociedade ou na economia). A proposta reforça, entre outros aspetos:

- A responsabilidade da gestão de topo na implementação das políticas de cibersegurança;
- A obrigatoriedade de planos de continuidade de negócio e de resposta a incidentes;
- A supervisão por parte do Centro Nacional de Cibersegurança (CNCS);
- E a necessidade de adoção de medidas técnicas e organizativas robustas, incluindo mecanismos de gestão de risco associados a fornecedores.

- *Regime Geral sobre a Proteção de Dados (RGPD*) - Regulamento da União Europeia (UE) que estabelece regras para a proteção de dados pessoais e a privacidade dos cidadãos da UE, impondo obrigações de segurança no tratamento de dados pessoais;

Com a entrada em vigor do Regulamento Geral de Proteção e Dados, a 25 de maio de 2018, foram estabelecidas regras e exigências no que respeita à proteção das pessoas singulares, nomeadamente no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE. Estas novas exigências resultam da publicação do Regulamento (UE) 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016, e subsequente publicação da Lei n.º 58/2019 em Diário da República que assegura a implementação do regulamento na ordem jurídica nacional.

De acordo com o RGPD, as IES têm responsabilidade de implementar um conjunto de práticas e políticas de cibersegurança, visando garantir a proteção de dados pessoais. Estas medidas devem assegurar a confidencialidade, integridade e disponibilidade dos dados, conforme exigido pelo regulamento, de forma a prevenir acessos não autorizados, alterações ou destruição indevida dos mesmos.

Em Portugal a autoridade de controlo nacional para efeitos do RGPD e da legislação associada é a Comissão Nacional de Proteção de Dados (CNPD). De acordo com o artigo 4.º n.º 2 da Lei 58/2019, a CNPD tem a função de controlar e fiscalizar o cumprimento do RGPD, bem como das demais disposições legais e regulamentares em matéria de

proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

Esta nova lei "*aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público (...)"*.

No que diz respeito às instituições de ensino superior públicas, estas encontram-se elencadas no artigo 12.º n.º 2, sendo obrigatória a designação de um encarregado de proteção de dados, cujas funções são, de acordo com o artigo n.º 11:

"*a) assegurar a realização de auditorias, quer periódicas, quer não programadas;*

b) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável de segurança;

c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados."

Para além da Lei n.º 58/2019, surge a Diretriz n.º 1/2018 que visa a delimitação da disponibilização de dados pessoais de estudantes, dos docentes e demais trabalhadores no sítio da Internet das IES, de modo a fazer face à utilização generalizada da Internet pelas instituições de ensino superior.

Estas legislações, embora complementares, abordam diferentes dimensões da segurança e proteção da informação. Enquanto o RGPD é aplicável a todas as entidades que tratem de dados pessoais, a Lei da Cibersegurança aplica-se a entidades que operam com redes e sistemas de informação, com foco específico na cibersegurança.

1.2.9.3 Legislação e normativos aplicados às IES no âmbito da proteção de dados e cibersegurança

As IES em Portugal, sejam públicas ou privadas, devem cumprir um conjunto de regulamentações e legislações no âmbito da cibersegurança e da proteção de dados

pessoais. Independentemente da sua natureza, as IES devem adotar uma abordagem holística e integrada para garantir a segurança da informação. Esta abordagem envolve não apenas a proteção de dados pessoais, mas também a segurança das redes e sistemas de informação, que são essenciais para o funcionamento da instituição.

No caso específico da Lei da Cibersegurança (Lei n.º 46/2018) esta aplica-se a todas a entidades que prestam serviços essenciais, como a educação e formação, e utilizam redes e sistemas de informação que podem ser considerados críticos, especialmente à medida que se expandem para o ensino à distância.

O RGPD, por sua vez, aplica-se a todas as IES no que se refere ao tratamento de dados pessoais de alunos, funcionários e outras partes. Este regulamento estabelece a obrigatoriedade de implementar medidas de segurança adequadas para proteger dados pessoais e notificar as autoridades competentes (CNPD) em caso de violação de dados.

1.2.10 Mecanismos de segurança da informação e boas práticas nas IES

No contexto das IES em Portugal, a implementação de medidas de segurança e a adoção de boas práticas de gestão da informação são fundamentais para garantir a integridade, confidencialidade e disponibilidade dos dados.

Segundo Amine et al (2023) as Instituições de Ensino Superior (IES) devem desenvolver e implementar uma estratégia de cibersegurança global e integrada, equilibrando os objetivos de segurança da informação com os custos associados.

No panorama nacional, o CNCS publicou a 26 de julho de 2019 o **Quadro Nacional de Referência para a Cibersegurança**, onde são descritas um conjunto de medidas de segurança que se traduzem em objetivos específicos.

De acordo com o CNCS, o QNRCS “constitui um conjunto de recomendações para que as organizações possam definir uma estratégia de cibersegurança que envolva toda a sua estrutura” e “disponibiliza as bases para que qualquer entidade possa cumprir os requisitos mínimos de segurança das redes e sistemas de informação por meio da implementação de medidas de Identificação, Proteção, Deteção, Resposta e Recuperação

contra ameaças que colocam em causa a segurança do ciberespaço, reduzindo assim o risco associado".

O QNRCS foi desenvolvido pelo CNCS tendo por base referenciais internacionalmente reconhecidos (ISO/IEC 27001, NIST-CSF, os Controlos do CIS e o COBIT). Estes referenciais abordam de forma complementar a segurança da informação, a cibersegurança e as boas práticas de gestão. O QNRCS adapta esses referenciais ao contexto nacional, proporcionando uma estrutura sólida e alinhada com as melhores práticas globais, garantindo a proteção de sistemas críticos, como os utilizados nas instituições de ensino superior, e assegurando uma gestão eficaz da segurança da informação no país.

O QNRCS comtempla um conjunto de medidas de segurança que se traduzem cinco objetivos específicos: Identificar, Proteger, Detetar, Responder e Recuperar, conforme figura 13:

Figura 13 - Objetivos de segurança segundo o QNRCS

Fonte: Adaptado de *Quadro Nacional de Referência para a Cibersegurança*, do Centro Nacional de Cibersegurança, 2019, consultado em https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

De forma mais específica, os cinco objetivos centrais da cibersegurança correspondem às seguintes temáticas:

- Identificar: envolve a compreensão do contexto organizacional e dos riscos associados, permitindo a definição de estratégias eficazes.
- Proteger: foca-se na implementação de medidas para assegurar a entrega de serviços críticos, abrangendo o controlo de acessos, a proteção de dados e a segurança física e lógica.
- Detetar: visa identificar precocemente incidentes de segurança.
- Responder: consiste na aplicação de ações para mitigar impactos adversos, reduzindo danos.
- Recuperar: assegura a resiliência organizacional, garantindo a continuidade das operações após um incidente.

Os objetivos encontram-se estruturados em categorias e subcategorias, integrando medidas de implementação técnica e processual, bem como evidências de implementação que permitam às organizações fortalecer a sua proteção e melhorar a resposta aos desafios da segurança da informação.

Segundo o CNCS, as medidas de segurança pretendem suportar as organizações no processo de sistematização da sua estratégia de gestão do risco de cibersegurança e "simplificam o processo de organização da informação, a tomada de decisão no âmbito da gestão do risco e o endereçamento de ameaças e fomentam a melhoria contínua recorrendo a lições aprendidas no âmbito de atividades realizadas". Estas medidas de segurança dividem-se pelos em cinco grandes objetivos supramencionados (Identificar, Proteger, Detetar, Responder e Recuperar), detalhados em categorias e subcategorias específicas (Apêndice 1 - QNRCS).

O QNRCS foi desenvolvido com base em práticas e normas internacionais reconhecidas, como o COBIT, o CIS CSC, a norma ISO/IEC 27001 e as diretrizes do NIST. A combinação destes referenciais visa a criação de uma abordagem integrada e eficaz para a gestão de cibersegurança em Portugal, alinhada às melhores práticas internacionais e adaptada às necessidades do contexto nacional.

Em Portugal, para além da aplicação do QNRCS nas IES tem-se verificado uma crescente adoção de IES da norma ISO/IEC 27000 em Instituições de Ensino Superior, em particular a ISO/IEC 27001. Esta tendência pode estar diretamente relacionada com a

sua natureza certificável, o seu reconhecimento internacional e à sua estrutura sistematizada, que facilita a implementação de um SGSI. O organismo ENISA (2014), destaca a relevância desta norma em vários contextos, referindo que "especificações como a ISO/IEC 27001 incentivam a adoção de uma estrutura organizacional padronizada, o que facilita a compreensão, por parte dos clientes, de como funcionam os processos e reduz também os custos associados a auditorias e diligências devidas. Isto deve-se, em grande parte, ao facto de estas normas organizacionais fornecerem um modelo para a implementação de um sistema de gestão da segurança, bem como um modelo para auditoria e verificação da conformidade de uma organização com as melhores práticas de segurança".

Conforme referido, o QNRCS define um conjunto de medidas e boas práticas que as organizações devem adotar de forma a garantir a proteção dos sistemas e dados. Todavia, apesar da implementação das referidas medidas nas organizações, não existe uma garantia absoluta de proteção. Neste contexto, o seguro de cibersegurança surge como uma solução complementar aos mecanismos de segurança e aos planos eficazes de resposta a incidentes, pois, embora não os substitua nem exclua, também não torna o seguro desnecessário ou redundante (Forbes Portugal, 2022). O seguro de cibersegurança tem sido estudado tanto no contexto do método de transferência de risco, quanto como um mecanismo para motivar a melhoria da cibersegurança (Khalili et al., 2017) Além de cobrir os custos associados a incidentes de cibersegurança, o seguro pode minimizar as perdas empresariais e também pode melhorar a reputação, uma vez que clientes e acionistas se sentem mais seguros ao ver que a empresa possui uma garantia na forma de uma apólice contratada (Balawejder e Ostrowska-Dankiewicz, 2019). Por outro lado, na ausência de mercados de seguros regulamentados ou seguros obrigatórios, a introdução do seguro deteriora a segurança da rede. Isso ocorre porque, ao transferirem parte do seu risco para a seguradora, os agentes segurados podem reduzir os seus níveis de esforço (Khalili et al., 2017).

No artigo da Forbes Portugal, publicado a 11 de fevereiro de 2022, é destacado um estudo desenvolvido pela consultora MDS, que revela que uma percentagem inferior a 1% das empresas portuguesas possuem seguros contra riscos de cibersegurança. No

entanto, o mesmo estudo revela que mais de um terço dos empresários e gestores identificarem o risco de cibersegurança como uma das principais preocupações.

Para além das medidas e boas práticas anteriormente mencionadas, torna-se relevante destacar uma abordagem adicional que pode reforçar a estratégia de cibersegurança nas IES: a avaliação através de modelos de maturidade. Segundo Becker et al (2009) a gestão de TI necessita de ferramentas de apoio que permitam avaliar o estado atual da organização, definir e priorizar medidas de melhoria e, subsequentemente, controlar o progresso da sua implementação.

No presente estudo, a escolha do *Data Governance Maturity Model* da Gartner revela-se mais adequada em comparação com outros modelos de maturidade em cibersegurança. Enquanto modelos de cibersegurança, como o Cybersecurity Maturity Model Certification (CMMC) ou o COBIT, se centram essencialmente em processos técnicos e operacionais de cibersegurança, o Data Governance Maturity Model da Gartner propõe uma abordagem mais holística e integrada. Isto é, este modelo não se limita exclusivamente a aspetos isolados de cibersegurança, abrangendo todos os elementos interdependentes associados à gestão e proteção da informação, como as políticas de utilização de dados, a qualidade e acessibilidade da informação, a conformidade legal, as responsabilidades organizacionais e os mecanismos de segurança da informação.

2 Estudo Empírico

Este capítulo tem como finalidade a apresentação do caso de estudo, dos objetivos que o orientam, bem como a abordagem metodológica adotada. Adicionalmente, são

descritos os procedimentos de recolha de dados utilizados para obter as informações necessárias ao presente estudo.

O presente estudo pretende averiguar a forma como os intervenientes na área da cibersegurança em instituições de ensino superior em Portugal avaliam ao grau de preparação destas entidades para enfrentar desafios e ameaças no domínio da cibersegurança. Para tal, serão explorados aspetos como a existência de políticas formais de segurança, a adoção de práticas de controlo, a gestão dos incidentes e os principais desafios e limitações enfrentados.

Neste seguimento, elencamos os cinco principais objetivos desta investigação:

Objetivo 1 - Avaliar o nível de preparação existente nas Instituições de Ensino Superior em Portugal e a sua capacidade para prevenir, detetar e responder a incidentes de cibersegurança;

Objetivo 2 - Identificar os principais desafios e vulnerabilidades enfrentados pelas Instituições de Ensino Superior em Portugal;

Objetivo 3 - Analisar a existência e a eficácia de políticas e práticas de cibersegurança;

Objetivo 4 - Avaliar a existência de um plano de resposta a ataques e a sua eficácia na mitigação de danos;

Objetivo 5- Recolher perspetivas sobre oportunidades de melhoria e necessidades futuras.

Em síntese, pretende-se evidenciar com o presente estudo a relevância das questões relacionadas com a cibersegurança no setor da educação, com foco particular nas Instituições de Ensino Superior. Estas instituições lidam com grandes volumes de dados sensíveis, incluindo informações pessoais, financeiras e de saúde de alunos e funcionários, além de dados relacionados com a investigação académica e com propriedade intelectual. Dada a natureza crítica destes ativos, torna-se fundamental garantir que as IES implementem medidas adequadas de segurança da informação de forma a proteger os dados contra ameaças.

Este estudo, visa, assim, sensibilizar para a necessidade de uma abordagem estratégica e robusta de cibersegurança nas IES, promovendo a segurança e a integridade da informação num contexto cada vez mais vulnerável a ataques de cibersegurança.

2.1 Metodologia de Investigação

A metodologia utilizada no presente estudo teve como objetivo confrontar os dados obtidos através da realização da revisão de literatura com o contexto operacional das Instituições de Ensino Superior. O estudo empírico seguiu as seguintes fases:

1. Análise de artigos, questionários e estudos relacionados com o tema em investigação;
2. Elaboração do guião da entrevista;
3. Análise das entrevistas e discussão dos resultados obtidos.

2.2 Caracterização da população e processo de seleção dos entrevistados

2.2.1 Caracterização da População

A secção que se insere tem como objetivo caracterizar a população utilizada para análise de dados e consequente processo de seleção para realização de entrevistas.

Em Portugal, e de acordo com os últimos dados disponíveis no site da Direção-Geral de Ensino Superior, doravante, DGES, a distribuição das instituições de ensino superior é organizada num sistema binário que integra o ensino universitário e o ensino politécnico e é ministrado em instituições públicas e privadas (DGES). Por sua vez, o ensino universitário inclui as universidades, os institutos universitários e outros estabelecimentos de ensino universitário e é orientado por uma perspetiva de promoção de investigação e de criação do saber e visa assegurar uma sólida preparação científica e cultural e proporcionar uma formação técnica que habilite para o exercício de atividades profissionais e culturais e fomente o desenvolvimento das capacidades de conceção, inovação e análise crítica. O ensino politécnico compreende os institutos politécnicos e outros estabelecimentos de ensino politécnico e é orientado por uma perspetiva de investigação aplicada e de desenvolvimento, dirigido à compreensão e solução de

problemas concretos e visa proporcionar uma sólida formação cultural e técnica de nível superior, desenvolver a capacidade de inovação e de análise crítica e ministrar conhecimentos científicos de índole teórica e prática e as suas aplicações com vista ao exercício de atividades profissionais.

Tabela 7 - Instituições de ensino superior em Portugal apresentadas por tipo de ensino e natureza

Tipo de Ensino/	Total
Politécnico	**62**
Privado	42
Público	20
Universitário	**36**
Privado	20
Público	16
Total IES	**98**

Fonte: DGES (2025)

Conforme tabela anterior, a população em estudo é composta por 98 instituições de ensino superior. A amostra será selecionada de forma a garantir a diversidade e representatividade dos diferentes tipos de instituições em Portugal.

2.2.2 Técnica de recolha de dados

Quanto à técnica de recolha de dados, a sua escolha assume particular relevância na elaboração de um estudo rigoroso e alinhado com os objetivos da investigação. A seleção do método mais adequado deve ter em conta a natureza da questão em análise, as características da população-alvo, bem como a disponibilidade e os recursos disponíveis.

No contexto do presente estudo, que visa compreender as práticas e os desafios associados à cibersegurança nas instituições de ensino superior foram inicialmente consideradas duas abordagens metodológicas para recolha de dados, nomeadamente as entrevistas e inquéritos. Cada uma destas técnicas apresenta vantagens e limitações específicas.

Todavia, dada a natureza do estudo e a necessidade de obter perceções detalhadas por parte dos intervenientes, optou-se pela utilização da técnica de entrevista como principal método de recolha de dados. Tendo em consideração a necessidade de uniformizar a recolha de dados e de facilitar a posterior comparação entre as respostas, optou-se pela realização de entrevistas estruturadas. Esta escolha permitiu assegurar que todos os intervenientes respondessem às mesmas questões, promovendo, assim, a consistência, a comparabilidade e a fiabilidade dos dados recolhidos sobre a realidade da cibersegurança nas instituições de ensino superior em Portugal.

2.2.3 Processo de seleção dos Entrevistados

Para a realização das entrevistas, optou-se pela seleção por conveniência dos entrevistados, com base na sua disponibilidade e relevância para o estudo. Este é um método aplicação simples e célere, que assenta na escolha dos elementos cujo acesso ou disponibilidade é maior. No entanto, devido ao seu carácter não aleatório e por não haver segurança de que a amostra seja satisfatoriamente representativa da população, os resultados e as conclusões obtidas são unicamente aplicáveis à amostra em questão, não sendo extrapoláveis para a globalidade (Hill & Hill, 2016).

O objetivo foi garantir que amostra abrangesse intervenientes do ensino superior pertencentes a diferentes naturezas institucionais e tipos de ensino, permitindo, deste modo, uma análise comparativa da estrutura e metodologias aplicadas em matérias de cibersegurança. Para tal foram definidos critérios para a seleção dos entrevistados:

i. Interveniente de cibersegurança de uma Instituição de Ensino Superior Público - Universitário
ii. Interveniente de cibersegurança de uma Instituição de Ensino Superior Privado - Universitário
iii. Interveniente de cibersegurança de uma Instituição de Ensino Superior Público - Politécnico
iv. Interveniente de cibersegurança de uma Instituição de Ensino Superior Privado - Politécnico

Não obstante os esforços envidados para assegurar uma amostra e um conjunto de informações obtidas nas entrevistas tão heterogéneos quanto possível, tornou-se necessário ajustar tanto a dimensão como a composição da amostra, de forma a garantir a viabilidade da recolha de dados e a concretização do estudo.

Assim, devido a limitações de disponibilidade e acessibilidade dos potenciais entrevistados, foi apenas possível cumprir dois desses critérios:

i. Interveniente de cibersegurança de uma Instituição de Ensino Superior Público – Universitário

iii. Interveniente de cibersegurança de uma Instituição de Ensino Superior Público - Politécnico

Em síntese, a seleção e definição do tamanho da amostra de entrevistados foram realizadas com base nos dois critérios supramencionados, culminando numa amostra composta por dois intervenientes de instituições de ensino superior.

2.3 Recolha de dados

2.3.1 Elaboração do Guião da Entrevista

A elaboração do guião da entrevista foi iniciada com uma revisão da literatura relacionada sobre a temática da investigação. A partir desta revisão, foram identificadas as questões de maior interesse e que, ao mesmo tempo, se revelaram essenciais para os objetivos do estudo.

Adicionalmente, o guião da entrevista foi fundamentado em modelos de questionários e inquéritos previamente utilizados em investigações semelhantes, tais como:

a) Inquérito à Utilização de Tecnologias da Informação e da Comunicação - Administração Pública Central e Regional (IUTICAP), desenvolvido pela Direção-Geral de Estatísticas da Educação e Ciência (2024).

b) Inquérito para Verificação da Cibersegurança nas Organizações Públicas Municipais em Portugal, desenvolvido por Branco Jr e Fonseca (2022), para simplificação, a partir deste ponto, o mesmo será referido como ICOPM.

Com base na análise destes questionários, procedeu-se à seleção e adaptação de questões consideradas mais relevantes para o presente estudo, as quais foram integradas no guião de entrevistas.

O IUTICAP apresenta um inquérito detalhado sobre a infraestrutura tecnológica e das práticas institucionais na administração pública. Para o presente estudo, foi considerado exclusivamente o Capítulo VII, que aborda as medidas, controlos e procedimentos aplicados em sistemas das TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados e dos sistemas. Este capítulo fornece dados relevantes sobre as práticas de cibersegurança adotadas pelas organizações da administração pública.

O ICOPM, desenvolvido por Branco Jr e Fonseca (2022), aborda as principais lacunas e desafios enfrentados pelas organizações municipais em Portugal.

Considerando a sua aplicabilidade, foram adaptadas algumas questões ao contexto das Instituições de Ensino Superior (IES), as quais foram incluídas no guião da entrevista a realizar aos intervenientes selecionados, com o objetivo de compreender como a proteção e gestão da informação são realizadas nessas instituições em ambientes digitais. A análise detalhada aos inquéritos IUTICAP e ICOPM, permitiu identificar e selecionar 12 questões que se mostraram relevantes para o objetivo da pesquisa, as quais foram adaptadas e integradas no guião de entrevista.

Na tabela seguinte, apresenta-se a correspondência entre as questões incluídas no guião das entrevistas e as questões originais do inquérito IUTICAP e do inquérito ICOPM, de modo a evidenciar a ligação entre os instrumentos de recolha de dados:

Tabela 8 - Correspondência entre as Questões do Guião de Entrevistas e as Questões do Inquérito IUTICAP e ICOPM

Nº Questão	Questões Guião da Entrevista	IUTICAP (Nº Questão)	ICOPM (Nº questão)
2	Descreva brevemente a estrutura de TI e cibersegurança da Instituição? Existe uma equipa dedicada exclusivamente à cibersegurança?	-	1
5	O Organismo tem definida uma estratégia/política para a segurança das redes e da informação? Se sim, já se encontra implementada na Instituição? É revista com que periodicidade?	9	25 e 26
5.1	A mesma encontra-se de acordo com o Regulamento Geral de Proteção de Dados (RGPD) e o Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021?	9.1	
6	De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), a Instituição efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)?	9.2	3 e 41
8	Quais as principais medidas de segurança da informação no controlo de acessos a sistemas e redes? A Instituição possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TI?	4	-
9	A Instituição utiliza alguma das seguintes medidas de segurança: - Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação - Atualização regular do software - Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN) - Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada offline) - Foram definidos métodos apropriados para estabelecer e provar a identidade dos usuários, dispositivos ou sistemas com confiança suficiente para tomar decisões de controle de acesso?	1 b), d), f), k)	Secção VI e VII (71 a 99)
10	Na Instituição existem programas de formação e promoção de boas práticas em cibersegurança regulares (voluntários e obrigatórios, contratuais) para funcionários, docentes e estudantes?	2	40 e 43
11	Na Instituição são realizados testes ou simulações de ataques, como campanhas de phishing, análises de vulnerabilidades e simulações de ransomware?	-	123
12	Na Instituição são realizados testes da segurança informática de intrusão, aos sistemas de alerta e de backup, revisões às medidas de segurança?	1 i)	-
13	A Instituição já sofreu algum incidente de segurança? Se sim, que tipo de incidente, qual o seu impacto para a Instituição e de que forma foi tratado?	7.1	-
14	Na Instituição existe um plano de resposta a incidentes? Se sim, este inclui o Plano de continuidade de negócios, o Plano de contingência, Plano de recuperação em caso de desastre e o Plano de gestão de crise?	-	112 e 123
15	A instituição possui uma apólice de seguro de cibersegurança ou está a ser considerada a possibilidade da sua contratação?	8	-

Fonte: IUTICAP (2024) e ICOPM (2022)

Para além dos inquéritos analisados, foi, igualmente, considerado o Data Governance Maturity Model-Gartner. Este modelo estabelece um enquadramento para avaliar o nível de maturidade das práticas de gestão de dados de uma organização, distribuído por cinco níveis: inicial, em desenvolvimento, definido, gerido e otimizado. A sua aplicação no presente estudo permitiu complementar a análise, proporcionando um referencial para compreender o grau de maturidade das Instituições de Ensino Superior no que se refere à gestão e proteção da informação.

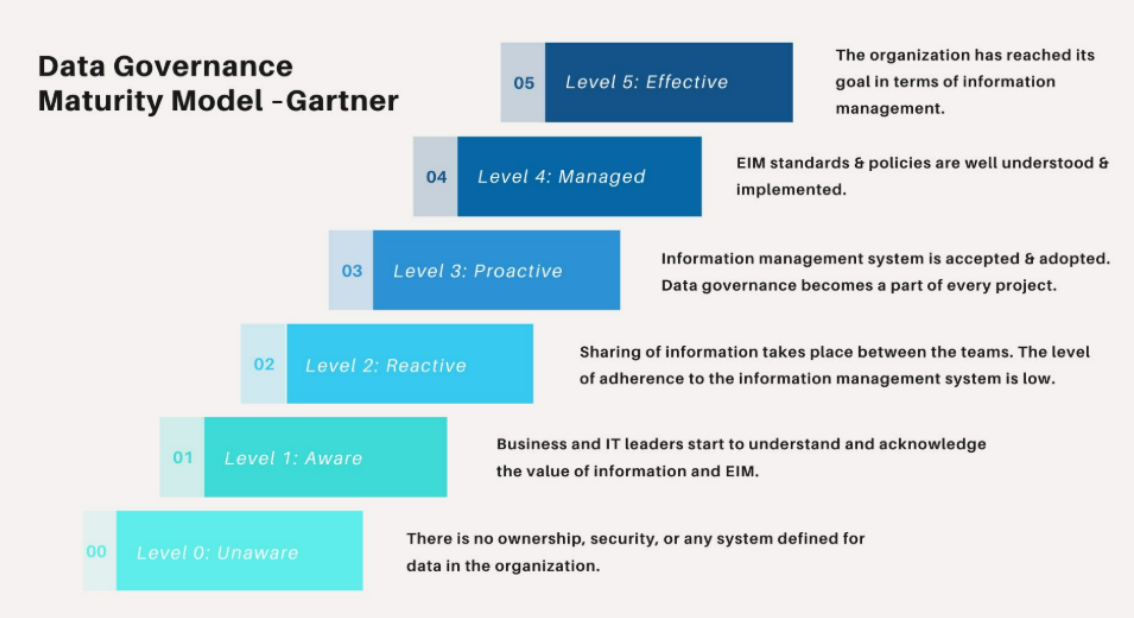

Figura 14 - Data Governance Maturity Model-Gartner

Fonte: Adaptado de *Data and Analytics Maturity Score for CDAOs*, por Gartner, 2025, https://www.gartner.com/en/data-analytics/research/data-analytics-maturity-score

Com base no referido modelo, foi desenvolvida a seguinte questão para integrar no guião de entrevistas, com o intuito de avaliar o nível de maturidade em gestão de dados que os intervenientes consideravam ter na sua IES à data da pesquisa:

Tabela 9 - Correspondência entre as Questões do Guião de Entrevistas e o Modelo de Maturidade de Cibersegurança da Gartner

Nº Questão	Questões Guião da Entrevista
17	Como classificaria o nível de maturidade da cibersegurança na sua Instituição de acordo com o Modelo de Maturidade de Cibersegurança da Gartner? Nível 1: Inicial: Não existe uma estratégia clara de cibersegurança. Nível 2: Reativo: A segurança é reativa, com principal foco em resolver problemas à medida que surgem. Nível 3: Definido: A segurança é bem definida e incorporada nos processos organizacionais. Nível 4: Gerido: A segurança é gerida de forma proativa com processos bem estabelecidos. Nível 5: Otimizado: A segurança é integrada de forma contínua na cultura organizacional e melhorada constantemente.

Fonte: Gartner (2025)

Para além dos inquéritos analisados, foram integradas no guião de entrevistas quatro questões de elaboração própria, desenvolvidas com o objetivo de aprofundar áreas específicas os questionários previamente considerados não abordaram de forma direta. A

elaboração destas questões resultou da identificação, ao longo da elaboração da revisão da literatura, de temas particularmente relevantes tendo em conta os objetivos da presente investigação.

Tabela 10 - Questões do Guião de Entrevistas de elaboração própria

Nº Questão	Questões Guião da Entrevista
3	Considera que a cibersegurança é uma prioridade na instituição? Porquê?
4	Na sua opinião quais são os principais desafios que a sua instituição e/ou o setor do ensino enfrentam em termos de cibersegurança atualmente?
7	Na Instituição são aplicados algumas destas normas ou frameworks de segurança: ISO 27001, NIST, COBIT, CIS? Quais? Como é garantido o seu cumprimento?
16	Na sua opinião existe necessidade de melhorar a Cibersegurança na sua Instituição? Se sim quais são os medidas e estratégias futuras que poderão a vir a ser implementadas na sua Instituição?

Fonte: Elaboração própria.

No apêndice 2 deste estudo, é apresentado o guião de entrevista. Como apresentado neste capítulo, o guião foi desenvolvido com base na revisão de literatura e na análise de inquéritos supramencionados. Com o intuito de evidenciar a correspondência entre as questões do guião de entrevistas e os objetivos definidos para a investigação, elaborou-se uma tabela em que se apresentam todas as questões formuladas, associadas ao respetivo objetivo a que dizem respeito (apresentados no capítulo 2):

Tabela 11 - Comparação entre as questões Guião da Entrevista com os objetivos do Estudo

Nº Questão	Questões Guião da Entrevista	Objetivos do Estudo
2	Descreva brevemente a estrutura de TI e cibersegurança da Instituição? Existe uma equipa dedicada	1
3	Considera que a cibersegurança é uma prioridade na instituição? Porquê?	1
4	Na sua opinião quais são os principais desafios que a sua instituição e/ou o setor do ensino enfrentam em termos de cibersegurança atualmente?	2
5	O Organismo tem definida uma estratégia/política para a segurança das redes e da informação? Se sim, já se encontra implementada na Instituição? É revista com que periodicidade?	3
5.1	A mesma encontra-se de acordo com o Regulamento Geral de Proteção de Dados (RGPD) e o Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021?	3
6	De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), a Instituição efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança,	3
7	Na Instituição são aplicados algumas destas normas ou frameworks de segurança: ISO 27001, NIST, COBIT, CIS? Quais? Como é garantido o seu cumprimento?	1
8	Quais as principais medidas de segurança da informação no controlo de acessos a sistemas e redes? A Instituição possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou	3
9	A Instituição utiliza alguma das seguintes medidas de segurança: - Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação - Atualização regular do software - Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN) - Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada offline) - Foram definidos métodos apropriados para estabelecer e provar a identidade dos usuários, dispositivos ou sistemas com confiança suficiente para tomar decisões de controle de acesso?	3
10	Na Instituição existem programas de formação e promoção de boas práticas em cibersegurança regulares (voluntários e obrigatórios, contratuais) para funcionários, docentes e estudantes?	3
11	Na Instituição são realizados testes ou simulações de ataques, como campanhas de phishing, análises de vulnerabilidades e simulações de ransomware?	4
12	Na Instituição são realizados testes da segurança informática de intrusão, aos sistemas de alerta e de backup, revisões às medidas de segurança?	4
13	A Instituição já sofreu algum incidente de segurança? Se sim, que tipo de incidente, qual o seu impacto para a Instituição e de que forma foi tratado?	4
14	Na Instituição existe um plano de resposta a incidentes? Se sim, este inclui o Plano de continuidade de negócios, o Plano de contingência, Plano de recuperação em caso de desastre e o Plano de gestão de crise?	4
15	A instituição possui uma apólice de seguro de cibersegurança ou está a ser considerada a possibilidade da	3
16	Na sua opinião existe necessidade de melhorar a Cibersegurança na sua Instituição? Se sim quais são os medidas e estratégias futuras que poderão a vir a ser implementadas na sua Instituição?	5
17	Como classificaria o nível de maturidade da cibersegurança na sua Instituição de acordo com o Modelo de Maturidade de Cibersegurança da Gartner? Nível 1: Inicial: Não existe uma estratégia clara de cibersegurança. Nível 2: Reativo: A segurança é reativa, com principal foco em resolver problemas à medida que surgem. Nível 3: Definido: A segurança é bem definida e incorporada nos processos organizacionais. Nível 4: Gerido: A segurança é gerida de forma proativa com processos bem estabelecidos. Nível 5: Otimizado: A segurança é integrada de forma contínua na cultura organizacional e melhorada constantemente.	Todos

Fonte: Elaboração Própria

2.3.2 Descrição da Amostra e Metodologia das Entrevistas

Conforme descrito anteriormente, os dados do presente estudo foram recolhidos por meio de entrevistas individuais com intervenientes de cibersegurança de Instituições de

Ensino Superior. As entrevistas foram realizadas entre março e abril de 2025, com os convites enviados por telefone, WhatsApp e e-mail, juntamente com o agendamento das mesmas.

Foram contactadas 11 Instituições de ensino superior, das quais duas aceitaram participar na pesquisa, mostrando disponibilidade para colaborar no desenvolvimento do estudo, conforme tabela 13:

Tabela 12 - Visão geral dos Intervenientes de IES contactados no âmbito das Entrevistas

Instituição	Natureza da Instituição	Tipo de Ensino	Entrevista	Data da Entrevista
I1	Público	Politécnico	Não	N/A
I2	Público	Universitário	Não	N/A
I3	Público	Politécnico	Não	N/A
I4	Público	Politécnico	Não	N/A
I5	Público	Politécnico	Sim	20/03/2025
I6	Público	Universitário	Sim	31/03/2025
I7	Público	Universitário	Não	N/A
I8	Privado	Universitário	Não	N/A
I9	Privado	Universitário	Não	N/A
I10	Privado	Universitário	Não	N/A
I11	Público	Politécnico	Não	N/A

Fonte: Elaboração Própria

As entrevistas foram realizadas via Zoom, com uma duração média de aproximadamente 25 minutos. As entrevistas foram realizadas exclusivamente entre o investigador e o entrevistado, gravadas em áudio, sendo o investigador responsável por esclarecer a natureza confidencial das gravações, destinadas apenas ao processamento de dados, sem qualquer objeção por parte dos entrevistados.

As entrevistas foram estruturadas em três fases distintas. Na primeira fase, procedeu-se à apresentação dos objetivos do estudo, bem como à explicação dos princípios éticos e legais aplicáveis, nomeadamente no que respeita à confidencialidade e à utilização dos dados recolhidos. A segunda fase correspondeu à condução da entrevista, durante a qual foram colocadas as questões previamente estruturadas no guião de entrevista (Apêndice 2). Por fim, a terceira fase das entrevistas consistiu no agradecimento pela participação.

2.4 Análise das Entrevistas e Discussão dos Resultados

Nesta secção procede-se à análise dos dados obtidos através das entrevistas estruturadas realizadas junto dos responsáveis pela cibersegurança em duas IES. O principal objetivo consiste na identificação dos principais desafios enfrentados pelas IES no que diz respeito à cibersegurança, assim como das estratégias e práticas adotadas para mitigar esses desafios. A discussão dos resultados tem como principal objetivo analisar e confrontar as evidências empíricas obtidas nas entrevistas com os fundamentos teóricos previamente expostos na revisão de literatura, bem como obter uma compreensão mais ampla da realidade da cibersegurança no Ensino Superior, destacando os pontos fortes, as lacunas existentes e as oportunidades para melhoria.

Questão 1: Apresentação dos Entrevistados

A primeira questão teve como objetivo contextualizar os entrevistados, recolhendo informações relativas à sua função, tempo de serviço na instituição e experiência profissional no domínio da cibersegurança.

Questão 1.1. Descrição do papel que assume na instituição e que tipo de Instituição.

Relativamente às funções exercidas, o entrevistado I5 indicou que leciona na instituição desde 2006, exercendo cumulativamente as funções de responsável pelo Sistema de Informação de Segurança da Organização (SISO) e de coordenador da equipa de resposta a incidentes de cibersegurança.

Por sua vez, o entrevistado I6, que representa uma instituição pública de ensino universitário, é responsável por várias unidades curriculares nas áreas da segurança da informação e da cibersegurança. Desempenha, ainda, funções de Pró-Reitor para a Universidade Digital, coordena o Gabinete de Cibersegurança e Proteção de Dados, e assume o cargo de Encarregado da Proteção de Dados (EPD) da instituição.

Questão 1.2. Há quanto tempo trabalha na Instituição?

Verifica-se que ambos os entrevistados possuem um percurso profissional prolongado nas respetivas instituições, com aproximadamente 19 anos (I5) e 14 anos (I6)

de experiência profissional. Este fator revela um conhecimento aprofundado sobre o funcionamento interno das IES, bem como uma familiaridade significativa com os desafios e práticas relacionadas à segurança da informação. A sua permanência prolongada nas organizações permite-lhes ter uma visão histórica e estratégica da evolução das políticas e infraestruturas de cibersegurança ao longo do tempo, conferindo robustez e relevância às perceções partilhadas durante as entrevistas.

Questão 1.3. Desenvolve funções relacionadas com a tecnologia e segurança da informação?

Ambos os entrevistados responderam perentoriamente à questão apresentada, referindo que trabalham diretamente em funções relacionadas com tecnologia e segurança da informação nas respetivas instituições.

Questão 1.4. Qual é a sua experiência profissional relacionada com a cibersegurança?

O entrevistado I5 é coordena a equipa de Resposta a Incidentes de Segurança Informática da sua instituição, onde também assume a direção de cursos na área da Cibersegurança e coordena o respetivo Centro de Competências em Cibersegurança. Para além destas funções, desenvolve investigação científica no domínio da segurança informática.

Por sua vez, o entrevistado I6 possui igualmente uma vasta experiência na área, tendo desenvolvido todo o seu percurso académico no domínio da segurança da informação e da cibersegurança. Para além disso, e conforme previamente mencionado, exerce funções como responsável pelo Gabinete de Cibersegurança e Proteção de Dados da sua instituição, dedica-se à investigação científica na área e integra comités científicos de revistas e conferências internacionais especializadas em cibersegurança.

Com base nas respostas à primeira questão, podemos concluir que os entrevistados possuem uma vasta experiência, tanto no contexto das suas organizações quanto no domínio da cibersegurança.

Questão 2. Descreva brevemente a estrutura de TI e cibersegurança da Instituição? Existe uma equipa dedicada exclusivamente à cibersegurança?

Relativamente a esta questão, o entrevistado I5 referiu que, na instituição onde exerce funções, existe uma equipa exclusivamente dedicada à cibersegurança, que integra uma equipa de resposta a incidentes (CSIRT), inserida na rede nacional CSIRT.

O entrevistado I6 refere que na instituição onde exerce funções existe uma equipa dedicada à cibersegurança, formalmente integrada na rede nacional CSIRT. Esta equipa é composta por diversos elementos, incluindo um representante que integra a comissão da própria rede CSIRT. O entrevistado I6 destaca ainda, que se trata de uma equipa multifacetada, que reúne estudantes de mestrado e doutoramento em Engenharia Informática, técnicos do serviço de informática e docentes da instituição.

Tendo em conta o aumento da complexidade das ciberameaças e a crescente digitalização das operações empresariais tornaram ainda mais evidente a necessidade de uma abordagem especializada e proativa na gestão da segurança digital. Assim, a existência de equipas exclusivamente dedicadas à cibersegurança revela-se cada vez mais indispensável nas instituições. Estas equipas, são, normalmente, compostas por profissionais especializados, e têm a responsabilidade de monitorizar, identificar e mitigar riscos, implementar políticas de segurança e responder eficazmente a incidentes. Além disso, a implementação de regulamentos como a Diretiva NIS 2 reforçou a exigência de práticas de segurança mais rigorosas, tornando a presença de equipas dedicadas não apenas uma vantagem estratégica, mas também uma obrigação legal para muitas organizações.

A integração de ambas as instituições na Rede Nacional de CSIRTs constitui um fator fundamental para aumentar a eficácia na resposta a incidentes de cibersegurança. Em Portugal, o CERT.PT coordena esta rede, permitindo a colaboração entre entidades públicas e privadas no tratamento de ameaças e vulnerabilidades emergentes. A adesão a esta rede facilita a troca de informações críticas, o que permite a deteção precoce de incidentes e a adoção de medidas preventivas mais eficazes. Além disso, a partilha de melhores práticas e conhecimento especializado entre os membros contribui para a melhoria contínua das capacidades de resposta a incidentes de segurança, aumentando a

eficácia na mitigação de riscos. Este esforço conjunto não só permite uma gestão mais eficiente dos incidentes, como também assegura o cumprimento de obrigações legais, como o RGPD. Desta forma, a integração nesta rede não só beneficia a segurança de uma organização, mas também contribui para o fortalecimento da cibersegurança nacional, criando uma rede colaborativa e resiliente contra as ciberameaças.

Questão 3. Considera que a cibersegurança é uma prioridade na instituição? Porquê?

Ambos os entrevistados reconheceram, de forma inequívoca, que a cibersegurança constitui uma prioridade nas respetivas instituições. No caso do entrevistado I6, a instituição que representa criou um cargo dedicado exclusivamente à segurança da informação, refletindo a importância desta área no seio da instituição.

Este reconhecimento é particularmente relevante, uma vez que se traduz num maior compromisso com o reforço das medidas de proteção e na implementação de políticas internas mais rigorosas, bem como na sensibilização junto dos colaboradores para os riscos e boas práticas no domínio digital. A valorização da cibersegurança por parte das lideranças demonstra uma crescente consciência da criticidade deste tema no contexto atual, nomeadamente nas IES, em que a salvaguarda da informação e a continuidade dos serviços dependem, cada vez mais, da resiliência face às ciberameaças.

Questão 4. Na sua opinião quais são os principais desafios que a sua instituição e/ou o setor do ensino enfrentam em termos de cibersegurança atualmente?

O entrevistado I5 destacou uma das particularidades das IES no que diz respeito à cibersegurança: a necessidade de conciliar diferentes domínios de segurança dentro da mesma organização. Por um lado, o domínio associado à investigação e ao ensino caracteriza-se por uma maior abertura ao nível dos acessos e da liberdade de utilização dos sistemas, promovendo a partilha de conhecimento e a colaboração académica. Por outro lado, a vertente administrativa, que assegura o funcionamento quotidiano da instituição, exige políticas de segurança mais restritivas e controladas, dada a sensibilidade dos dados e processos envolvidos. Este dualismo cria um desafio

significativo, uma vez que os mesmos utilizadores — docentes, investigadores ou funcionários — podem atuar em ambos os domínios, exigindo um equilíbrio delicado entre flexibilidade e segurança. Assim, o maior desafio reside na própria natureza das IES, que, por definição, devem manter-se instituições abertas à aprendizagem e à investigação, sem comprometer a proteção da informação e dos sistemas.

O entrevistado I6 reconhece que os desafios enfrentados no contexto da cibersegurança são de natureza macro, abrangendo aspetos estruturais e financeiros significativos. Um dos principais desafios identificados é a dificuldade em atrair recursos humanos altamente especializados, uma vez que o setor público não oferece salários tão competitivos quanto o setor privado, especialmente em áreas como a cibersegurança, onde a procura por profissionais qualificados é elevada. Este cenário limita a capacidade de recrutamento de profissionais com as competências necessárias para enfrentar as crescentes ciberameaças. Além disso, o entrevistado destaca a limitação orçamental como outro desafio relevante, uma vez que os recursos financeiros disponíveis não permitem à instituição adquirir todo o equipamento e as licenças necessárias para garantir um nível ideal de cibersegurança.

De acordo com a revisão de literatura realizada, observa-se uma correlação entre os desafios identificados pelos entrevistados e as vulnerabilidades descritas na seção 1.2.7 da revisão de literatura. Para além da escassez de recursos humanos altamente qualificados, que é um desafio recorrente nas Instituições de Ensino Superior (IES), destaca-se também a limitação orçamental, que restringe a capacidade de investimento adequado em cibersegurança.

Conforme indicado por FireEye, Inc. (2015), as IES frequentemente enfrentam dificuldades em atrair e reter profissionais especializados, devido à discrepância salarial existente em relação ao setor privado. No que diz respeito às limitações orçamentais, ao definirem as suas prioridades de despesa, os administradores tendem a privilegiar, em muitos casos, as iniciativas académicas e de investigação em detrimento dos investimentos necessários em cibersegurança.

Relativamente à natureza aberta das IES, que, por estarem orientadas para a aprendizagem e investigação, adotam políticas de segurança mais flexíveis, observa-se

que essa abertura pode gerar vulnerabilidades. Segundo EDUCAUSE (2018), as instituições encontram dificuldades na implementação de políticas de segurança eficazes, uma vez que é necessário equilibrar a liberdade de acesso com a proteção das suas infraestruturas e dados sensíveis.

Questão 5. O Organismo tem definida uma estratégia/política formal para a segurança das redes e da informação? Se sim, encontra-se implementada na Instituição? É revista com que periodicidade?

O entrevistado I5 afirmou que a instituição que representa possui uma política formal definida e implementada para a segurança das redes e dos sistemas de informação, a qual é revista, pelo menos, uma vez por ano, bem como sempre que tal se revele necessário no âmbito da resposta a incidentes. Refere ainda que a instituição adota a *framework* do NIST como referência para a definição e implementação das suas práticas de cibersegurança. Acrescenta que, dada a maturidade do CSIRT da instituição, é obrigatória a incorporação sistemática das lições aprendidas, sempre que ocorrem incidentes, alterações legislativas ou são identificados novos pontos críticos no processo de resposta. Salienta, ainda, que, por integrarem a Rede Nacional de CSIRTs e possuírem um protocolo de colaboração com o CNCS, podem surgir necessidades de ajustamento decorrentes de orientações ou diretrizes emanadas a nível central.

O entrevistado I6 reconhece a existência de diversos procedimentos e práticas relacionados com a segurança da informação na instituição. No entanto, sublinha que estes se encontram atualmente dispersos por diferentes documentos, carecendo de consolidação numa política institucional formal, estruturada e integrada. Ainda que alguns desses procedimentos estejam documentados, não existe, até ao momento, um documento único que defina de forma sistemática a política de segurança da informação. Não obstante, o entrevistado destaca que a elaboração dessa política constitui um dos objetivos estratégicos da instituição a curto ou médio prazo.

Questão 5.1. A mesma encontra-se de acordo com o Regulamento Geral de Proteção de Dados (RGPD) e o Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021?

Ambos os entrevistados confirmam que as políticas de segurança implementadas nas suas instituições estão em conformidade com o RGPD e o RJSC No entanto, o entrevistado I5 demonstra alguma expectativa e incerteza relativamente à aplicação da diretiva NIS 2. Referindo que, apesar de a proposta ter sido submetida à Assembleia da República, esta não foi ainda aprovada, o que deixa as IES numa situação ambígua. Estas foram inicialmente enquadradas numa categoria que pressupõe a emissão de orientações por parte do CNCS. No entanto, o entrevistado salienta que o CNCS se encontra limitado na sua atuação, uma vez que não pode emitir diretrizes vinculativas com base numa legislação que ainda não se encontra formalmente em vigor. Esta indefinição legislativa gera, assim, incerteza quanto às obrigações específicas das IES no âmbito da nova diretiva europeia.

Questão 6. De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), a Instituição efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)?

Os entrevistados I5 e I6 afirmam que as suas instituições cumprem integralmente as obrigações legais associadas à cibersegurança. O entrevistado I6 destaca que, no que se refere às obrigações periódicas a entidade cumpre integralmente as obrigações legais associadas, dispondo de um ponto de contacto formalmente designado para a cibersegurança, bem como de um Encarregado de Proteção de Dados devidamente identificado e comunicado à autoridade competente. Refere, ainda que a instituição elabora e submete anualmente o relatório previsto relatório anual de cibersegurança previsto no artigo 25.º da Lei n.º 46/2018, alterada pelo Decreto-Lei n.º 65/2021, que estabelece o RJSC. Além disso, é assegurada a atualização regular da lista de ativos críticos, sendo essa comunicação efetuada sempre que se verifiquem alterações relevantes, como ocorreu no último ano.

Questão 7. Na Instituição são aplicados algumas destas normas ou *frameworks* de segurança: ISO/IEC 27001, NIST, COBIT, CIS? Quais? Como é garantido o seu cumprimento?

O entrevistado I5 refere que na instituição, é aplicado o QNRCS. Referindo ainda que, embora não seja uma norma internacional específica como a ISO/IEC 27001, é baseado em boas práticas reconhecidas internacionalmente e devidamente adaptado à realidade nacional. Relativamente à garantia de cumprimento, o entrevistado I5 salientou que a sua aplicação é assegurada por mecanismos de controlo interno, que visam verificar a conformidade das práticas com os requisitos definidos. Assim, ao aplicar estas políticas por meio de controlos de segurança, a instituição garante também o cumprimento da legislação em vigor e das boas práticas de cibersegurança.

O entrevistado I6 refere que, embora exista conhecimento interno relativamente a normas de segurança da informação — nomeadamente por parte de elementos do corpo técnico, estudantes e membros do serviço de informática —, a sua aplicação ainda não se encontra uniformemente implementada na instituição. Com o intuito de colmatar estas lacunas, foi realizado um estudo interno na instituição, e foi contratada uma entidade externa com o objetivo de uniformizar as práticas institucionais com os requisitos da norma ISO/IEC 27001. O entrevistado I6 indica, ainda, que a instituição realiza auditorias de cibersegurança com alguma periodicidade, recorrendo, em diversos casos, a boas práticas e diretrizes estabelecidas em normas e *frameworks* internacionais, nomeadamente o NIST. No entanto, sublinha que a adoção destas referências normativas não é integral em todos os domínios organizacionais.

Questão 8. Quais as principais medidas de segurança da informação no controlo de acessos a sistemas e redes? A Instituição possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TI?

No que respeita às medidas de segurança da informação aplicadas ao controlo de acessos a sistemas e redes, o entrevistado I5 referiu que a instituição dispõe de diversas políticas documentadas, nomeadamente políticas de utilização e política de uso aceitável (AUP), políticas de gestão de palavras-passe e outras diretrizes internas orientadas para diferentes áreas dos serviços. Embora algumas destas políticas sejam de caráter mais restrito e destinadas a uso interno, todas são sujeitas a auditoria antes de entrarem em produtivo, sendo realizados testes de intrusão (*pen tests*) e análise de vulnerabilidades

pela equipa de resposta a incidentes, garantindo, assim, a sua conformidade e eficácia. Adicionalmente, são divulgadas boas práticas específicas para as equipas técnicas e de gestão, inspiradas em orientações internacionais reconhecidas. A seleção e aplicação destas medidas são sempre orientadas por uma análise de risco, ajustada à criticidade dos ativos em causa.

O entrevistado I6 indica que a instituição dispõe de manuais e normas internas documentados que detalham procedimentos específicos para o controlo de acessos a sistemas e redes. Neste âmbito, destaca-se a existência de regras claras para a construção e gestão de palavras-passe, cuja definição, periodicidade de renovação e critérios de complexidade se encontram formalmente estabelecidos e divulgados internamente. O controlo de acessos é ajustado conforme a criticidade das contas e dos sistemas. Os sistemas identificados como mais sensíveis estão sujeitos a mecanismos reforçados de segurança, nomeadamente através de autenticação multifator (MFA), complementada com requisitos adicionais específicos para o primeiro fator de autenticação. Adicionalmente, o entrevistado refere que a instituição adota um modelo de segurança em camadas, para assegurar um controlo rigoroso e proporcional ao grau de criticidade dos ativos digitais, utilizando redes privadas virtuais (VPN).

Questão 9. A Instituição utiliza alguma das seguintes medidas de segurança?

Para facilitar a compreensão e comparação das respostas obtidas, optou-se por apresentar, em formato de tabela, as questões de resposta dicotómica (sim/não) colocadas aos entrevistados. Esta forma de organização permite evidenciar, de forma clara e concisa, os pontos de convergência e divergência entre os participantes.

Tabela 13 - Respostas dos Entrevistados à questão 9.

Questão do Guião	I5	I6
9.1. Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação	Sim. O entrevistado refere que a sua aplicação depende da criticidade do ativo em questão.	Sim. O entrevistado refere que, embora a autenticação multifator (MFA) já esteja amplamente implementada entre os funcionários e docentes, a sua aplicação aos estudantes tem sido gradual, sendo atualmente obrigatória apenas para novos ingressos e para utilizadores identificados como estando

		em risco, com base numa monitorização semanal. Esta abordagem faseada deve-se, em parte, à limitação de recursos disponíveis.
9.2. Atualização regular do software	Sim.	Sim. Sempre que existe uma atualização a mesma é realizada.
9.3. Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN)	Sim.	Sim.
9.4. Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada online)	Sim. O entrevistado menciona que a instituição vai além desta prática, implementando medidas adicionais para garantir uma melhor segurança dos dados.	Sim. Embora algumas cópias sejam realizadas de forma automática e outras exijam intervenção manual, todas cumprem rigorosamente esta regra.
9.5. Foram definidos métodos apropriados para estabelecer e provar a identidade dos utilizadores, dispositivos ou sistemas com confiança suficiente para tomar decisões de controlo de acesso?	Sim.	Sim, com ressalvas. Para docentes e funcionários, a criação de contas institucionais apenas ocorre após a confirmação do vínculo com a instituição. No entanto, no caso dos estudantes de ciclos de mestrado e doutoramento, existe um período inicial em que a identidade ainda não foi confirmada presencialmente. A validação formal apenas ocorre após a entrega dos documentos na instituição. Esta é uma prática, comum em várias universidades e representa uma limitação temporária no processo de autenticação.

As respostas dos entrevistados revelam práticas semelhantes em relação à segurança da informação nas duas instituições. Em relação à autenticação multifator (MFA), uma prática de segurança amplamente reconhecida como uma medida essencial de segurança da informação por várias normas e *frameworks*, já é aplicada em ambas as instituições. O entrevistado I5 explicou que a MFA é aplicada conforme o risco identificado em determinados utilizadores, enquanto o entrevistado I6 revelou planos para expandir essa prática para todos os novos estudantes a partir do próximo ano, além de aplicá-la também aos estudantes identificados com risco, com base em uma monitorização contínua.

Ambos os entrevistados confirmaram atualização regular do software e controlo de acessos remotos à rede das instituições. No que respeita à implementação da regra 3-2-1 para a realização de cópias de segurança, o entrevistado I5 mencionou que para além desta regra, a instituição que representa adota, igualmente, medidas adicionais para fortalecer a segurança dos *backup*s, enquanto o entrevistado I6 destacou o uso de automatismos nos processos de *backup*, garantindo maior consistência e reduzindo o risco de falhas humanas.

Relativamente aos métodos adotados para estabelecer e comprovar a identidade de utilizadores, dispositivos ou sistemas, os entrevistados reconheceram a importância de ajustar os métodos de autenticação ao grau de criticidade dos ativos e ao perfil dos utilizadores envolvidos.

De um modo geral, as respostas recolhidas evidenciam que ambas as instituições estão empenhadas em adotar boas práticas de cibersegurança, procurando alinhar os seus procedimentos com orientações nacionais, nomeadamente o QNRCS (Capítulo 1.2.10 e Apêndice 1), bem como com normas e *frameworks* internacionais, como a ISO/IEC 27001 ou o NIST. Apesar de existirem algumas limitações operacionais e especificidades institucionais, é visível um esforço na implementação de medidas robustas de controlo de acessos, autenticação e gestão de risco.

10. Na Instituição existem programas de formação e promoção de boas práticas em cibersegurança regulares (voluntários e obrigatórios, contratuais) para funcionários, docentes e estudantes?

Relativamente à formação e sensibilização em cibersegurança, o entrevistado I5 referiu que a instituição promove, pelo menos uma vez por ano, campanhas de consciencialização dirigidas à comunidade académica. Para além destas iniciativas regulares, são também realizados simulacros de ataques, com o objetivo de testar a resposta dos utilizadores e reforçar a adoção de boas práticas de segurança no quotidiano institucional.

O entrevistado I6 refere que, embora existam iniciativas de formação e sensibilização em cibersegurança na instituição, estas não são ainda realizadas de forma regular. Destaca, contudo, a colaboração com o CNCS, nomeadamente através da participação na iniciativa *Cybersecurity Academy*, que resultou na disponibilização de formações abertas à comunidade em geral. O entrevistado I6 refere ainda, que atualmente, por exemplo, decorre um curso de princípios básicos de cibersegurança, com sessões semanais. Paralelamente, são promovidas pequenas campanhas de sensibilização ao longo do ano, através de suportes digitais internos, como ecrãs informativos e newsletters, que abordam temas como *ransomware*, *phishing* e outras ameaças comuns, com o objetivo de fomentar boas práticas entre os utilizadores.

A realização de ações de formação e sensibilização em cibersegurança é essencial para promover uma cultura de segurança nas instituições e reduzir o impacto do erro humano, que continua a ser um dos principais pontos vulneráveis nos sistemas de informação, conforme referido no capítulo 1.2.6 do presente estudo.

Questão 11. Na Instituição são realizados testes ou simulações de ataques, como campanhas de *phishing*, análises de vulnerabilidades e simulações de *ransomware*?

O entrevistado I5 confirma que, na instituição, são realizados testes e simulações de ataques, nomeadamente campanhas de *phishing*, análises de vulnerabilidades e, pontualmente, exercícios relacionados com *ransomware*.

Relativamente, ao entrevistado I6, este refere que na instituição, realizam-se testes e simulações de ciberataques, como campanhas de *phishing* e análises de vulnerabilidades, ainda que com uma abordagem bastante cautelosa e recursos limitados. De acordo com o entrevistado, há uma preocupação com o impacto que algumas simulações, nomeadamente de *phishing*, podem ter nos utilizadores, uma vez que, segundo o entrevistado, em certos contextos, estas ações podem até aumentar a suscetibilidade ao próprio ataque.

Questão 12. Na Instituição são realizados testes da segurança informática de intrusão, aos sistemas de alerta e de *backup*, revisões às medidas de segurança?

O entrevistado I5 refere que a instituição realiza diversos testes de segurança informática de intrusão, bem como aos sistemas de alerta e *backpup*.

O entrevistado I6 menciona que, na instituição, a equipa responsável pela resposta a incidentes realiza auditorias de segurança aos sistemas de informação de forma regular. Este processo é cuidadosamente planeado, começando com a comunicação prévia aos responsáveis pelos sistemas. Embora eles colaborem ativamente na auditoria, a condução do processo fica a cargo de profissionais externos à área de informática, o que garante uma visão mais imparcial e objetiva. Durante essas auditorias, são realizados testes de intrusão e outras análises técnicas, com o objetivo de identificar vulnerabilidades e áreas que possam ser melhoradas. Os resultados desses testes são organizados num relatório, resultando num plano de ação, e num acompanhamento contínuo das correções implementadas. O entrevistado acrescenta ainda que este ciclo de auditorias se repete periodicamente, permitindo à instituição monitorizar e melhorar constantemente a segurança dos seus sistemas.

Estas ações têm como objetivo principal avaliar a robustez dos sistemas de defesa e os mecanismos de alerta, contribuindo para uma resposta mais eficaz face a potenciais incidentes de cibersegurança.

Questão 13. A Instituição já sofreu algum incidente de segurança? Se sim, que tipo de incidente, qual o seu impacto para a Instituição e de que forma foi tratado?

O entrevistado I5 opta por não fornecer detalhes específicos sobre eventuais incidentes de segurança ocorridos na instituição. Contudo, esclarece que a comunicação dos índices relativos a incidentes de segurança é sempre feita diretamente ao CNS.

O entrevistado I6 relata que, em 2022, a instituição foi alvo de um ciberataque significativo, que teve um impacto profundo nos seus sistemas críticos. A instituição ficou sem qualquer acesso aos seus sistemas e a magnitude do ataque foi tal que afetou todos

os sistemas essenciais da universidade. Apesar das várias ofertas de ajuda externa, o entrevistado destaca que a equipa interna foi fundamental na recuperação, dada a sua familiaridade com os sistemas. A equipa iniciou a reinstalação de todas as máquinas do parque informático e restaurou os dados a partir dos *backup*s. O entrevistado refere, ainda que, o processo foi longo e complexo, sendo os primeiros seis meses especialmente desafiantes, exigindo um esforço contínuo e dedicado da equipa para restabelecer os sistemas da universidade.

Questão 14. Na Instituição existe um plano de resposta a incidentes? Se sim, este inclui o Plano de continuidade de negócios, de contingência, de recuperação em caso de desastre e o plano de gestão de crise?

O entrevistado I5, refere que na instituição, existe, de facto, um plano de resposta a incidentes bem estruturado, que inclui protocolos claros para lidar com diferentes tipos de incidentes, tanto os já identificados como os que possam surgir no futuro. Este plano envolve uma equipa dedicada à resposta a incidentes, que trabalha em colaboração com as equipas de infraestruturas e de apoio a serviços e aplicações. Quando se trata de recuperação, o plano inclui uma abordagem específica para situações de desastre, garantindo que os sistemas essenciais sejam rapidamente restaurados. Para ativos menos críticos, a instituição utiliza máquinas de teste, sem dados sensíveis, para realizar simulações e garantir que o sistema funcione de forma eficaz em situações de recuperação. No que diz respeito ao domínio administrativo da instituição, o plano de recuperação é mais abrangente e garante, inclusive, a continuidade dos negócios, com medidas que asseguram que os serviços não parem, mantendo assim a operação da instituição mesmo em situações adversas.

O entrevistado I6 explica que, tanto antes como após o ciberataque, a instituição não possuía um plano de resposta a incidentes estruturado. Devido às consequências do ataque, a equipa concentrou-se exclusivamente na recuperação e na mitigação dos danos, o que impediu o desenvolvimento de um plano adequado até o momento. Embora o entrevistado acredite que a instituição tenha saído mais forte e resiliente dessa experiência, reconhece que os efeitos do ataque ainda são visíveis em algumas áreas e destaca a importância de desenvolver um plano de resposta a incidentes.

Relativamente a esta questão, o CNCS destaca a importância de um plano de resposta a incidentes estruturado, que inclua medidas como continuidade de negócios, contingência e recuperação. Através da análise das respostas obtidas concluímos que a instituição I5 já cumpre estas orientações, com processos definidos e testados, e ainda que a instituição do entrevistado I6 não tenha um plano formalizado até o momento, o fato de já ter enfrentado um ataque significativo reforça a importância de alinhar suas práticas com as recomendações do CNCS, a fim de fortalecer sua resiliência.

Questão 15. A instituição possui uma apólice de seguro de cibersegurança ou está a ser considerada a possibilidade da sua contratação?

O entrevistado I5 não revela se a instituição possui ou não uma apólice de seguro de cibersegurança, no entanto, considera que a contratação de uma apólice pode ser importante, desde que não crie uma falsa sensação de segurança. Ele destaca que, embora a cobertura de cibersegurança possa ser útil, é necessário ter uma compreensão clara das limitações desse seguro, especialmente em relação à legislação em Portugal e na Europa, onde as apólices não protegem contra todas as situações.

O entrevistado I6 refere que neste momento não está a ser considerada a contratação de uma apólice de seguro de cibersegurança. O entrevistado destaca que, apesar do ataque sofrido, a instituição tem redirecionado os esforços e os recursos financeiros para outras soluções de segurança, que considera mais relevantes. Entre essas soluções, menciona a implementação de *backup*s automáticos, que permitem uma recuperação mais rápida em caso de futuros incidentes. Para o entrevistado, esses investimentos são mais prioritários e eficazes para a proteção e recuperação dos sistemas da instituição do que a contratação de um seguro de cibersegurança.

Embora ambos os entrevistados reconheçam a importância de mecanismos de segurança, o seguro de cibersegurança é visto como uma solução complementar, não substituindo outras práticas essenciais, como as definidas pelo QNRCS, conforme abordado no capítulo 1.2.10.

Questão 16. Na sua opinião existe necessidade de melhorar a Cibersegurança na sua Instituição? Se sim quais são os medidas e estratégias futuras que poderão a vir a ser implementadas na sua Instituição?

O entrevistado I6 reconhece que há sempre espaço para melhorar a cibersegurança na instituição e menciona que estão continuamente a trabalhar nesse sentido. Em relação às medidas e estratégias futuras, o entrevistado aponta, por exemplo, a melhoria das soluções de *backup* e a aprovação do plano de resposta a incidentes, que ainda não está totalmente formalizado, bem como a formalização de planos, como o plano de gestão e tratamento da segurança da informação.

Durante a entrevista com o entrevistado I5 houve um lapso que impediu a realização da questão número 15, previamente prevista no guião. Embora essa questão não tenha sido abordada nesta entrevista, a ausência da resposta não comprometeu a análise global, uma vez que as informações obtidas durante entrevista foram suficientes para sustentar as conclusões da pesquisa.

Questão 17. Como classificaria o nível de maturidade da cibersegurança na sua Instituição de acordo com o Modelo de Maturidade de Cibersegurança da Gartner?

- **Nível 1 - Inicial: Não existe uma estratégia clara de cibersegurança.**
- **Nível 2 - Reativo: A segurança é reativa, com principal foco em resolver problemas à medida que surgem.**
- **Nível 3 - Definido: A segurança é bem definida e incorporada nos processos organizacionais.**
- **Nível 4 - Gerido: A segurança é gerida de forma proativa com processos bem estabelecidos.**
- **Nível 5 - Otimizado: A segurança é integrada de forma contínua na cultura organizacional e melhorada constantemente.**

O entrevistado I5 considera que o nível de maturidade da cibersegurança na sua instituição, de acordo com o Modelo de Maturidade da Gartner, varia consoante o domínio analisado. Ao avaliar a instituição como um todo, aponta para um nível 4 –

Gerido, justificando que existem processos bem estabelecidos e uma gestão proativa da segurança. No entanto, distingue esta análise em dois domínios dentro da instituição: o domínio administrativo, que classifica como nível 5 – Otimizado, dado o elevado grau de integração e melhoria contínua das práticas de segurança; e o domínio académico, onde identifica maiores dificuldades de implementação e limitações estruturais, situando-o no nível 3 – Definido. Esta diferenciação reflete a complexidade e os diferentes desafios existentes dentro da mesma organização.

O entrevistado I6 refere que, embora a instituição ainda não disponha de todos os documentos formalmente aprovados, nem de um plano global de cibersegurança consolidado, várias práticas já estão implementadas e são aplicadas de forma consistente e proativa. Destaca, por exemplo, a existência de processos internos de monitorização e resposta a incidentes, como a verificação semanal de acessos a sites maliciosos, a aplicação imediata de medidas corretivas, e um controlo rigoroso das ligações de rede, que requer aprovação prévia por parte de elementos da equipa. Além disso, menciona a participação ativa na análise de relatórios de cibersegurança. Apesar destas medidas refletirem um nível de maturidade elevado, o entrevistado opta por classificar a instituição no nível 3 e justifica a sua escolha com a ausência de um plano estruturado e formalmente aprovado, o qual considera importante para garantir a continuidade das práticas em caso de mudança ou ausência da equipa atual. Ainda assim, acredita que a instituição se tornou mais robusta e resiliente após o incidente de cibersegurança, reconhecendo, no entanto, que existe sempre espaço para melhorar.

CONCLUSÃO

A transformação digital está a mudar profundamente a forma como as Instituições de Ensino Superior funcionam e se relacionam com o mundo e apoiam os seus estudantes, docentes e investigadores. Com estas mudanças surgem novas oportunidades, mas também novas responsabilidades — principalmente no que toca à segurança da informação. A digitalização, aliada à crescente internacionalização das IES exige uma abordagem estruturada à segurança da informação, uma vez que estas instituições lidam diariamente com dados académicos, administrativos, financeiros e pessoais de milhares de utilizadores. A garantia de segurança da informação não depende apenas de soluções tecnológicas, mas também de regras claras, rotinas bem organizadas e, acima de tudo, do envolvimento de todos na construção de uma cultura de responsabilidade digital dentro da instituição. É neste contexto que a adoção de medidas de segurança se revela essencial não só para prevenir incidentes, mas também para garantir a continuidade das atividades de ensino e de investigação, mesmo perante eventuais ciberameaças.

A adoção de boas práticas de cibersegurança — como a segmentação de redes, a autenticação multifator, a encriptação de dados e a formação contínua de quem usa os sistemas — é essencial para tornar as instituições mais preparadas e resilientes. Além disso, ações como a realização de auditorias com regularidade, responder rapidamente a incidentes e manter os sistemas atualizados ajudam a cumprir as obrigações legais e proteger a informação.

No presente estudo empírico foi possível concluir que ambas as Instituições demonstram um compromisso claro com a cibersegurança, ainda que se encontrem em fases distintas de maturidade organizacional. Enquanto a Ensino Superior Público – Politécnico apresenta uma estrutura mais consolidada, com políticas formais e práticas regulares de sensibilização e auditoria, a Instituição Ensino Superior Público – Universitário já implementou várias medidas de segurança, no entanto ainda não se encontram formalizadas num único documento estratégico. Em ambos os casos, destaca-se a consciência crescente sobre a importância da segurança digital e a adoção de medidas técnicas e organizacionais que, apesar de poderem ser aperfeiçoadas, seguem orientações alinhadas com o QNRCS e outras normas reconhecidas internacionalmente.

Principais Contributos

Este estudo visa contribuir para a consciencialização sobre o panorama e os desafios atuais relacionados com a implementação de práticas de cibersegurança nas instituições de ensino superior. Em particular, pretende-se destacar as dificuldades enfrentadas por estas instituições devido à escassez de recursos humanos especializados e/ou fundos disponíveis para o desenvolvimento de medidas mais eficazes, bem como à crescente complexidade das ameaças de cibersegurança.

Limitações

Uma das principais limitações do presente estudo prende-se com a reduzida representatividade das universidades e institutos politécnicos incluídos na amostra. Relativamente às entrevistas, apesar do esforço envidado para obter uma maior participação de intervenientes com responsabilidades na área da cibersegurança das IES, verificaram-se dificuldades na recolha de dados. Em vários casos, os intervenientes contactados encontravam-se indisponíveis nos períodos estabelecidos para a recolha de dados, seja por constrangimentos de agenda, seja por mudanças organizacionais em curso nas respetivas instituições.

Adicionalmente, destaca-se a ausência de instituições de ensino superior privadas na amostra, o que limita a possibilidade de identificar eventuais diferenças estruturais entre os setores público e privado no que concerne às medidas de cibersegurança implementadas. A inclusão de universidades do setor privado no estudo poderia proporcionar uma análise mais completa e comparativa entre as práticas adotadas em ambos os setores.

Para a realização das entrevistas, optou-se pela seleção por conveniência dos entrevistados, com base na sua disponibilidade e relevância para o tema da cibersegurança nas instituições de ensino superior.

Estas limitações metodológicas comprometem a abrangência dos resultados obtidos, restringindo a sua capacidade de generalização para um universo mais alargado de instituições de ensino superior.

Trabalho Futuro

Tendo em conta as limitações inerentes ao presente estudo, considera-se pertinente a realização de uma investigação futura que envolva o contributo de uma maior percentagem de universidades públicas e privadas e institutos politécnico do país. Deste modo, será possível identificar e compreender as diferentes realidades institucionais e práticas de cibersegurança, contribuindo para uma análise mais realista e rigorosa do panorama de cibersegurança em Portugal.

REFERÊNCIAS BIBLIOGRÁFICAS

Altbach, P. G. (2004). Globalization and the university: Myths and realities in an unequal world. In National Education Association (Ed.), The NEA 2005 almanac of higher education (pp. 63-74). Washington, DC: National Education Association.

Altbach, P. G., & Knight, J. (2007). The internationalization of higher education: Motivations and realities. Journal of Studies in International Education, 11(3–4), 290–305. https://doi.org/10.1177/1028315307303542

Altbach, P. G., Reisberg, L., & Rumbley, L. E. (2009). Trends in global higher education: Tracking an academic revolution. A report prepared for the UNESCO 2009 World Conference on Higher Education. United Nations Educational, Scientific and Cultural Organization.

Amine, A. M., Chakir, E. M., Issam, T., & Khamlichi, Y. I. (2023). A review of cybersecurity management standards applied in higher education institutions. International Journal of Safety and Security Engineering, 13(6), 1109–1116.

Anderson, J., & Lanzolla, G. (2010). The Digital Revolution is Over: Long Live the Digital Revolution! Business Strategy Review, 21(1), pp.74–77.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management – A procedure model and its application. Business & Information Systems Engineering, 1(3), 213–222.

Belk, R. W. (2013). You are what you can access: Sharing and collaborative consumption online. Journal of Business Research, 67(8), 1595–1600.

Branco Jr, T. T., & Fonseca, I. C. da. (2022). Um inquérito para verificação da cibersegurança nas organizações públicas municipais em Portugal. Revista Ibérica de Sistemas e Tecnologias de Informação, (48), 41–58.

de Wit, H., & Altbach, P. G. (2021). Internationalization in higher education: Global trends and recommendations for its future. Policy Reviews in Higher Education, 5(1), 28–46.

de Wit, H., & Knight, J. (1996). Strategies for internationalization of higher education: Historical and conceptual perspectives.

Defense in depth. (s.d.). Recuperado de https://csis.pace.edu/~lombardi/sciences/computer/systems/windows/docs/defenseindepth.pdf

Direção-Geral de Estatísticas da Educação e Ciência. (2024). A segurança das TIC (cibersegurança) na administração pública - 2023.

Direção-Geral do Ensino Superior. (s.d.). Programas Impulso. Disponível em https://programasimpulso.dges.gov.pt/

Forbes Portugal. (2022, fevereiro 11). Menos de 1% das empresas portuguesas têm seguro contra riscos cibernéticos. Forbes Portugal. https://www.forbespt.com/menos-de-1-das-empresas-portuguesas-tem-seguro-contra-riscos-ciberneticos/

Górniak, S. (2014). Standardisation in the field of Electronic Identities and Trust Service Providers (Publicação nº TP-06-14-227-EN-N). Agência da União Europeia para a Cibersegurança (ENISA).

Hess, T.; Matt, C.; Benlian, A.; Wiesböck, F. (2016). Options for Formulating a Digital Transformation Strategy. MIS Quarterly Executive, 15(2), 103-119.

Hill, M. M., & Hill, A. (2016). Investigação por Questionário (2 ed.). Edições Sílabo, Lda.

ISO/IEC. (2018). ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management. ISO.

ISACA. (s.d.). COBIT | Control Objectives for Information Technologies. ISACA. https://www.isaca.org/resources/cobit/

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review.

KPMG LLP. (2023). Understanding ISO 27001:2022: People, process, and technology. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/understanding-iso27001-2022-people-process-technology.pdf

Knight, J. (1994). Internationalization: Elements and checkpoints (Research Monograph, No. 7). Ottawa, Canada: Canadian Bureau for International Education.

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids—A comprehensive survey. Comput. Stand. Interfaces, 56, 62–73.

Luziriaga, Lorenzo. (1985). História da educação e da Pedagogia. 16. ed. São Paulo: Ed. Nacional.

Microsoft. (2024, 10 de outubro). Instituições de ensino entre os principais alvos de ciberataques. Microsoft News Center. https://news.microsoft.com/pt-pt/2024/10/10/instituicoes-de-ensino-entre-os-principais-alvos-de-ciberataques/

Microsoft. (2024, 10 de outubro). Cyber Signals: Cyberthreats in K-12 and higher education. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/

NIST. (2013). Cybersecurity Framework, NIST, nov. 2013.

PrivacyEngine. (2023, 10 de novembro). ISO 27001 vs. NIST Cybersecurity Framework: comparação detalhada. PrivacyEngine. https://www.privacyengine.io/blog/iso-27001-vs-nist-cybersecurity-framework/

Prey Project. (2024, 10 de maio). NIST or CIS framework?: Which is better for schools. Prey Project. https://preyproject.com/blog/nist-or-cis-framework-which-is-better-for-schools

Priberam. (2024). Ciber. Em Dicionário Priberam da Língua Portuguesa. Priberam. Disponível em: https://dicionario.priberam.org/ciber

Scott, Peter. (2005). “The Global Dimension: Internationalising Higher Education.” In: Barbara Khem, Hans de Wit (eds.). Internationalization in Higher Education: European Responses to the Global Perspective. Amsterdam: European

Association for International Education and the European Higher Education Society.

Soderqvist, M. (2002). Internationalization and its management at higher-education institutions: Applying conceptual, content and discourse analysis. Helsinki, Finland: Helsinki School of Economics.

Turkle, S. (2011). Alone Together: Why We Expect More from Technology and Less from Each Other. Basic Books.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144.

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press.

Wit, H., & Knight, J. (1996). Strategies for internationalization of higher education: Historical and conceptual perspectives.

Wit, H., & Knight, J. (2022). Internationalisation of higher education new players.

Zhang, L. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Eric C. K. Cheng & Tianchong Wang.

Governo de Portugal. (2018). Resolução do Conselho de Ministros n.º 26/2018. Diário da República, 1.ª série, N.º 43, 1 de março de 2018. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/26-2018-114832288

Centro Nacional de Cibersegurança. (2024). Relatório Riscos e Conflitos 2024. https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf

Centro Nacional de Cibersegurança. (2019). Quadro Nacional de Referência para a Cibersegurança. https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

Centro Nacional de Cibersegurança. (2022). Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança v.1.1. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

EDUCAUSE. (2024, 10 de outubro). Pass or fail? Data privacy and cybersecurity risks in higher education. EDUCAUSE Review. https://er.educause.edu/articles/sponsored/2024/10/pass-or-fail-data-privacy-and-cybersecurity-risks-in-higher-education

APÊNDICES

APÊNDICE 1. Guião da Entrevista

iscac Politécnico de Coimbra COIMBRA BUSINESS SCHOOL 100 ANOS since 1921

Principais Riscos e Práticas de Controlo em Cibersegurança – Perceções dos Intervenientes e Estratégias Implementadas em Instituições de Ensino Superior em Portugal

Guião de Entrevista (Tempo estimado 20 a 30 min)

Tema da Dissertação: Principais Riscos e Práticas de Controlo na Cibersegurança em Instituições de Ensino Superior em Portugal – Perceções dos Intervenientes e Estratégias Implementadas

1. Apresentação do Entrevistado
   1.1. Descrição do papel que assume na instituição e que tipo de Instituição.
   1.2. Há quanto tempo trabalha na Instituição?
   1.3. Desenvolve funções relacionadas com a tecnologia e segurança da informação?
   1.4. Qual é a sua experiência profissional relacionada com a cibersegurança?
2. Descreva brevemente a estrutura de TI e cibersegurança da Instituição? Existe uma equipa dedicada exclusivamente à cibersegurança?
3. Considera que a cibersegurança é uma prioridade na instituição? Porquê?
4. Na sua opinião quais são os principais desafios que a sua instituição e/ou o setor do ensino enfrentam em termos de cibersegurança atualmente?
5. O Organismo tem definida uma estratégia/politica formal para a segurança das redes e da informação? Se sim, encontra-se implementada na Instituição? É revista com que periodicidade?

5.1. A mesma encontra-se de acordo com o Regulamento Geral de Proteção de Dados (RGPD) e o Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021?

6. De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), a Instituição efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)?
7. Na Instituição são aplicados algumas destas normas ou frameworks de segurança: ISO 27001, NIST, COBIT, CIS? Quais? Como é garantido o seu cumprimento?
8. Quais as principais medidas de segurança da informação no controlo de acessos a sistemas e redes? A Instituição possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TI?
9. A Instituição utiliza alguma das seguintes medidas de segurança:

9.1. Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação

9.2. Atualização regular do software

9.3. Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN)

9.4. Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada offline)

9.5. Foram definidos métodos apropriados para estabelecer e provar a identidade dos utilizadores, dispositivos ou sistemas com confiança suficiente para tomar decisões de controle de acesso?

Ana Margarida Seixas Costa | INSTITUTO SUPERIOR CONTABILIDADE E AUDITORIA DE COIMBRA

iscac Politécnico de Coimbra COIMBRA BUSINESS SCHOOL 100 ANOS since 1921

Principais Riscos e Práticas de Controlo em Cibersegurança – Perceções dos Intervenientes e Estratégias Implementadas em Instituições de Ensino Superior em Portugal

10. Na Instituição existem programas de formação e promoção de boas práticas em cibersegurança regulares (voluntários e obrigatórios, contratuais) para funcionários, docentes e estudantes?
11. Na Instituição são realizados testes ou simulações de ataques, como campanhas de *phishing*, análises de vulnerabilidades e simulações de *ransomware*?
12. Na Instituição são realizados testes da segurança informática de intrusão, aos sistemas de alerta e de backup, revisões às medidas de segurança?
13. A Instituição já sofreu algum incidente de segurança? Se sim, que tipo de incidente, qual o seu impacto para a Instituição e de que forma foi tratado?
14. Na Instituição existe um plano de resposta a incidentes? Se sim, este inclui o Plano de continuidade de negócios, de contingência, de recuperação em caso de desastre e o plano de gestão de crise?
15. A instituição possui uma apólice de seguro de cibersegurança ou está a ser considerada a possibilidade da sua contratação?
16. Na sua opinião existe necessidade de melhorar a Cibersegurança na sua Instituição? Se sim quais são os medidas e estratégias futuras que poderão a vir a ser implementadas na sua Instituição?
17. Como classificaria o nível de maturidade da cibersegurança na sua Instituição de acordo com o Modelo de Maturidade de Cibersegurança da Gartner?
    - Nível 1: Inicial: Não existe uma estratégia clara de cibersegurança.
    - Nível 2: Reativo: A segurança é reativa, com principal foco em resolver problemas à medida que surgem.
    - Nível 3: Definido: A segurança é bem definida e incorporada nos processos organizacionais.
    - Nível 4: Gerido: A segurança é gerida de forma proativa com processos bem estabelecidos.
    - Nível 5: Otimizado: A segurança é integrada de forma continua na cultura organizacional e melhorada constantemente.