Análise da Cibersegurança em Instituições de Ensino

O estado atual nos Agrupamentos de Escolas e Escolas Não Agrupadas da região de Leiria

Mestrado em Cibersegurança e Informática Forense

Filipe André Pereira Bagagem

Leiria, junho de 2024

escola superior de tecnologia e gestão
instituto politécnico de leiria

Análise da Cibersegurança em Instituições de Ensino

O estado atual nos Agrupamentos de Escolas e Escolas Não Agrupadas da região de Leiria

Mestrado em Cibersegurança e Informática Forense

Filipe André Pereira Bagagem

Número: 2220558

Trabalho de Projeto realizado sob a orientação da Professora Doutora Marisa da Silva Maximiano, do Professor Doutor Mário João Gonçalves Antunes e do Professor Ricardo Jorge Pereira Gomes.

Leiria, junho de 2024

Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Dedicatória

Dedico este trabalho de projeto à minha esposa Ana e aos meus filhos Lara e Mateus, pela ausência que a mesma me fez prescindir da companhia de ambos.

Agradecimentos

Foram muitas as pessoas que, direta ou indiretamente, tornaram este trabalho possível. A todos eles, o meu muito obrigada.

A todos os Professores que fizeram parte do meu percurso académico, em especial aos que me acompanharam nestes últimos dois anos de mestrado, pelo conhecimento, excelência e rigor.

Um especial agradecimento aos orientadores deste trabalho de projeto, Professora Doutora Marisa Maximiano, Professor Doutor Mário Antunes e Professor Ricardo Gomes, por toda a disponibilidade em colaborador neste trabalho e pelos sábios conselhos.

A todos os inquiridos, o meu muito obrigada por toda a disponibilidade, simpatia e interesse em colaborar.

Por último, dirijo um agradecimento especial à minha esposa, pelo apoio incondicional, incentivo e paciência no caminho para a concretização deste objetivo.

A ela dedico este trabalho!

Resumo

A cibersegurança, ou segurança digital, é um tema cada vez mais importante e presente no mundo digital em que vivemos. A cibersegurança tem-se tornado uma prática imprescindível nas organizações, pois assume um papel cada vez mais importante no que diz respeito à segurança dos sistemas de informação. O principal objetivo é assegurar a confidencialidade, integridade e disponibilidade dos ativos e/ou dos dados em relação às ameaças do ciberespaço.

As instituições de ensino, tanto públicas quanto privadas, disponibilizam vários serviços para a Internet e, por esse facto, estão sujeitas a ciberataques que podem comprometer a segurança de dados sensíveis, como informações dos utentes/ex-utentes (alunos, docentes, não docentes e colaboradores), registos académicos e financeiros. É fundamental que estas instituições de ensino estejam preparadas para as ameaças provocadas pelos ciberataques e implementem medidas de segurança adequadas para proteger os seus dados e a própria infraestrutura contra ameaças cibernéticas.

Este projeto tem como principal objetivo avaliar o estado atual de cibersegurança nos Agrupamentos de Escolas e Escolas Não Agrupadas que pertencem à região de Leiria, mais concretamente aos concelhos de Alvaiázere, Ansião, Batalha, Castanheira de Pera, Figueiró dos Vinhos, Leiria, Marinha Grande, Pedrógão Grande, Pombal e Porto de Mós. Ao longo deste projeto foi elaborado um guia de cibersegurança com vista à mitigação de potenciais consequências graves à infraestrutura de uma instituição de ensino provenientes de incidentes de cibersegurança.

Numa primeira fase, são analisados vários conceitos inerentes à compreensão do tema para a realização deste projeto, desde a organização do sistema educativo português, à definição de cibersegurança e os fatores que a circulam como os tipos de ataques cibernéticos, a cibersegurança como política pública, a legislação e o cibercrime em Portugal, as *frameworks* de cibersegurança mais comuns e por fim os trabalhos relacionados.

Numa segunda fase, é definida a metodologia e as técnicas para a recolha de dados através de um questionário que foi preparado especificamente para o público-alvo do caso de estudo, em que o principal foco é avaliar o estado atual da Cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) que pertencem à região de Leiria. Ainda nesta

segunda fase, os resultados obtidos no questionário quantitativo foram analisados estatisticamente.

Na terceira e última fase, é apresentada uma proposta de um guia de cibersegurança que pode ser adotado e ajustado pelas instituições públicas de ensino para reforçar a sua presença segura no ciberespaço.

Palavras-chave: Segurança Cibernética, Escolas Públicas, Ensino, Guia de Cibersegurança, Segurança da Informação, *Frameworks*

Abstract

Cybersecurity, or digital security, is an increasingly important and present topic in the digital world in which we live. Cybersecurity has become an essential practice in organizations, as it plays an increasingly important role with regard to the security of information systems. The main objective is to ensure the confidentiality, integrity and availability of assets and/or data in relation to cyberspace threats.

Educational institutions, both public and private, provide various services on the Internet and, as a result, are subject to cyberattacks that can compromise the security of sensitive data, such as information from users/former users (students, teachers, non-teachers and employees), academic and financial records. It is essential that these educational institutions are prepared for the threats caused by cyberattacks and implement appropriate security measures to protect their data and the infrastructure itself against cyber threats.

This master's project's main objective is to evaluate the current state of cybersecurity in School Groups and Non-Group Schools that belong to the Leiria region, more specifically in the municipalities of Alvaiázere, Ansião, Batalha, Castanheira de Pera, Figueiró dos Vinhos, Leiria, Marinha Grande, Pedrógão Grande, Pombal and Porto de Mós. Throughout this project, a cybersecurity guide was developed with a view to mitigating potential serious consequences for the infrastructure of an Educational Institution arising from cybersecurity incidents.

In the first phase, several concepts vital to the understanding of the topic are analyzed to carry out this project, from the organization of the Portuguese educational system to the definition of cybersecurity and the factors that circulate it, such as the types of cyberattacks, cybersecurity as a public policy, the legislation and cybercrime in Portugal, the most common cybersecurity frameworks and finally related work.

In a second phase, the methodology and techniques for data collection are defined through a questionnaire that was prepared specifically for the target audience of the case study, in which the main focus is to evaluate the current state of Cybersecurity in Schools that belong to the Leiria region. Still in this second phase, the results obtained in the quantitative questionnaire were statistically analyzed.

In the third and final phase, a proposal for a cybersecurity guide is presented that can be adopted and adjusted by public educational institutions to reinforce their secure presence in cyberspace.

Keywords: Cybersecurity, Public Schools, Teaching, Cybersecurity Guide, Information Security, Frameworks

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

2FA	*Two-Factor Authentication*
AE	Agrupamento de Escolas
AMA	Agência para a Modernização Administrativa
ANCC	Autoridade Nacional de Certificação em Cibersegurança
AP	Administração Pública
BYOD	*Bring Your Own Device*
CERT	*Computer Emergency Response Team*
CET	Cursos de Especialização Tecnológica
CIA	*Confidentiality, Integrity and Availability*
CID	Confidencialidade, Integridade e Disponibilidade
CIS	*Center for Internet Security*
CISO	*Chief Information Security Officer*
CNCS	Centro Nacional de Cibersegurança
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*
CV	*Curriculum Vitae*
DaaS	*Desktop as a Service*
DDoS	*Distributed Denial-of-service*
DKIM	*DomainKeys Identified Mail*
DGEEC	Direção-Geral de Estatísticas da Educação e Ciência
DGES	Direção-Geral do Ensino Superior
DMARC	Domain-Based Message Authentication Message Conformance
DNS	*Domain Name System*
DoS	*Denial-of-service*
ENA	Escolas Não Agrupadas
ENISA	European Network and Information Security Agency
ESTG	Escola Superior de Tecnologia e Gestão

FCT	Fundação para a Ciência e Tecnologia
HIDS	*Host-based Intrusion Detection Systems*
HTTP	*Hypertext Transfer Protocol*
IA	Inteligência Artificial
ICMP	*Internet Control Message Protocol*
ICT	*Information and Communications Technology*
IEC	*International Electrotechnical Commission*
IGeFE	Instituto de Gestão Financeira da Educação
IoT	*Internet of Things*
IP	*Internet Protocol*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization.*
ISP	*Internet Service Provider*
IT	*Information Technology*
IUTIC	Inquérito à Utilização das Tecnologias da Informação e da Comunicação
IUTICAP	Inquérito à Utilização de TIC na Administração Pública Central
MEC	Ministério da Educação e Ciência
MFA	*Multi-Factor Authentication*
MISI	Gabinete Coordenador do Sistema de Informação do Ministério da Educação
MITM	*Man-In-The-Middle*
NATO	*North Atlantic Treaty Organization*
NIS	*Network and Information Security*
NIST	*National Institute of Standards and Technology*
NIST CSF	*NIST Cybersecurity Framework*
PCN	Pontos de Contacto Nacionais
PRI	Plano de Resposta a Incidentes
PUA	Política de Utilização Aceitável
OSCE	*Organization for Security and Co-operation in Europe*
QNRCS	Quadro Nacional de Referência para a Cibersegurança

RAE	Rede Alargada da Educação
RCM	Resolução do Conselho de Ministros
RCTS	Rede Ciência, Tecnologia e Sociedade
RDP	*Remote Desktop Protocol*
RGPD	Regulamento Geral de Proteção de Dados
RISTI	Revista Ibérica de Sistemas e Tecnologias de Informação
RJSC	Regime Jurídico da Segurança do Ciberespaço
SciELO	*Scientific Electronic Library Online*
SEN	Sistema Estatístico Nacional
SIEM	*Security Information and Event Management*
SIGO	Sistema de Informação e Gestão da Oferta educativa e formativa
SMS	*Short Message Service*
SOC	*Security Operations Centre*
SPF	*Sender Policy Framework*
SQL	*Structured Query Language*
TCP	*Transmission Control Protocol*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
URL	*Uniform Resource Locator*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WAN	*Wide-Area Network*

1. Introdução

Melhorar a segurança das tecnologias da informação é uma prioridade máxima para organizações de todos os setores, mas é especialmente importante no setor da educação para ajudar a proteger a confidencialidade, integridade e disponibilidade da informação e dos sistemas.

Os sistemas de informação são, nos dias de hoje, uma das partes mais importantes e essenciais ao bom funcionamento das organizações [1]. Embora se identifique uma dependência natural entre a atividade das organizações e o normal funcionamento dos sistemas de informação e comunicação, as ameaças contra a confidencialidade, integridade e disponibilidade dos sistemas podem resultar em situações prejudiciais para o normal funcionamento das organizações [2].

A cibersegurança é um tema cada vez mais importante e presente no mundo digital em que vivemos. As instituições de ensino, tanto públicas quanto privadas, com a disponibilização de vários serviços para a Internet estão sujeitas a ciberataques que podem comprometer a segurança de dados sensíveis, tais como informações dos seus utilizadores (alunos, docentes, não docentes e colaboradores), registos académicos e financeiros. É fundamental que estas instituições de ensino estejam preparadas e tenham medidas de segurança adequadas para proteger os seus dados e a própria infraestrutura contra ciberataques.

A pandemia Covid-19 obrigou a uma rápida adaptação das Escolas ao ensino à distância, em particular a partir do dia 16 de março de 2020, situação que se manteve, pelo menos, até ao final do ano letivo de 2019/2020. Esta circunstância trouxe vários desafios de cibersegurança e mostrou a importância desta área para as necessidades de digitalização do ensino.

De acordo com o *Boletim de maio de 2022* [3], do Centro Nacional de Cibersegurança (CNCS), entre fevereiro e março de 2020, o número de incidentes registados pelo CERT.PT – serviço que coordena a resposta a incidentes de cibersegurança em Portugal – aumentou 84% e, em comparação com o número de incidentes registados em março de 2019, o aumento foi de 176%. Os meses de abril e maio confirmaram esta tendência, com aumentos de 142% e 134%, respetivamente, relativamente ao período homólogo de 2019. Segundo a mesma fonte, o tipo de incidente reportado com maior aumento neste período de pandemia foi o

phishing, que aumentou 217% entre fevereiro e março. Os autores destas campanhas de *phishing* aproveitaram o confinamento para simular serviços digitais com maior fidelização e consumo, como os serviços de conteúdos digitais em *streaming*, vendas online e *homebanking*. Com a pandemia as redes sociais foram o canal privilegiado para a desinformação e para a disseminação de campanhas de *phishing*.

Mais recentemente, as instituições de ensino e a investigação registaram a taxa mais elevada de ciberataques, contando em média com 2.281 por semana, entre janeiro e julho de 2023, conforme é possível verificar na Figura 1 [4], uma vez que dispõem muitas vezes de poucos recursos, no que respeita a cibersegurança.

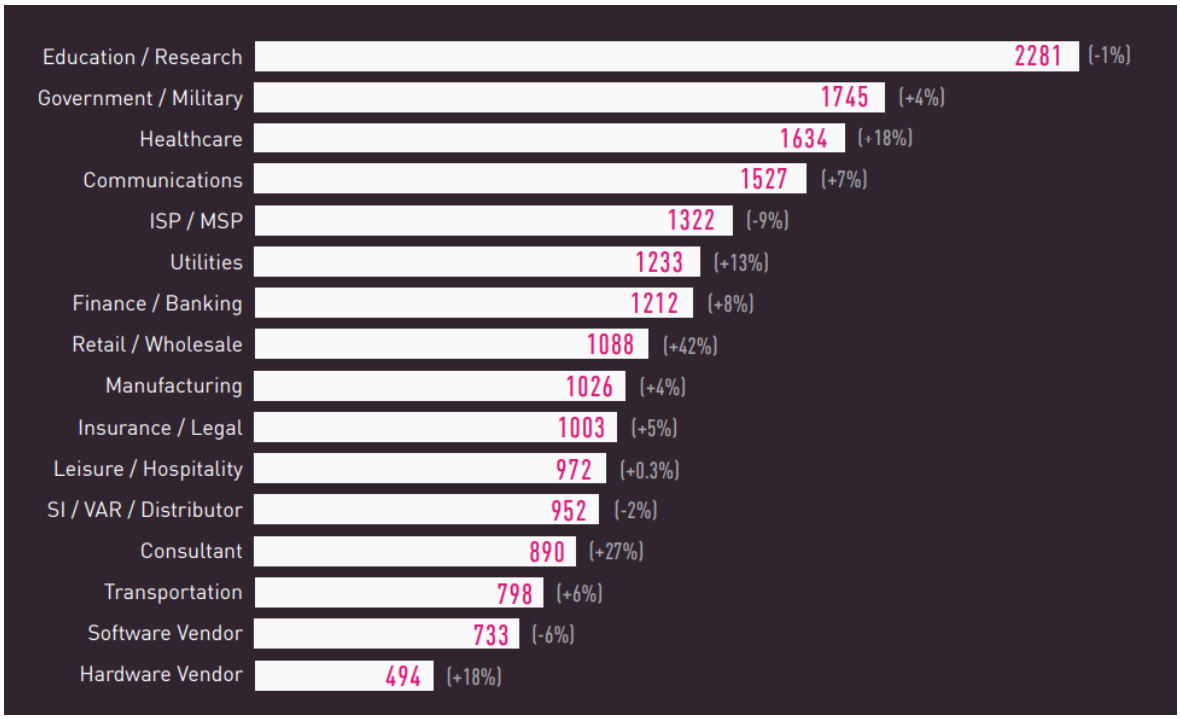


Figura 1 - Média Global de Ataques Semanais, por Setor no 1º Semestre 2023.

Fonte: 2023 Mid-Year Cyber Security Report (Check Point) [4]

As instituições, ao não aplicarem medidas de segurança, estão sujeitas a impactos reputacionais, digitais, económicos, físicos e sociais. Por exemplo, um ataque bem-sucedido pode inoperacionalizar os serviços essenciais para o correto funcionamento da instituição de ensino, resultar na perda, corrupção ou roubo de informação confidencial e, por conseguinte, colocar em causa a confiança da comunidade escolar na instituição de ensino. De acordo com o relatório *ENISA Threat Landscape 2023* [5] o setor da administração pública foi o setor mais visado entre julho de 2022 e junho de 2023 com uma taxa de 19%, o setor da educação e investigação ocupa a décima posição do *ranking* com uma taxa de 4%.

Relativamente ao tipo de ataque *Distributed Denial of Service* (DDoS) o setor industrial foi o mais afetado com 35% dos ataques. O setor financeiro, bancário e de seguros surge na segunda posição com mais de 30% de ataques, e na terceira e quarta posição surge o setor da administração pública e o setor da educação com 15% e 5%, respetivamente.

Uma vez que existe uma grande dependência das Tecnologias de Informação e Comunicação (TIC) no funcionamento das instituições de ensino, torna-se fundamental a definição de um guia de cibersegurança, através do qual as instituições de ensino consigam ter conhecimento dos riscos a que estão expostas e possam adequar as medidas de prevenção, preparação, resposta e recuperação, garantindo ao máximo as três propriedades que constituem a segurança da informação, nomeadamente:

- **Confidencialidade** - a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.
- **Integridade** - a informação é exata e completa.
- **Disponibilidade** - a informação é acessível e utilizável (a pedido de uma entidade autorizada).

Além das três propriedades apresentadas acima, existe a arquitetura AAA (Autenticação, Autorização e *Accounting*), que é essencial para garantir a segurança e o bom funcionamento de qualquer sistema que necessite de identificação e gestão de utilizadores [6], nomeadamente:

- **Autenticação** - processo pelo qual a identidade de um utilizador é verificada;
- **Autorização** - uma vez verificada a identidade do utilizador, é necessário estabelecer quais as ações e recursos que este está autorizado a utilizar no sistema;
- ***Accounting*** - é responsável por monitorizar as ações realizadas no sistema, por cada utilizador.

Desta forma, conclui-se que a tríade CID (Confidencialidade, Integridade e Disponibilidade) descreve as três propriedades que constituem a segurança da informação. Por outro lado, o modelo AAA descreve os métodos através dos quais as três propriedades, que constituem a segurança da informação, podem ser realizadas.

1.1.Motivação

As instituições de ensino dependem cada vez mais dos sistemas de Tecnologia de Informação e Comunicação (TIC), e estas têm na sua posse uma grande quantidade de dados confidenciais e sensíveis. Como resultado, tornam-se potenciais alvos de ciberataques. Um ataque cibernético a uma instituição de ensino pode afetar negativamente a sua capacidade de funcionamento, a sua reputação e as suas obrigações legais de manter dados pessoais sensíveis seguros e confidenciais.

Um bom Guia de Cibersegurança ajuda a proteger as instituições de ensino contra ciberataques prejudiciais que podem comprometer gravemente a capacidade de funcionamento de uma Escola. Também ajuda a impedir o acesso não autorizado a grandes quantidades de dados pessoais confidenciais armazenados nos sistemas de Tecnologia de Informação (TI).

A Cibersegurança deve, portanto, ser uma prioridade importante para as instituições de ensino que dependem das TIC. As direções dos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) devem ter conhecimento dos riscos a que estão expostos e prevenirem-se com planos para mitigar os impactos que os incidentes de segurança possam ter para a instituição.

Não é uma questão de se, mas sim quando a instituição de ensino vai ser atacada. Para estar preparada, é necessário ter um plano de cibersegurança bem definido e atualizado com regularidade.

1.2.Objetivos

O objetivo principal deste trabalho é avaliar quantitativamente, através de dados obtidos por meio de um questionário, o estado atual da cibersegurança nos Agrupamentos de Escolas e Escolas Não Agrupadas da região de Leiria.

De modo a atingir o objetivo principal, pretende-se estudar e analisar primeiramente o estado referente à área da cibersegurança, nomeadamente a legislação em vigor, os *standards* existentes e as boas práticas de segurança digital para suster o estudo empírico sobre o público-alvo do caso de estudo, de forma a apurar se as instituições de ensino estão em conformidade com a legislação, normas e regulamentos em vigor no âmbito da segurança da

informação, bem como se adotam algumas das recomendações e boas práticas de cibersegurança para proteger o seu espaço digital.

Resultado do estudo empírico, pretende-se ainda que o presente trabalho tenha um contributo prático. Deste modo, espera-se que este projeto possa contribuir academicamente para a segurança dos sistemas de TI dos AE e ENA do sistema de ensino português, com um guia de cibersegurança que permita auxiliar os responsáveis pelas TIC a definirem e implementarem uma estratégia de cibersegurança, identificando os principais pontos relevantes que devem ser tidos em conta.

1.3. Cronologia de Desenvolvimento do Projeto

O presente projeto seguiu uma sequência de várias fases que se encontram documentadas na Figura 2.

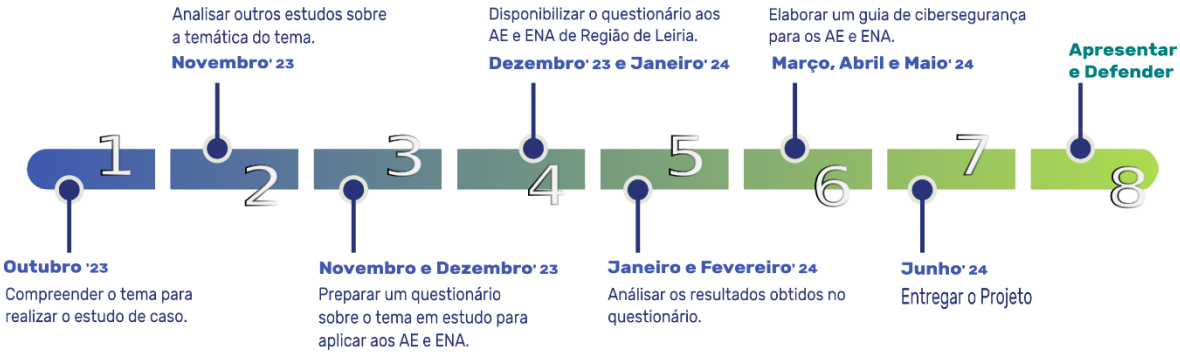


Figura 2 - Cronograma para a Realização do Projeto

O projeto teve início em outubro de 2023 com o estudo, compreensão do tema e análise do trabalho já realizado com a temática do presente projeto.

Na fase seguinte foi realizada uma análise cuidada a vários estudos que foram realizados no âmbito do presente tema, onde o foco principal incidiu sobre um inquérito realizado pela Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) à Administração Pública Central [7]. Foi também analisada uma aplicação de autoavaliação da MetaRed Portugal, utilizada no âmbito do projeto “ProtegeOTeuCampus” [8].

Seguiu-se a fase onde foi preparado um questionário de acordo com a análise realizada na fase anterior cujo objetivo foi permitir obter uma visão geral do panorama atual sobre o tema em estudo nos AE e ENA que pertencem à região de Leiria.

Na fase seguinte o questionário foi disponibilizado às 23 instituições de ensino participantes no estudo para que na fase posterior os dados obtidos no questionário fossem analisados.

Com os resultados obtidos, foi elaborado um guia de cibersegurança para auxiliar as instituições de ensino a reforçarem a sua presença no ciberespaço. Tendo sido este, no final, disponibilizado às instituições de ensino participantes.

1.4.Estrutura do Documento

O restante documento está estruturado em cinco capítulos que abordam os diferentes aspetos do trabalho realizado.

No segundo capítulo, será apresentado o estado da arte que procurou reunir informação sobre o sistema educativo português, a cibersegurança e a segurança da informação, a governança de cibersegurança, e por fim, os trabalhos relacionados com o presente estudo.

No terceiro capítulo, será descrita a metodologia de investigação, o método e técnicas para a recolha de dados, bem como todas as fases que compuseram este estudo. Para finalizar o capítulo são apresentados os dados recolhidos bem como a sua análise.

No quarto capítulo, é elaborado um guia de cibersegurança para as instituições de ensino.

Por fim, no último capítulo são apresentadas as conclusões deste trabalho, assim como quais foram as principais limitações encontradas e são elencados alguns aspetos que podem ser aprofundados futuramente.

2. Estado da Arte

Esta secção apresenta um conjunto de conceitos relativos à cibersegurança, nomeadamente a sua definição, a política pública, a cibersegurança no setor da educação, a cibercriminalidade e os dados do cibercrime em Portugal.

2.1. O Sistema Educativo Português

O Sistema Educativo Português é regulado pelo Ministério da Educação e pelo Ministério da Ciência, Tecnologia e Ensino Superior. O ensino público é o que apresenta uma taxa superior de oferta (79%), quando comparado com o ensino privado em que a taxa, no ano letivo 2021/22, foi de 21%, conforme é possível verificar na Figura 3. A taxa de implantação do ensino em Portugal é extremamente elevada, sendo a taxa de escolarização do pré-escolar e do ensino básico e secundário onde a evolução é mais significativa, com uma subida, de 0,9% e 1,3% em 1960/61, para 90,4% e 85,1% em 2020/21 [9].

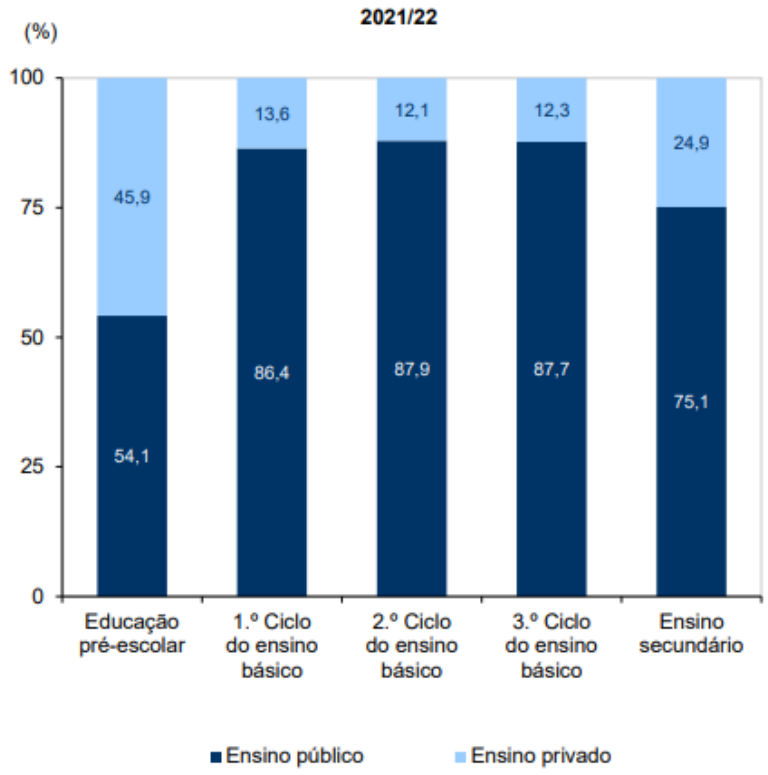


Figura 3 – Distribuição dos Níveis de Ensino pelas Escolas Públicas e as Escolas Privadas

Fonte: DGEEC, Recursos Tecnológicos das Escolas - 2021/2022 [9]

A partir de 1986, com a aprovação da Lei de Bases do Sistema Educativo [10], determinou-se que o Sistema Educativo Português, seria composto por:

- O ensino pré-escolar é de frequência facultativa e destina-se a crianças com idades entre os 3 anos, e a entrada no ensino básico, que corresponde à escolaridade obrigatória;
- O ensino básico está estruturado em três ciclos sequenciais: 1º ciclo, 2º ciclo e 3º ciclo, com uma duração de 4, 2 e 3 anos, respetivamente;
- O ensino secundário tem como referência três anos letivos (10º, 11º e 12º) com cursos orientados para quem pretende prosseguir estudos, ou para quem pretende iniciar-se no mundo do trabalho;
- O ensino pós-secundário, não superior, encontra-se organizado em Cursos de Especialização Tecnológica (CET), com uma visão mais orientada ao mundo do trabalho e com um nível 4 de formação profissional;
- O ensino superior, que se encontra estruturado ao abrigo dos princípios da Declaração de Bolonha [11] e é ministrado em universidades, institutos politécnicos, sejam eles de natureza pública ou privada. Ainda no ensino superior, realça-se o aparecimento dos Cursos Técnicos Superiores Profissionais (CTeSP), que têm uma duração de 2 anos letivos.

O sistema de educação e formação integra ainda as seguintes modalidades:

- educação especial;
- formação profissional;
- educação de adultos;
- ensino à distância;
- ensino português no estrangeiro.

Na Figura 4 é possível visualizar uma representação do atual Sistema Educativo Português.

Figura 4 - Organização do Sistema Educativo Português

Fonte: DGEEC, Educação e Formação em Portugal (2021) [12]

O marco inicial do Sistema de Educação em Portugal teve início no ano letivo 1944/1945, com 657.368 alunos inscritos, quando comparado com o ano letivo 2020/21, no qual o número de alunos matriculados/inscritos era 1.987.674. A taxa de crescimento é de 202,4%, conforme é possível verificar na Figura 5.

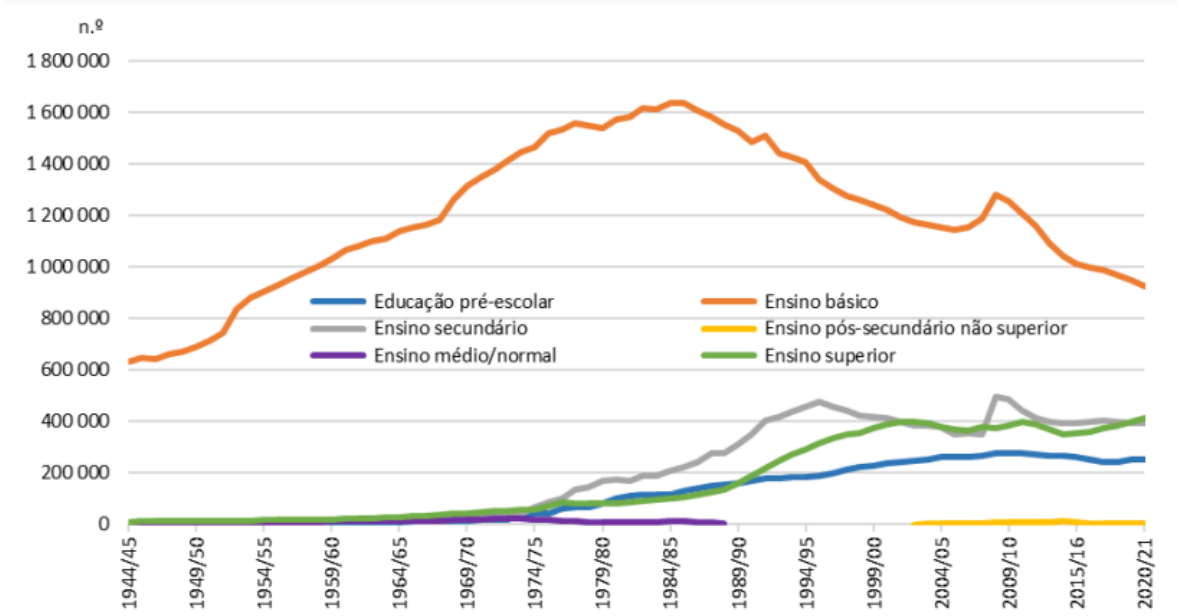


Figura 5 - Número de Alunos Matriculados 1944 a 2021

Fonte: DGEEC, 75 anos de estatísticas da Educação em Portugal [13]

O ano letivo onde se verificou o maior número de alunos inscritos/matriculados foi em 2008/09, com 2.435.665, conforme é possível verificar na Figura 6.

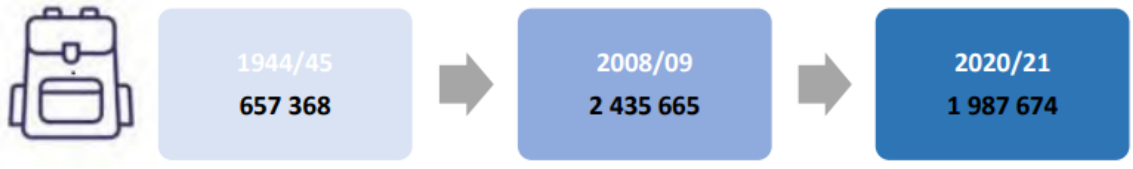


Figura 6 - Número de Alunos Inscritos/Matriculados

Fonte: DGEEC, Educação e Formação em Portugal (2021) [12]

Relativamente ao número total de educadores de infância e de docentes dos ensinos básico e secundário, entre o ano letivo de 1956/57, e o ano letivo 2020/21, este teve um crescimento de 379,9%. No ano letivo 1956/57 contava com 31.286, e no ano letivo 2010/21 com 150.127, sendo que o ano letivo com o valor mais elevado foi o 2004/05, com 185.157 educadores e docentes, conforme é possível verificar na Figura 7.

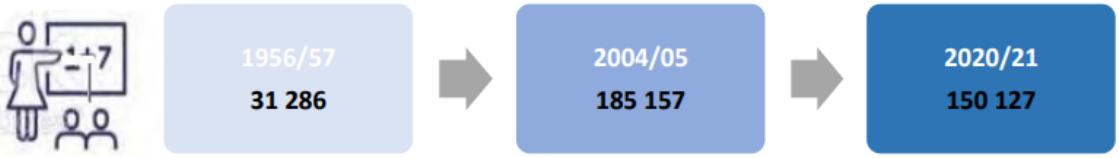


Figura 7 - Número de Docentes e Educadores

Fonte: DGEEC, Educação e Formação em Portugal (2021) [12]

Os últimos dados divulgados pela DGEEC [9], são referentes ao ano letivo 2021/22 e os níveis de ensino do pré-escolar até ao secundário, onde o total de alunos inscritos/matriculados é 1.586.453, 150.649 docentes, e 77.032 não docentes, num total de 8.199 estabelecimentos de ensino, conforme é possível verificar o resumo na Tabela 1.

Dados referentes ao Ano Letivo 2021/22		
Alunos	**Total**	**1 586 453**
	Educação pré-escolar	259 030
	1.º Ciclo do ensino básico	374 620
	2.º Ciclo do ensino básico	212 914
	3.º Ciclo do ensino básico	342 789
	Ensino secundário	397 100

Docentes	**Total**	**150 649**
	Educação pré-escolar	17 260
	1.º Ciclo do ensino básico	31 149
	2.º Ciclo do ensino básico	23 415
	3.º Ciclo do ensino básico e ensino secundário	78 825
Pessoal não docente		**77 032**
Estabelecimentos de ensino		**8 199**

Tabela 1 - Números de Alunos, Docentes e Não Docentes do Ano Letivo 21/22

2.1.1. Definição de Agrupamento de Escolas e Escolas Não Agrupadas

Os Agrupamentos de Escolas (AE) são hoje, de acordo com a lei, entidade orgânicas, dotadas de órgãos próprios de administração e gestão, que integram os estabelecimentos de ensino do pré-escolar, e escolas de diferentes níveis e ciclos de ensino [9]. Um dos princípios para a criação dos agrupamentos de escolas foi a partilha de recursos materiais e humanos entre estabelecimentos de ensino, e a tomada de decisões conjuntas, com o objetivo de melhorar a qualidade do ensino. No agrupamento de escolas existe sempre um Estabelecimento de Ensino (EE) designado por Escola Sede (ES), e é nesta que a direção do agrupamento desempenha as suas funções de assegurar a organização e o funcionamento de todos os estabelecimentos de ensino que compõem o agrupamento de escolas, conforme é possível verificar na Figura 8.

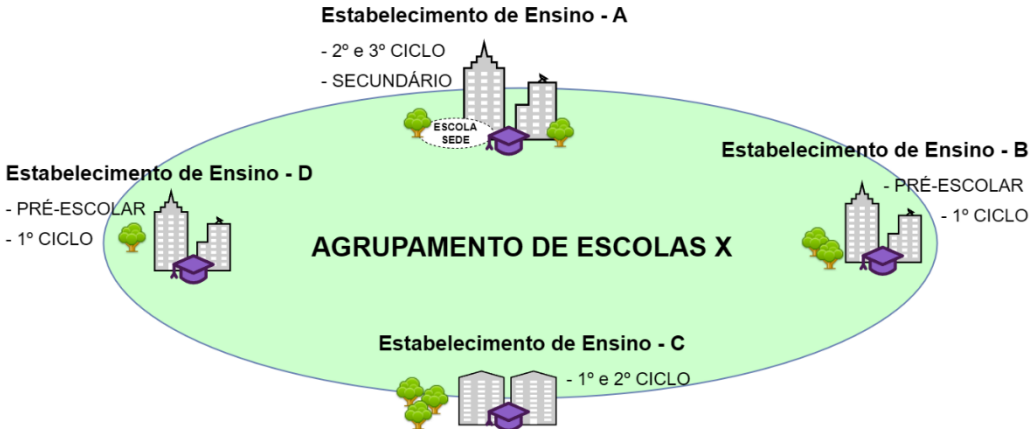


Figura 8 - Exemplo da Composição de um Agrupamento de Escolas.

Uma Escola Não Agrupada (ENA) é um estabelecimento de ensino que possui autonomia administrativa e pedagógica, ou seja, opera de forma isolada das outras instituições de ensino. Como não pertence a nenhum agrupamento de escolas pode tomar decisões por conta

própria, sem a necessidade de coordenação e partilha de recursos com outras instituições de ensino, conforme é possível verificar na Figura 9.

Figura 9 - Exemplo de uma Escola Não Agrupada

2.1.2. Recursos Tecnológicos nas Escolas

De acordo com o último estudo realizado pela Direção-Geral de Estatísticas da Educação e Ciência – DGEEC, intitulado de "Recursos Tecnológicos das Escolas 2021/2022" [14], é possível verificar dados estatísticos e oficiais sobre os recursos tecnológicos existentes em estabelecimentos de ensino tutelados pelo Ministério da Educação e Ciências, sendo eles públicos e privados, geograficamente localizados no Continente. Este estudo contempla os equipamentos (computadores portáteis) e ligações à Internet disponibilizados a alunos no âmbito do "Projeto Escola Digital" [15].

No gráfico da Figura 10 é possível verificar os computadores, por tipologia do estabelecimento de ensino, nomeadamente o Jardim de Infância, o Ensino Básico, o Ensino Básico e Secundário, e o Ensino Secundário. De acordo com os dados apurados, os estabelecimentos de ensino, apenas com o Ensino Básico, são as que têm mais computadores alocados.

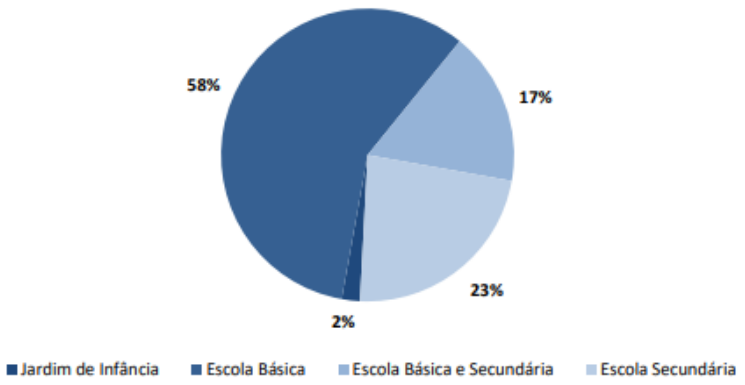


Figura 10 - Computadores por Tipologia do Estabelecimento de Ensino (Total)

Fonte: Recursos Tecnológicos das escolas 2021/2022 (DGEEC) [14]

Na Figura 11 é possível verificar os computadores, por natureza e tipologia do estabelecimento de ensino. O maior destaque incide na quantidade de computadores existentes no Ensino Público, que corresponde a 826.450, num universo de 900.556.

	N	%
Total	**900 556**	**100**
Jardim de Infância	14 490	2
Escola Básica	524 741	58
Escola Básica e Secundária	155 802	17
Escola Secundária	205 523	23
Público	**826 450**	**92**
Jardim de Infância	2 969	0
Escola Básica	511 542	62
Escola Básica e Secundária	129 630	16
Escola Secundária	182 309	22
Privado dependente do Estado	**19 199**	**2**
Jardim de Infância	8 618	45
Escola Básica	3 184	17
Escola Básica e Secundária	6 562	34
Escola Secundária	835	4
Privado independente do Estado	**54 907**	**6**
Jardim de Infância	2 903	5
Escola Básica	10 015	18
Escola Básica e Secundária	19 610	36
Escola Secundária	22 379	41

Figura 11 - Computadores por Natureza e Tipologia do Estabelecimento de Ensino

Fonte: Recursos Tecnológicos das Escolas 2021/2022 (DGEEC) [14]

Na Figura 12 é possível verificar o tipo de computador, bem como a sua finalidade e antiguidade. Num total de 900.556 computadores, 856.710 são para fins pedagógicos, e 43.846 para fins administrativos. Um dado importante é o facto de 72,31% dos computadores para fins administrativos já terem mais de 3 anos, o que poderá colocar em causa a segurança dos mesmos no acesso à Internet e da informação que armazenam.

	Total		Inferior ou igual a 3 anos		Superior a 3 anos	
	N	%	N	%	N	%
Total Computadores	**900 556**	**100**	**664 769**	**100**	**235 787**	**100**
Para fins pedagógicos	856 710	95	652 629	98	204 081	87
Para fins administrativos	43 846	5	12 140	2	31 706	13
Computadores de secretária (não portáteis)	**197 688**	**22**	**23 705**	**4**	**173 983**	**74**
Para fins pedagógicos	161 212	82	14 529	61	146 683	84
Para fins administrativos	36 476	18	9 176	39	27 300	16
Computadores portáteis	**660 557**	**73**	**625 282**	**94**	**35 275**	**15**
Para fins pedagógicos	654 128	99	622 831	100	31 297	89
Para fins administrativos	6 429	1	2 451	0	3 978	11
Tablets / iPads	**42 311**	**5**	**15 782**	**2**	**26 529**	**11**
Para fins pedagógicos	41 370	98	15 269	97	26 101	98
Para fins administrativos	941	2	513	3	428	2

Figura 12 - Computadores por Tipo, Finalidade e Antiguidade

Fonte: Recursos Tecnológicos das Escolas 2021/2022 (DGEEC) [14]

Relativamente aos servidores existentes nas instituições públicas de ensino não foi identificado qualquer estudo.

2.1.3. Rede alargada da Educação

O projeto "Rede Alargada da Educação" (RAE), promovido pelo Ministério da Educação e Ciência (MEC) teve o seu início em setembro de 2008, com o objetivo de garantir melhores serviços de comunicações e sistemas de informação aos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA), no território de Portugal Continental [16].

De acordo com a informação divulgada pela FCCN [17], unidade da Fundação para a Ciência e Tecnologia (FCT), a RAE é uma infraestrutura com cobertura nacional que interliga um total de cerca de 4.435 escolas e com cerca de 1 milhão de utilizadores (alunos, docentes e administrativos) registados. De entre os serviços que disponibiliza, destacam-se as ligações à Internet de todos os estabelecimentos da rede pública (do 1.º ciclo do Ensino Básico até ao Ensino Secundário), bem como de todos os organismos regionais e centrais do Ministério de Educação e Ciência.

É possível identificar um conjunto alargado de serviços que são disponibilizados aos vários organismos do MEC, nomeadamente:

- rede nacional de comunicação de dados (WAN);
- estrutura de diretórios;
- gestão do serviço de correio eletrónico;
- gestão do serviço de resolução de nomes (DNS);
- vários tipos de alojamento de plataformas e virtualização;
- serviços de Voz sobre IP (VoIP);
- serviço de visualização de *desktop* (DaaS);
- sistemas de gestão e alojamento de bases de dados diversas;
- componente de cibersegurança de toda a rede dos organismos do MEC em conjunto com os serviços disponibilizados pelo fornecedor de serviço de Internet e pela FCT.

Relativamente ao serviço de Internet prestado às escolas, na atual configuração, cada lote de agrupamentos e escolas não agrupadas constituí uma Rede Privada Virtual (VPN), num total de 3, que estão fisicamente interligadas através de meios de comunicação ao ponto central. O ponto central garante as medidas de segurança e a interligação, assim como a entrega e receção de todo o tráfego de, e para a Internet. Por sua vez a componente de Internet é disponibilizada pela Rede Ciência, Tecnologia e Sociedade (RCTS), conforme ilustrado na Figura 13.

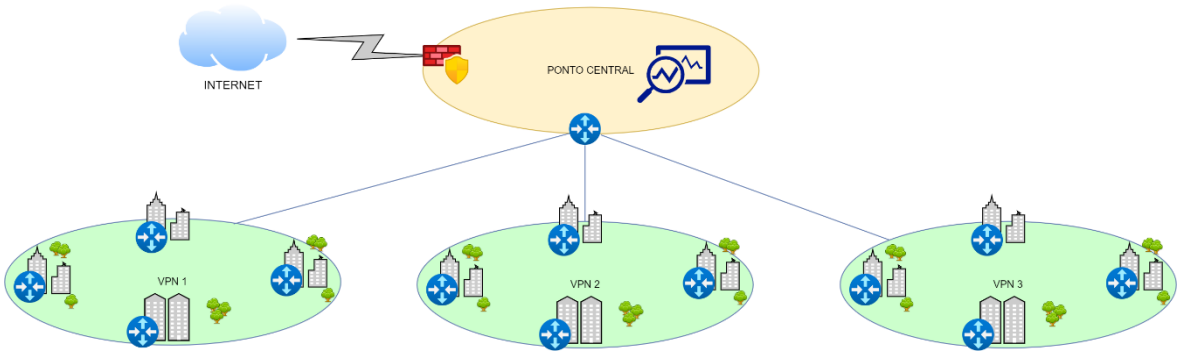


Figura 13 - Segmentação dos AE e ENA por 3 Lotes (VPN)

A gestão dos endereços IP públicos dos AE e ENA, passaram a estar sob a responsabilidade da Direção-Geral de Estatísticas da Educação e Ciência (DGEEC). Existe também a partilha de aplicações e informação entre as diversas escolas agrupadas, e as escolas sede de Agrupamento, que estão na mesma rede de dados, de forma a não aumentar a largura de banda de acesso à Internet. Estes serviços são de extrema importância para a eficácia do funcionamento de todos os procedimentos relacionados com a gestão escolar e permitem, na

prática, que vários polos geograficamente separados do mesmo agrupamento de escolas operem como se estivessem no mesmo espaço físico.

A nível das plataformas suportadas são mantidos os seguintes serviços tecnológicos:

- Portal das escolas;
- Informação das escolas;
- Informação dos cursos;
- Portal das qualificações;
- Sistema de Informação e Gestão da Oferta Educativa e Formativa (SIGO);
- Sistema de importação, gestão e armazenamento de dados das escolas e agrupamentos (MISI);
- *Scientific Electronic Library Online* (SciELO), biblioteca eletrónica que abrange uma coleção selecionada de periódicos científicos.

2.1.4. Medidas de segurança anunciadas pela DGEEC

A DGEEC em 2014, apresentou um conjunto de medidas a implementar nas escolas do ensino básico e secundário [18], nomeadamente:

- Realização de um diagnóstico relativamente à segurança digital da escola, através de um portal disponibilizado para o efeito. Após a realização da candidatura ao selo de segurança digital [19] foi definido um plano de ação, para os agrupamentos e escolas não agrupadas procederem às melhorias sugeridas;
- Ao nível da proteção de dados e dados pessoais, devem ser aplicadas medidas tecnológicas ao nível da exposição ao exterior dos servidores que contenham bases de dados ou informação sensível. O acesso a servidores ou sistemas através do protocolo *Remote Desktop Protocol* (RDP), deve ser condicionado, limitando o acesso a sistemas ou redes confiáveis. O RDP não deve estar acessível a partir do exterior da escola. Caso se opte por expor os servidores para a Internet, o seu acesso deverá ser protegido com credenciais de acesso robustas;
- A comunicação entre os estabelecimentos de ensino do mesmo Agrupamento, para acesso aos servidores/sistemas, deve ser realizada através da RAE. Não deve ser utilizada a comunicação entre escolas mediante a utilização de IP públicos, mas apenas mediante a solução já apresentada e sem encargos para as escolas;

- Havendo a necessidade de expor servidores ao exterior, tal deve acontecer através da RAE e não com a utilização de outros acessos à Internet. Os acessos à Internet fornecidos pelo MEC estão protegidos com uma *firewall* central que, embora não atue sobre portos de entrada permitidos, permite analisar mais facilmente potenciais ataques e tomar medidas preventivas;
- Devem ser escolhidos fornecedores de serviços que assegurem canais de comunicação seguros e com certificados digitais de segurança, para garantir que a transmissão de dados via Internet com recurso a serviços, aplicações e/ou sistemas com interface Web é segura;
- Devem ser realizadas cópias regulares de segurança (*backups*) da informação para suportes que posteriormente são desligados e permanecem *off-line*. De preferência, devem ser realizados *backups* totais para aumentar a possibilidade de recuperação total de dados;
- Desenvolvimento de uma política da instituição de ensino para as questões da segurança digital, contribuindo para a proteção e privacidade dos dados dos alunos, professores e restante comunidade educativa.

2.1.5. Transferência de Competências

No reconhecimento de que as autarquias locais são a estrutura essencial para a gestão de serviços públicos numa dimensão de proximidade, a Lei n.º 50/2018 de 16 de agosto [20], veio estabelecer o quadro da transferência de competências para as autarquias locais e para as Comunidades Intermunicipais (CIM) em diversos domínios de atuação do Estado, onde se inclui a Educação [21].

Nesta ótica, foram publicados vários diplomas do âmbito setorial, entre os quais o Decreto-Lei n.º 21/2019, de 30 de janeiro [22], posteriormente alterado pelo artigo 189.º do Decreto-Lei n.º 84/2019, de 28 de junho que estabelece as disposições necessárias à execução do Orçamento do Estado para 2019, aprovado pela Lei n.º 71/2018, de 31 de dezembro [23], que concretiza o quadro de transferência de competências para os órgãos municipais e para as entidades intermunicipais no domínio da educação.

Neste domínio, os órgãos municipais passaram, entre outras ações, a participar na aquisição de bens e serviços relacionados com o funcionamento dos estabelecimentos e a recrutar, selecionar e gerir o pessoal não docente inserido nas carreiras de assistentes operacional e de assistente técnico, no que se refere à rede pública de educação pré-escolar e de ensino

básico e secundário, incluindo o ensino profissional. Estas funções eram anteriormente da competência do governo central.

Assim, ao abrigo do referido Decreto-Lei, até ao dia 31 de março de 2022 todas as competências no âmbito da Educação foram transferidas para as autarquias locais e comunidades intermunicipais.

2.1.6. Proteção de dados em contexto escolar

As instituições de ensino no desenvolvimento das suas funções e atividades operam com vários tipos de tratamento de dados pessoais. A especificidade inerente ao tratamento de dados de menores, alguns deles de grande sensibilidade, impõe naturalmente responsabilidades e cuidados acrescidos na proteção dessa informação pessoal e confidencial. As escolas armazenam também dados pessoais relativos ao pessoal docente e não docente, das filiações (pai e mãe) e dos encarregados de educação [24].

Com o crescimento da informatização das instituições de ensino, o desenvolvimento e disponibilização de plataformas digitais, surgiram novos riscos, que devem acautelar a segurança dos dados e minimizar as potencialidades da sua utilização indevida.

2.2. Cibersegurança e Segurança da Informação

A informação é um ativo importante e crucial nos tempos atuais, e a sua proteção tornou-se essencial para a continuidade de negócio e sucesso das organizações. De acordo com a Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho [25], a cibersegurança pode ser definida 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."*.

As definições formais de segurança da informação, cibersegurança, segurança de redes de computadores e segurança física, entre outras, é assegurada pelo *National Institute of Standards and Technology* (NIST) [26]. Genericamente, 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"*.

A segurança da informação assenta sobre três pilares, conforme se ilustra na Figura 14, habitualmente designados pela tríade CIA (C*onfidentiality, Integrity and Availability*).

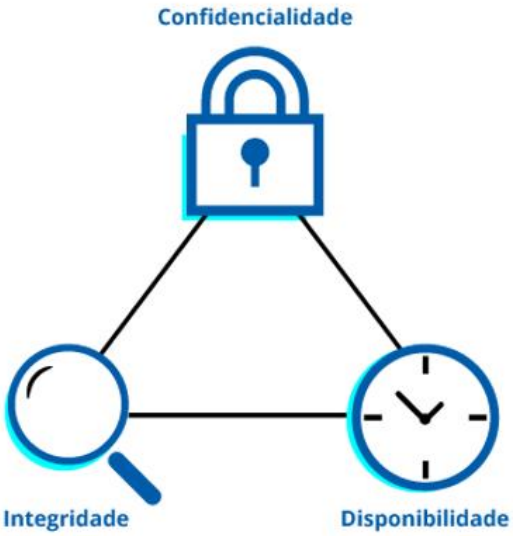


Figura 14 - Três Pilares da Segurança da Informação

2.2.1. Tipos de Ataques Cibernéticos

Segundo a Cisco [27], um ataque cibernético é uma tentativa maliciosa e deliberada de um indivíduo ou grupo de indivíduos violarem o sistema de informação de outro indivíduo ou organização. Existem vários tipos de ataques cibernéticos [28], uns mais conhecidos do que outros, que têm como objetivo causar falhas no serviço, extorquir dinheiro, obter informações com motivações políticas, ou, em casos mais extremos, danificar sistemas com o pretexto de criar o pânico.

Deste modo, resumem-se de seguida, alguns dos ciberataques mais comuns que acontecem diariamente no ciberespaço.

Malware – Um *malware*, ou software malicioso, é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas [29]. Alguns dos exemplos são: *Adware, Spyware, Vírus, Worms, Trojan, Ransomware, Rootkit, Keylogger*, Criptomineração Maliciosa, *Exploits*, entre outros. Destes, os mais conhecidos são:

- *Trojan* (cavalo de tróia) [30], apresenta-se ao utilizador do sistema com algo útil de forma a enganar o utilizador, mas quando entra no sistema, consegue obter acesso não autorizado ao sistema em causa, e rouba informações financeiras ou até instala outras ameaças.

- *Ransomware* [31], bloqueia o acesso a um dispositivo e/ou cifra os ficheiros existentes no sistema e, normalmente, é exigido o pagamento de um resgate para a devolução da chave que foi utilizada para cifrar os dados. Atualmente, é a ameaça mais comum dos atacantes, uma vez que implica um pagamento em criptomoeda [32], cujo rasto é difícil de seguir.

Phishing - É um tipo de ataque onde são aplicadas técnicas de engenharia social para obter informação sensível de uma vítima através de um e-mail. O atacante que utiliza este tipo de ataque procura ludibriar os recetores de e-mails para que estes disponibilizem informação sensível através do clique em anexos e/ou *URL* maliciosos, ou da partilha de dados em páginas fraudulentas, conforme exemplo da Figura 15. Para o efeito, o atacante falseia uma marca credível ou representa alguém de confiança. Quando esta técnica é utilizada através de *SMS*, dá pelo nome de *smishing* e, por telefone (voz), de *vishing*. Esta técnica também pode ser aplicada através das mensagens instantâneas em aplicações de redes sociais [33].

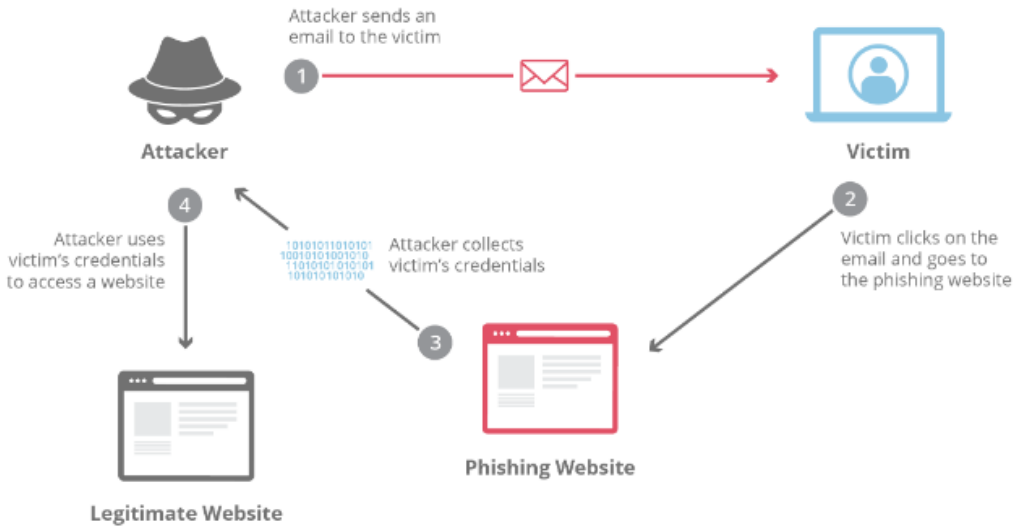


Figura 15 - Ataque de *Phishing*

Fonte: Cloudflare, What is a phishing attack? [34]

Man-In-The-Middle **(MITM)** - é um tipo de ataque em que o atacante interceta uma conversa existente ou transferência de dados. O atacante consegue infiltrar-se no meio da conversa/transferência, e o atacante finge ser ambos participantes legítimos, conforme exemplo da Figura 16. Desta forma, o atacante interceta informação e dados de qualquer uma das partes, ao mesmo tempo que envia *links* maliciosos ou outras informações a ambos os participantes legítimos [31].

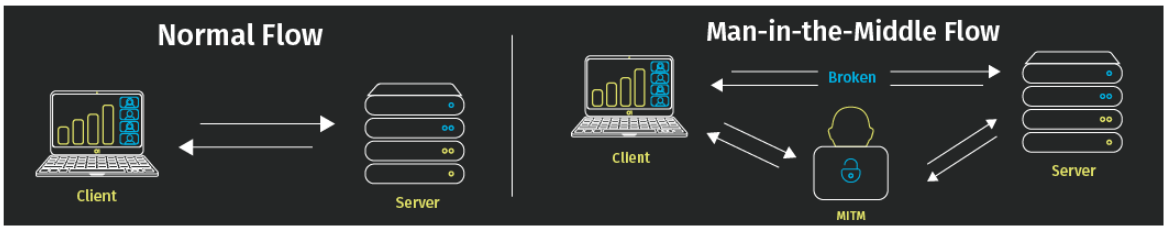


Figura 16 - Ataque *Man-in-the-middle attack* (MITM)

Fonte: *Veracode, Man in the Middle (MITM) Attack* [35]

***Distributed Denial-of-Service* (DDoS)** - Um ataque distribuído de negação de serviço (DDoS) é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede, sobrecarregando o alvo ou a infraestrutura circundante com um número anormal (excessivo) de tráfego de dados [36]. Exemplos destes ataques são o *Internet Control Message Protocol* (ICMP) *flodding* (ou *smurf attack* ou *ping of death*), nestes o atacante aproveita dispositivos de rede mal configurados e envia pacotes falsificados que executam *ping* aos computadores da rede de destino. Outro tipo é o *SYN flodding*, no qual o atacante envia pacotes de *SYN* para vários portos, mas sem concluir o *handshake* do *Transmission Control Protocol* (TCP), fazendo com que os utilizadores legítimos tenham dificuldades no acesso. Um outro tipo é o ataque *Denial-of-service* (DoS) [31], que se caracteriza por ser apenas uma fonte a realizar o ataque, conforme exemplo da Figura 17.

Figura 17 – Ataque DoS

Fonte: *Cloudflare, What is a DDoS attack?* [37]

SQL injection - O *SQL injection* é uma falha de segurança, ainda muito comum, que permite ao atacante consultar informação de uma ou várias bases de dados de uma determinada aplicação/sistema, conforme exemplo da Figura 18. Nestes casos, o atacante pode modificar ou apagar informação da base dados, causando assim alterações persistentes no conteúdo ou comportamento da aplicação/sistema [38].

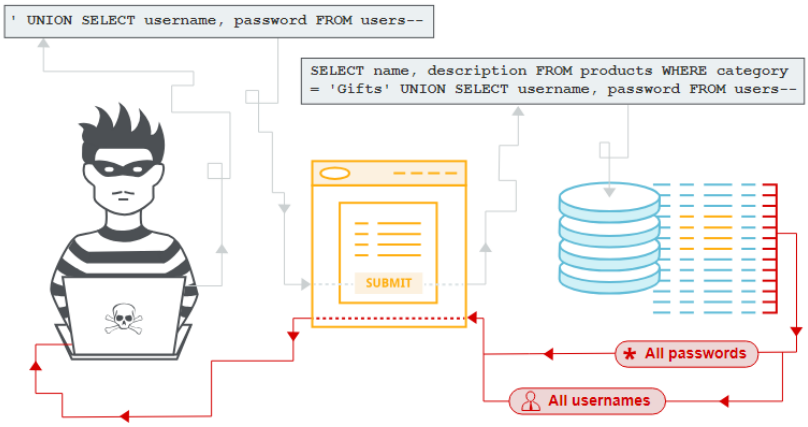


Figura 18 - Ataque SQL *Injection*

Fonte: *PortSwigger, SQL injection* [39]

Zero-day exploit - Uma exploração de dia zero (também designada por ameaça de dia zero) é um ataque que tira vantagem de uma vulnerabilidade de segurança, para a qual ainda não existe uma correção por parte do fabricante. É chamada de ameaça de dia zero porque, uma vez descoberta a falha, o fabricante/organização tem zero dias para encontrar uma solução [40].

DNS Tunneling - Um ataque de *DNS Tunneling*, (também conhecido por encapsulamento de DNS) é um ataque que consiste em explorar o DNS para ocultar dados em pedidos e respostas DNS. A informação pode ser codificada e escondida nos pedidos de DNS, de modo a enviar dados confidenciais para um atacante [41], conforme exemplo da Figura 19.

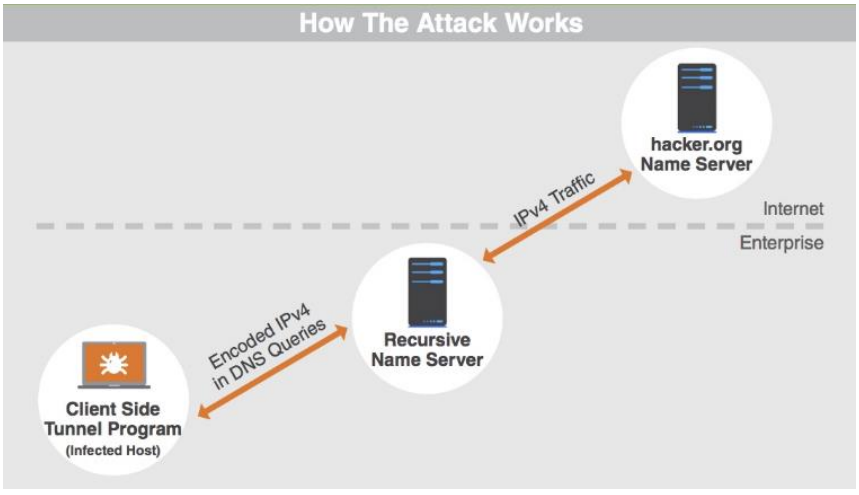


Figura 19 - Ataque DNS *Tunneling*

Fonte: *InfoBlox, What is DNS Tunneling?* [42]

2.2.2. A Cibersegurança como Política Pública

A Cibersegurança, entendida como política pública, possui uma natureza transversal que abrange diversas áreas setoriais e está cada vez mais presente devido à aceleração do processo de transição digital das instituições públicas. Os riscos e ameaças à segurança das redes e sistemas de informação aumentam, apresentando desafios significativos para as entidades que dependem desses recursos para as suas atividades [43].

Em Portugal, as estratégias, programas e ações no domínio da Cibersegurança são fundamentadas num conjunto de dispositivos legais e regulamentares que estabelecem o quadro normativo de referência para o desenvolvimento e implementação de políticas de segurança do ciberespaço. Além disso, há uma componente institucional responsável pelo planeamento, execução, monitorização e fiscalização do cumprimento desse quadro normativo, designadamente o direito à cibersegurança, impondo ao Estado o dever de definir políticas públicas que garantam a proteção dos cidadãos e das redes e sistemas de informação [44].

A participação de Portugal na União Europeia, bem como em organizações internacionais como a *North Atlantic Treaty Organization* (NATO) e a *Organization for Security and Co-operation in Europe* (OSCE), influencia o panorama jurídico-político nacional em Cibersegurança, uma vez que, as medidas adotadas e os compromissos assumidos nessas organizações, têm um impacto direto nas políticas internas. A cooperação internacional é essencial para a prevenção e resolução de incidentes, bem como para a construção de um ciberespaço mais seguro, numa sociedade cada vez mais digital.

Agência da União Europeia para Cibersegurança

A Agência da União Europeia para Cibersegurança (ENISA) foi criada em 2004 e reforçada em 2019 pelo Regulamento Cibersegurança da EU [45], e contribui para a política do ciberespaço da União Europeia (UE), reforçando a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, cooperando com os Estados-Membros e os organismos da UE, e ajuda a Europa a preparar-se para os desafios de segurança do ciberespaço que se avizinham. Através da partilha de conhecimentos, do reforço de capacidades e da sensibilização, a ENISA trabalha em colaboração com os seus principais *stakeholders* para reforçar a confiança, aumentar a resiliência das infraestruturas da UE e manter a segurança digital da sociedade e dos cidadãos europeus [46].

Centro Nacional Cibersegurança

O Centro Nacional de Cibersegurança é criado a 6 de outubro de 2014, dentro do Gabinete Nacional de Cibersegurança, através do Decreto-Lei n.º 69/2014, de 9 de maio com a designação "CNCSeg" [47]. O CNCS adquire a sua designação atual (CNCS) através do Decreto-Lei n.º 136/2017, de 6 de novembro [48]. O CNCS tem como missão contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional. Atua como coordenador operacional e autoridade nacional em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais. O CNCS transporta também a sua ação para a sociedade em geral.

2.2.3. Dados recentes do Cibercrime em Portugal

A Equipa de Resposta a Incidentes de Segurança Informática Nacional, designada por CERT.PT, no ano de 2022, recebeu e processou 8.971 notificações, mais 48,7% que no ano anterior, em que cerca de 22,6% dessas notificações resultaram na abertura de incidentes de Cibersegurança analisados e resolvidos. Destes incidentes de segurança, "33,2% afetaram entidades da Administração Pública", verificando-se assim um aumento em relação ao ano anterior [49].

Por tipologia de incidentes, registou-se no ano 2022 um aumento na abertura de incidentes em todas as classes, nomeadamente:

- **Fraude**, registaram-se 871 (+68 em relação ao período homologo);
- **Código malicioso**, registaram-se 300 (+25 em relação ao período homologo);
- **Intrusão**, registaram-se 202 (+48 em relação ao período homologo);
- **Recolha de informação**, registaram-se 300 (+39 em relação ao período homologo).

As restantes classes registaram a abertura de 350 incidentes, mais 62 em relação ao período homologo.

À semelhança dos relatórios de anos transatos, os ataques de *Phishing* e *Smishing*, este último com um forte crescimento em 2022, continuam a dominar. As marcas utilizadas nestas campanhas afetam entidades do setor bancário e serviços financeiros, entidades do setor de transporte e logística, e entidades fornecedoras de serviços de e-mail eletrónico. Estas campanhas têm como objetivo principal a recolha de credenciais de acesso do serviço

homebanking, e recolha de dados de cartões de crédito ou débito. Adicionalmente, registaram-se várias campanhas com o intuito de recolha de credenciais de acesso, que são posteriormente utilizadas como vetor inicial de ataques de *ransomware*.

2.3. Governança de Cibersegurança

Nesta secção iremos abordar algumas leis, normas, recomendações e boas práticas existentes no âmbito da cibersegurança, que vamos analisar, de modo a servir de base para a proposta que foi apresentada aos AE/ENA.

2.3.1. A Lei de Cibersegurança em Portugal

A Legislação Portuguesa 46/2018 [50] estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148 [50] 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. Além disso, o Decreto-Lei 65/2021 [51] regula o regime jurídico da segurança do ciberespaço, e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Em Portugal, a Assembleia da República aprovou o regime de segurança do Ciberespaço (Lei nº 46/2018, de 13 de agosto), transpondo a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, sobre medidas para garantir um alto nível de segurança de redes e informações em toda a União Europeia [52].

A Lei aprovada pelo Parlamento Europeu prevê:

- A definição de uma Estratégia Nacional de Segurança do Ciberespaço;
- A estrutura nacional de segurança do ciberespaço, incluindo a criação do Conselho Superior de Segurança do Ciberespaço;
- Identificar o Ponto de Contato Nacional (PCN) para cooperação internacional;
- A definição dos requisitos de segurança em redes e sistemas de informação;
- A aprovação das obrigações de comunicação de incidentes ao Centro Nacional de Cibersegurança (CNCS);
- A definição do regime de delitos aplica-se à violação da lei;

- O Centro Nacional de Segurança Cibernética é a Autoridade Nacional de Segurança Cibernética, e a equipa nacional de resposta a incidentes de segurança cibernética (CSIRT) está subordinada a ela.

A Lei 46/2018 estabelece regras para a Administração Pública, para os operadores de infraestruturas críticas, para os operadores de serviços essenciais, para os prestadores de serviços digitais e para quaisquer outras entidades que utilizem redes e sistemas de informação. Para efeitos do disposto na Lei 46/2018, integram a Administração Pública: o Estado, as regiões autónomas, as autarquias locais, as entidades administrativas independentes, os institutos públicos, as empresas públicas, e as associações públicas.

No âmbito deste trabalho de projeto e de modo a validar se os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) estão sujeitas ao cumprimento das leis aplicadas à Administração Pública, foi enviado um e-mail ao Centro Nacional de Cibersegurança (CNCS) a solicitar a confirmação desta informação. A resposta obtida, veio confirmar que os AE e ENA têm as mesmas obrigações que as restantes entidades da Administração Pública, conforme é possível verificar na transcrição abaixo.

Nos termos previstos na alínea a) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, encontra-se abrangida pelo âmbito de aplicação deste regime jurídico a Administração Pública.
A tipologia de entidades no âmbito de aplicação do Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019, consta do n.º 1 do artigo 2.º do referido normativo o qual remete para as alíneas a) a d) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto.
Nos termos do artigo 75.º da Constituição da República Portuguesa, o Estado cria uma rede de estabelecimentos públicos de ensino. De acordo com o enquadramento estabelecido na Lei n.º 46/86, de 14 de outubro, que estabelece a Lei de Bases do Sistema Educativo, respetivamente no artigo 40.º, e nos termos previstos no n.º 1 do artigo 6.º do Decreto-Lei n.º 75/2008, de 22 de abril, que aprova o regime de autonomia, administração e gestão dos estabelecimentos públicos da educação pré-escolar e dos ensinos básico e secundário, o agrupamento de escolas é uma unidade organizacional,

dotada de órgãos próprios de administração e gestão, constituída por estabelecimentos de educação pré-escolar e escolas de um ou mais níveis e ciclos de ensino.
A Administração Pública integra os agrupamentos de escolas, no âmbito do Ministério da Educação e da Direção-Geral dos Estabelecimentos Escolares, como rede pública de estabelecimentos de ensino, ficando por isso no âmbito de aplicação da Lei 46/2018, de 13 de agosto, e do Decreto-Lei n.º 65/2021, de 30 de julho.

2.3.1. Quadro Nacional de Referência para a Cibersegurança

Em Portugal, o Centro Nacional de Cibersegurança (CNCS)[1] publicou a 26 de julho de 2019 o Quadro Nacional de Referência para a Cibersegurança (QNRCS) [53], o qual permite às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases e orientações para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação, nas suas diversas componentes.

A estrutura central do QNRCS foi definida numa perspetiva de ciclo de vida da gestão da cibersegurança de uma organização, tendo em consideração o aspeto humano, os processos e a tecnologia, com foco nos processos e procedimentos da gestão do risco.

O QNRCS está estruturado num conjunto de medidas de segurança que traduzem cinco objetivos específicos: Identificar, Proteger, Detetar, Responder e Recuperar (Figura 20).

[1] O CNCS funciona no âmbito do Gabinete Nacional de Segurança (GNS) com as atribuições que lhe foram conferidas pela Lei Orgânica do Gabinete Nacional de Segurança e pela Lei nº46/2018, de 13 de agosto, que definiu o Regime Jurídico de Segurança do Ciberespaço, e do decreto-lei Nº65/2021, de 30 de julho. Tem como missão contribuir para que Portugal use o ciberespaço no respeito pelos princípios e objetivos da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, exercendo, para esse efeito, poderes de autoridade nacional em matéria de cibersegurança.

Figura 20 - Objetivos de Segurança

Fonte: CNCS, QNRCS [43]

Estes objetivos estão organizados por categorias e subcategorias temáticas onde se explanam medidas técnicas e processuais, bem como evidências de implementação que permitam às organizações melhorar a sua capacidade de proteção e de resposta aos desafios do ciberespaço e da segurança da informação.

2.3.2. Roteiro para as Capacidades Mínimas de Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) definiu um modelo de capacitação em cibersegurança, visando a melhoria de processos, pessoas e tecnologias nas organizações nacionais. O Roteiro apresenta um conjunto de ações, divididas em cinco fases (Figura 21) pensadas para uma adaptação gradual, a implementar em cada organização, seja por meios próprios internos, ou recorrendo a subcontratação ou externalização de soluções [54].

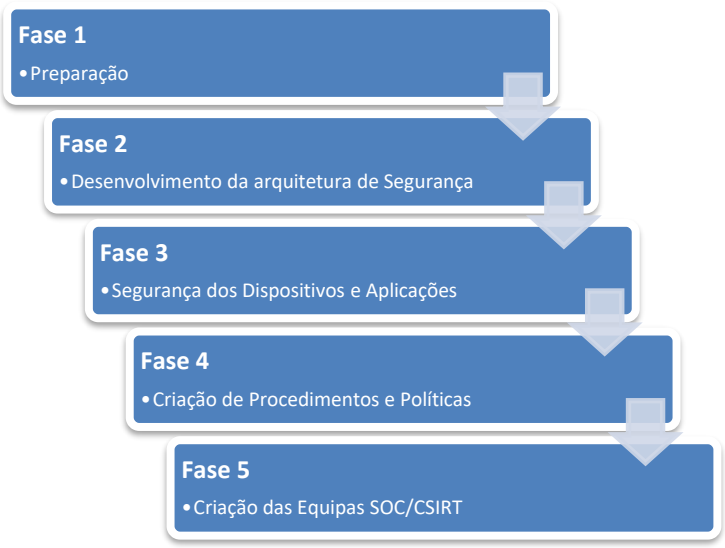


Figura 21 - Fases do Roteiro para as Capacidades Mínimas de Cibersegurança

Fase 1

A fase preparatória consiste no conjunto de ações que permite estabelecer a cooperação entre a organização e o CNCS. Nesta fase são definidos também os canais de comunicação entre a organização e o CNCS.

Fase 2

A segunda fase consiste no desenvolvimento da arquitetura de segurança, focando-se em delimitar as várias áreas de segurança, e aplicar regras de controlo de acessos que permitam dotar a organização com os principais recursos técnicos e processuais de base para uma defesa eficaz dos seus ativos, quer a nível de servidores, postos de trabalho e outros dispositivos. Nesta fase são ainda definidos processos internos que garantam a conformidade da organização com requisitos legais e normativos da área de atividade.

Fase 3

A terceira fase prevê a instalação de *firewall*, sistemas de deteção de intrusão em dispositivos e aplicações, nomeadamente *Host-based Intrusion Detection Systems* (HIDS), *honeypots* e controlo de acessos web (*proxy*), de acordo com a arquitetura de rede e defesas perimétricas definidas na fase anterior. Esta fase também contempla auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização num sistema integrado de gestão de eventos, em inglês *Security Information and Event Management* (SIEM).

Fase 4

A quarta fase procura consolidar e formalizar alguns processos e normativos internos definidos nas fases anteriores, bem como capacitar os recursos humanos no domínio da cibersegurança.

Fase 5

Por último, a quinta fase, aplica-se às organizações cuja dimensão, criticidade ou complexidade o justifique, e consiste na formalização de equipas dedicadas à deteção e resposta de incidentes, com as seguintes capacidades: monitorização e alerta de incidentes de cibersegurança através do *Security Operations Centre* (SOC), e/ou *Computer Security Incident Response Team* (CSIRT). Por esta razão, a execução desta fase pode ser objeto de avaliação conjunta entre a organização e o CNCS.

O cumprimento destas ações, ao longo das cinco fases, vai permitir a criação de capacidades mínimas, no domínio da cibersegurança.

2.4.*Frameworks* de cibersegurança mais populares

Nesta secção iremos abordar algumas das *frameworks* em Segurança da Informação mais populares, de modo a apresentá-las aos AE/ENA no guia de cibersegurança.

As *frameworks* de cibersegurança mais populares são as seguintes:

- Normas da *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC), designadamente as que fazem parte da família 27000 [55];
- *Cyber Security Framework* (CSF 2.0) [56] do *National Institute of Standards and Technology* (NIST);
- *Control Objectives for Information and Related Technologies* (COBIT) [57];
- *Center for Internet Security* (CIS) *Controls* [58].

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. Na avaliação da cibersegurança e adoção de boas práticas, é possível e, em certa medida desejável, aplicar mais do que uma *framework* na mesma organização [59].

2.4.1. ISO/IEC da família 27000

A família de normas ISO 27000 corresponde a um conjunto de diretrizes desenvolvidas pela ISO/IEC, com o objetivo de disponibilizar às organizações padrões robustos e abrangentes, para que estas possam gerir e melhorar os seus sistemas de informação.

A norma ISO/IEC 27001 [55] especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados de acordo com as necessidades individuais da organização. A sua implementação demonstra a preocupação da organização em preservar a confidencialidade, integridade e disponibilidade da informação, que é um bem crítico para a operação e para a sobrevivência de uma organização. A implementação da norma ISO/IEC 27001 permite às organizações uma eficaz gestão e proteção de toda a informação considerada crítica, através da correta seleção e implementação dos controlos de segurança, originando assim um elevado grau de

confiança de todas as partes interessadas, principalmente dos clientes. A norma adota o modelo de sistema de gestão da ISO, permitindo assim a sua fácil integração com outros sistemas.

Os principais benefícios da implementação e posterior certificação de acordo com este referencial são:

- Identificação proativa das ameaças e vulnerabilidades a que uma organização está sujeita;
- Elevada confidencialidade e integridade da informação;
- Definição de um plano de recuperação de desastres, considerando os procedimentos existentes para reativação dos serviços e infraestruturas críticas;
- Garantia da continuidade de negócio;
- Garantia de proteção dos sistemas em todo o ciclo de desenvolvimento;
- Criação de uma cultura de segurança da informação, através da divulgação de políticas e de linhas de orientação;
- Monitorização contínua das infraestruturas que suportam os sistemas.

A ISO/IEC 27001 promove uma abordagem holística à segurança da informação nos seguintes pilares: pessoas, políticas e tecnologia.

2.4.2. NIST Cybersecurity Framework

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 [60].

A primeira versão (1.0) desta *framework*, *CyberSecurity Framework* (CSF), foi publicada em 2014 [61], posteriormente foi disponibilizada em 2018 a versão 1.1 [62], e mais recentemente (2024) foi publicada a versão 2.0 [56]. A última versão foi projetada para todos os públicos, setores industriais e tipos de organização, desde as de menor escala e organizações sem fins lucrativos, até as maiores agências e corporações, independentemente do seu grau de maturidade em cibersegurança.

A *framework* CSF 1.1 da NIST apresenta cinco funções (identificar, proteger, detetar, responder e recuperar) com uma subdivisão em 23 categorias. Para cada categoria existem outras subcategorias com um total de 108 controlos. A versão mais recente da *framework* da

NIST (CSF 2.0) apresenta seis funções (governar, identificar, proteger, detetar, responder e recuperar) com uma subdivisão em 22 categorias. A mudança mais notável foi a introdução da função governar, porque é um elemento vital que estava anteriormente em falta na *framework* da NIST, e que permite estabelecer estratégias e políticas de gestão de riscos cibernéticos das organizações de forma estruturada.

Além disso, o CSF 2.0 oferece um catálogo pesquisável de referências informativas [63] que permite verificar como as ações são mapeadas com esta *framework*. Este catálogo permite ainda que as organizações cruzem as orientações da CSF com mais de 50 outros documentos de segurança cibernética, como a ISO/IEC 27001:2022, NIST SP800-53 Rev 5, entre muitas outras referências, para alcançar resultados específicos de cibersegurança, por via da aplicação de controlos.

A NIST com o lançamento do CSF 2.0 disponibilizou vários guias de início rápido, projetados para utilizadores específicos [64], tais como pequenas empresas, gestores de risco empresarial, e organizações que procuram proteger todo o seu ecossistema.

2.4.3. CIS *Controls Framework*

O *CIS Controls* é uma *framework* que disponibiliza um conjunto de boas práticas orientadas à segurança cibernética para auxiliar as organizações a proteger os seus ativos críticos contra ameaças. A *framework* foi desenvolvida pelo *Center for Internet Security* (CIS), uma organização sem fins lucrativos dos EUA, que se dedica a ajudar pessoas, empresas e governos a protegerem-se de ameaças cibernéticas [58].

A *framework CIS Controls* disponibiliza 20 controlos, organizados em três categorias (Básico, Fundamental e Organizacional), nomeadamente:

- **Básico**
    1. Controlo e inventário de ativos de *hardware.*
    2. Controlo e inventário de ativos de *software.*
    3. Gestão contínua de vulnerabilidades.
    4. Uso controlado de privilégios administrativos.
    5. Configuração segura para *hardware* e *software* em dispositivos móveis, portáteis, postos de trabalho e servidores.
    6. Manutenção, monitorização e análise de *logs* de auditoria.

- **Fundamental**
    7. Proteção do e-mail e navegador da Web.
    8. Defesas contra *malware.*
    9. Limitação e controlo de portas, protocolos e serviços de rede.
    10. Recursos de recuperação de dados.
    11. Configuração segura para dispositivos de rede, como *firewalls*, *routers* e *switches.*
    12. Defesa do perímetro.
    13. Proteção de dados.
- **Organizacional**
    14. Acesso controlado com base na necessidade de saber.
    15. Controlo de acesso sem fios.
    16. Monitorização e controlo de contas.
    17. Avaliação das competências de segurança e formação adequada.
    18. Segurança na utilização do software.
    19. Resposta e gestão de incidentes.
    20. Testes e exercícios de penetração (*Pentesting*).

A lista de controlos do *CIS Controls* é atualizada frequentemente para acompanhar os avanços tecnológicos. As organizações são incentivadas a implementar estes controlos com base nas suas necessidades específicas e perfis de risco. A *framework* pode servir como um roteiro para as organizações que procuram melhorar a sua postura de segurança cibernética.

2.4.4. *Control Objectives for Information and Related Technologies* (COBIT)

Control Objetives for Information and Related Technology (COBIT) é uma *framework* desenvolvida pela *Information Systems Audit and Control Association* (ISACA) para a gestão e governança de TI em contexto empresarial. Esta *framework* fornece um conjunto de diretrizes e práticas recomendadas para alinhar os objetivos de Tecnologias de Informação (TI) com os objetivos do negócio [57]. A *framework* dispõe de uma estrutura categorizada em quatro domínios, nomeadamente:

1) **Planeamento e organização**: Este domínio centra-se no planeamento estratégico, na definição da arquitetura da informação, e na garantia de que os recursos de TI são efetivamente organizados e geridos;

2) **Adquisição e implementação**: Este domínio abrange os processos necessários para adquirir, desenvolver e implementar soluções e serviços de TI, incluindo a gestão de projetos, definição de requisitos e identificação de soluções;
3) **Entrega e suporte**: Este domínio concentra-se na gestão de processos de TI para fornecer e dar suporte a serviços de TI. Inclui áreas como prestação de serviços, gestão de problemas, gestão de incidentes e melhoria contínua;
4) **Monitoração e avaliação**: Este domínio envolve a monitorização do desempenho das TI, garantindo a conformidade com a legislação e regulamentação aplicável, e permite avaliar a eficácia dos controlos de TI.

2.5. Trabalhos relacionados

Nesta secção, pretende-se facultar uma visão global de outros trabalhos relevantes identificados durante a fase de pesquisa prévia englobada nos objetivos do projeto.

The Importance of Cybersecurity Education in School

Os autores *Rahman at al.*, em [59], apresentam um estudo sobre a necessidade de preparar as crianças para o uso consciente das novas tecnologias, por via de ações de formação nas próprias instituições de ensino.

Para a realização deste estudo, os autores analisaram mais de 240 artigos científicos publicados, dos quais selecionaram 25 estudos para obter resposta para as seguintes questões:

1) *Qual a importância da educação em cibersegurança nas Escolas?*
2) *Quais são as estratégias que as partes interessadas podem utilizar para promover a educação em cibersegurança nas Escolas?*

Como conclusão deste estudo, os autores sugerem que as crianças, desde cedo, tenham conhecimento dos potencias riscos na utilização da internet, redes sociais, *chats* e jogos online. Os funcionários da instituição de ensino não devem ser excluídos destas ações de formação, pelo que devem ter também conhecimento dos potenciais riscos a que estão expostos. Os autores referem que é necessário envolver toda a comunidade escolar, bem como o governo, para em conjunto encontrarem uma solução para proteger as crianças do cibercrime e do *ciberbulling* através da educação em cibersegurança nas escolas.

K12 Security Information Exchange (K12 SIX)

K12 Security Information Exchange (K12 SIX) é uma organização sem fins lucrativos dos EUA que se dedica exclusivamente a ajudar as escolas públicas e privadas, de ensino não superior, contra ameaças emergentes à segurança cibernética, como *ransomware* e ataques de *phishing*. A organização teve início no final do ano 2020 em resposta aos crescentes desafios de segurança cibernéticos enfrentados pelas escolas em todo o país [65]. Todos os anos é publicado um relatório anual designado por «*State of K-12 Cybersecurity: Year in Review*», onde é apresentado o estado da segurança cibernética no ensino, referente ao ano transato. De acordo com o último relatório divulgado (*2022 Annual Report*) [66], que se refere ao ano civil 2021, o r*ansomware* foi, pela primeira vez, o tipo de incidente mais frequente, afetando um total de 62 distritos escolares públicos, em 24 estados distintos. Pelo terceiro ano consecutivo o *ransomware* foi o tipo de ataque que contabilizou mais de que 50 incidentes/ano. Os autores concluem que dada a crescente dependência da tecnologia, os incidentes continuarão a aumentar significativamente caso não sejam tomadas algumas medidas a curto e médio-prazo, tais como:

- Criar e melhorar o conteúdo informativo sobre os incidentes cibernéticos;
- Implementar controlos de segurança cibernética nas instituições de ensino;
- Garantir que os fornecedores das instituições de ensino, aplicam as boas práticas no desenvolvimento das suas soluções digitais;
- Criar conteúdo informativo, específico e direcionado às instituições de ensino, com orientações e melhores práticas sobre ameaças à segurança cibernética;
- Criar grupos de trabalho para as instituições de ensino coletivamente resolverem os problemas, e para se prepararem melhor para os desafios da segurança cibernética.

A adesão a esta comunidade (K12 SIX) está aberta a todas as instituições de ensino dos EUA com o objetivo de proporcionar um ecossistema de segurança cibernética mais forte e resiliente. Para garantir a integridade e confidencialidade da comunidade, todos os membros passam por um processo de aprovação. A comunidade apoia a adoção de práticas recomendadas por especialistas, como a *Cybersecurity and Infrastructure Security Agency* (CISA), a *NIST Cybersecurity Framework* e o *CIS Controls*, entre outras.

Estratégia integrada de avaliação e consciencialização cibernética em contexto escolar

O autor Frederico Marques em [67], apresenta uma estratégia de consciencialização cibernética que foi implementada e avaliada em contexto escolar. O autor definiu três objetivos para o projeto e conseguiu concretizá-los. O primeiro objetivo era avaliar os comportamentos e atitudes dos alunos face à cibersegurança, para o efeito criou e disponibilizou um questionário a três turmas (finalistas) do 2º e 3º ciclo de escolaridade de uma instituição de ensino. O segundo objetivo era disponibilizar um segundo questionário para os utilizadores realizarem uma autoavaliação dos seus conhecimentos de cibersegurança. No final do questionário os utilizadores obtinham uma pontuação e um conjunto de recomendações. Para a elaboração dos dois questionários o autor recorreu à escala de *Likert* para avaliar as respostas. Por último, o terceiro objetivo do projeto era desenvolver um plano de aula, para abordar a curto-prazo, os temas da cibersegurança e ciberconsciência nas aulas de TIC e Educação para a Cidadania. Da análise realizada aos dados recolhidos através dos questionários, o autor conclui que existe um longo caminho a percorrer, sendo necessário sensibilizar a comunidade educativa sobre a necessidade de implementar estratégias de cibersegurança quer nas instituições de ensino, quer junto das famílias. Como trabalho futuro, o autor propõe que seja intensificada a promoção e divulgação de questionários de avaliação de atitudes e comportamentos noutros estabelecimentos de ensino para promover a segurança cibernética e os hábitos de ciberhigiene. O autor propõe também que os currículos das disciplinas de TIC e Cidadania passem a incluir um conjunto de aulas exclusivas sobre o tema cibersegurança. Sugere também um planeamento de sessões autónomas de sensibilização destinadas aos docentes e não docentes com o intuito de melhorarem as suas habilidades de ciberconsciencialização, reduzindo os riscos de segurança cibernética.

Ciberexercícios na Comunidade Académica

Bruno Pereira em [68], apresenta como projeto a preparação de um guião para planear, executar e avaliar um ciberexercício no âmbito e contexto de uma instituição de ensino superior. O objetivo inicial da dissertação era cumprir com os objetivos propostos e normas planeadas pelo projeto *CyberLab* [69]. O projeto *CyberLab*, tem como objetivo principal, a criação de um laboratório de inovação e experimentação de soluções de cibersegurança adaptadas aos diferentes contextos da Administração Pública. Contudo, com a ausência de

recursos tecnológicos, o autor teve de reformular os objetivos da dissertação, que passou a ser a preparação do guião. O autor baseou-se nas normas e referências de segurança, nomeadamente, compilou os requisitos, características, e fundamentos das normas NIST NICE *Cybersecurity Workforce Framework*, NIST *Framework*, a Diretiva NIS, o MITRE ATT\&CK e a família de normas ISO 27000, dando especial atenção à ISO 27001. Concluída a fase de análise, o autor preparou dois exercícios: um sobre *Tabletop Ransomware (Lockbit)*, e outro sobre *Red Team Vs Blue Team*, nos quais descreve o objetivo do exercício, bem como apresenta uma proposta do planeamento e a avaliação a realizar. O autor recorreu a duas metodologias, o modelo CANVAS e análise SWOT, para realizar o seu projeto. O autor comprovou da necessidade de investir em cibersegurança na área de ensino superior em Portugal e, que os serviços administrativos das instituições de ensino necessitam de mais e melhor sensibilização para a temática, e mais treino para conseguirem lidar com os vários tipos de incidentes. Constatou também que o processo de criar exercícios de cibersegurança, para além do conhecimento técnico, necessita do envolvimento de outras áreas como: logística, comunicação e relações interinstitucionais. Como trabalho futuro, o autor propõe que o guião criado sirva de base para iniciar o desenvolvimento dos ciberexercícios adaptados ao contexto das instituições de ensino superiores.

Programa "ProtegeOTeuCampus" da Metared Portugal

A MetaRed Portugal [8] é uma associação de instituições de ensino superior públicas e privadas portuguesas, aberta igualmente a outras entidades da administração pública que desenvolvam atividade relevante no domínio das Tecnologias da Informação e Comunicação (TIC), e em particular na sua aplicação no âmbito do ensino superior. Pretende ser um ponto de encontro para debate, reflexão e trabalho colaborativo sobre o uso das TIC no ensino superior, com total respeito ao princípio da autonomia das instituições, respeitando a sua liberdade individual para tomar as suas próprias decisões, propondo recomendações e promovendo a partilha de experiências e boas práticas.

A MetaRed nasceu sob proposta de algumas universidades e com o apoio da *Universia*, com base em experiências semelhantes de outros países como Espanha (Crue-Tic[2]), México (AnuiesTic[3]) entre outros. Assenta na preocupação e consciencialização das instituições de ensino superior sobre o papel que as tecnologias desempenham nas suas instituições,

[2] https://tic.crue.org/
[3] https://anuies-tic.anuies.mx/web/

propondo-se a MetaRed a promover uma colaboração mais estreita e mais efetiva entre os seus membros, e a comunidade em geral.

Como missão, a MetaRed Portugal pretende:

- Assessorar e propor aos Reitores das Universidades e Presidentes dos Politécnicos portugueses, temas que se considerem oportunos no âmbito das TIC para melhorar a qualidade, a eficácia e a eficiência das instituições de ensino superior;
- Estudar as necessidades e aplicações destas tecnologias na gestão, na docência e na investigação, propondo ações e atuações conjuntas;
- Fomentar, promover e liderar a cooperação a nível nacional e também internacional;
- Fomentar a participação conjunta em projetos de investigação aplicada, estudos e iniciativas de *benchmarking*, promovendo a colaboração, partilha e adoção de boas práticas;
- Promover a realização e participação em ações de formação, conferências e seminários, bem como a articulação com fornecedores e fabricantes de soluções no âmbito das TIC.

A campanha "ProtegeOTeuCampus" [70] arrancou em outubro de 2021, no sentido de sensibilizar e informar as comunidades académicas do ensino superior para os riscos e as boas práticas na área da cibersegurança. O responsável pela cibersegurança, o diretor de Tecnologias de Informação (TI) ou equivalente da instituição de ensino superior, tem a possibilidade de solicitar o acesso ao Kit de Sensibilização no portal da MetaredTIC Portugal[4]. Este Kit é constituído por recursos gráficos, elementos interativos e informativos bem como outros recursos tecnológicos. O objetivo da Metared Portugal é que qualquer instituição de ensino superior o possa utilizar e implementar de acordo com as necessidades específicas, e à velocidade que entender. Atualmente, já conta com mais de 40 instituições de ensino superior aderentes, entre universidades e politécnicos. O Kit tem o apoio de várias entidades como o Centro Nacional de Cibersegurança (CNCS), a Fundação para a Ciência e a Tecnologia (FCT), a Agência para a Modernização Administrativa (AMA), o Portugal Digital, a IDC *digital transformation* e a Direção-Geral do Ensino Superior (DGES) [71].

[4] https://www.metared.org/pt/kit-sensibilizacao.html

Inquérito – A utilização das TIC na Administração Pública Central

O Inquérito à Utilização das Tecnologias da Informação e da Comunicação (IUTIC) é um inquérito do Sistema Estatístico Nacional (SEN), definido pela Lei n.º 22/2008 [72], de 13 de maio, de resposta obrigatória, que recolhe informação sobre a disponibilidade e utilização de tecnologias da informação e da comunicação. Este, é dirigido a todos os organismos da Administração Pública Central, aos organismos da Administração Pública Regional (nas Regiões Autónomas), bem como a todas as Câmaras Municipais [73].

A Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) [74] divulgou em junho de 2023 o sumário estatístico do inquérito à utilização das Tecnologias da Informação e Comunicação (TIC) na Administração Pública Central e Regional, referente ao ano de 2022. O Inquérito à Utilização da TIC na Administração Pública Central (IUTICAP) encontra-se inscrito no Sistema Estatístico Nacional (Lei n.º 22/2008, de 13 de maio) de resposta obrigatória, registado no Instituto Nacional de Estatística (INE), e trata-se de um instrumento para a recolha e divulgação das estatísticas oficiais em matéria de Sociedade da Informação na Administração Pública em Portugal, com uma periodicidade anual.

A população alvo do inquérito IUTICAP são os Organismos da Administração Central (exceto fundos de segurança social), constituídos em pessoas coletivas, com exceção das empresas públicas sob controlo de uma unidade da administração central ou regional, universidades, estabelecimentos de ensino, estabelecimentos hospitalares e estruturas temporárias.

O universo inquirido no período de setembro de 2022 a fevereiro de 2023, através de um método de inquérito online, foi de 273 organismos, com uma taxa de resposta de 100%.

Os indicadores de Segurança das TIC (cibersegurança) incluem componentes, tecnologias, serviços, recomendações e procedimentos aplicados em sistemas TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados, e dos sistemas de informação, neste caso particular referente aos Organismos da Administração Pública, nomeadamente:

- Tecnologias e aplicações de segurança das TIC utilizadas nos Organismos (ex.: segurança de redes e correio eletrónico, software antivírus, *firewall*);
- Medidas de segurança das TIC implementadas nos Organismos;
- Formação e consciencialização em matéria de segurança das TIC;

- Recursos afetos à realização de atividades de segurança das TIC;
- Incidentes de segurança das TIC.

Os indicadores divulgados são produzidos através dos dados recolhidos nos seguintes módulos:

- Infraestrutura tecnológica;
- Utilização das TIC;
- Comércio eletrónico;
- *Big data;*
- Computação em nuvem (*cloud computing*);
- Transformação digital;
- Cibersegurança;
- Inteligência Artificial (IA);
- Internet das Coisas (IoT);
- TIC e o ambiente;
- Recursos humanos e despesa em TIC.

Em 2022 o universo de inquiridos foi composto pela Administração Pública Central, com 273 respostas, a Região Autónoma dos Açores com 56 respostas, a Região Autónoma da Madeira com 58 respostas, e os Municípios com um total de 308, tendo-se obtido uma taxa de resposta de 100% em ambas as operações estatísticas.

Em jeito de conclusão desta secção é importante reter que o setor da educação dispõe de Sistemas de Informação (SI) que armazenam muita informação confidencial e diariamente são milhares de utilizadores, que fazem parte do ecossistema da educação, a operar com esta informação, sob uma infraestrutura tecnológica que poderá conter algumas fragilidades que devem ser mitigadas para minimizar os riscos de ataques informáticos. Para o efeito existem várias *frameworks* de segurança que podem servir de base para auxiliar os responsáveis pelas Tecnologias de Informação e Comunicação (TIC) nas instituições de ensino.

3. Estudo Empírico

Nesta secção pretende-se abordar o estado atual da cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da região de Leiria, e compreender se a legislação em vigor está a ser devidamente aplicada, identificando se estão a adotar as boas práticas de cibersegurança.

Atendendo às características do estudo empírico que se pretende desenvolver, optou-se por uma análise quantitativa, recorrendo a um questionário direcionado aos responsáveis pelas Tecnologias Informação e Comunicação (TIC) destas instituições.

3.1. Metodologia de Investigação

Para analisar os factos do ponto de vista empírico, e para confrontar a visão teórica com a realidade operacional das AE e ENA, é essencial traçar um modelo conceptual e operacional da pesquisa.

O estudo realizado envolveu as seguintes etapas:

1. Revisão de literatura, de modo a sustentar e enriquecer o estudo empírico;
2. Análise de outros inquéritos sobre o tema em estudo, para correlacionar as questões e selecionar as que se enquadram para o caso de estudo;
3. Construção e disponibilização do questionário;
4. Análise dos dados obtidos no questionário.

A investigação científica, conforme a metodologia adotada, é do tipo quantitativo e permite obter dados objetivos e quantificáveis.

3.2. Método e técnicas de recolha de dados

Como referido no ponto anterior, neste estudo serão analisados dados obtidos através de um questionário, que se descreve de seguida, nesta secção.

3.2.1. Inquéritos em análise

O questionário elaborado no âmbito do presente projeto teve como referência dois outros inquéritos, nomeadamente:

- Inquérito à utilização das Tecnologias da Informação e Comunicação na Administração Pública Central (IUTICAP-2023) [75], promovido pela DGEEC;
- Inquérito de autoavaliação de cibersegurança, promovido pela Metared Portugal [76].

Resultado da análise detalhada a cada uma das questões, estas foram classificadas da seguinte forma: **Com interesse para o estudo** ou **Sem interesse para o estudo**, conforme Tabela 2.

Com interesse para o estudo	✓
Sem interesse para o estudo	✗

Tabela 2 - Classificação das Questões

A principal razão para se excluir parte das questões dos inquéritos analisados, foi criar um questionário sucinto, que permitisse aferir se o público-alvo está em cumprimento com a legislação em vigor, e identificar se estão a aplicar algumas das boas práticas no âmbito da cibersegurança. Para o efeito, definiu-se o limite aproximado de 30 questões de resposta fechada (escolha única ou múltipla) para agilizar e facilitar o processo da análise estatística.

Inquérito IUTIC-2023

Relativamente ao Inquérito à Utilização das Tecnologias da Informação e da Comunicação (IUTICAP) de 2023, embora tenha sido preparado pela DGEEC com vários módulos, conforme descrito na secção 2.5, do presente relatório, optou-se por selecionar apenas o módulo de cibersegurança para o estudo de caso. A versão completa do inquérito IUTICAP poderá ser consultada no **Anexo A**.

Através da análise comparativa entre os inquéritos IUTICAP de 2023 e IUTICAP de anos anteriores, identificaram-se algumas diferenças que permitem aferir que os inquéritos de um ano para o outro sofrem algumas alterações, acompanhando assim as recomendações e boas práticas no âmbito da cibersegurança. Como exemplo destas diferenças verifica-se que o número mínimo de caracteres numa palavra-passe segura no inquérito IUTICAP de 2021 era de 10 caracteres e no último inquérito IUTICAP de 2023 passou a ser 12 caracteres.

Na Tabela 3, são apresentadas todas as questões do módulo de segurança das TIC do inquérito IUTICAP do ano 2023, bem como a classificação, com a importância da questão para o estudo de caso.

Id.	Questão	Opções de resposta	Classificação
Segurança das TIC - medidas, controlos e procedimentos aplicados em sistemas das TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados e dos sistemas.			
1	**O Organismo utiliza alguma das seguintes medidas de segurança das TIC?**		
a)	Autenticação dos utilizadores através de uma palavra-passe segura (mínimo de doze caracteres com letras maiúsculas e minúsculas, algarismos, caracteres especiais, uma palavra-passe por cada plataforma)	sim / não	✓
b)	Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação (i.e. combinação de palavra-passe definida pelo utilizador, palavra-passe de uso único (OTP), código gerado por *token* de segurança ou recebido via smartphone, métodos biométricos (impressões digitais, reconhecimento de voz, reconhecimento facial))	sim / não	✓
c)	Autenticação do utilizador através de métodos biométricos (impressões digitais, voz, rostos)	sim / não	✗
d)	Atualização regular do software (incluído sistemas operativos)	sim / não	✓
e)	Técnicas de proteção por método criptográfico de dados, documentos ou/ e-mail	sim / não	✗
f)	Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN)	sim / não	✓
g)	Conservação de registos (histórico) para análise depois da ocorrência de incidentes de segurança	sim / não	✓
h)	Análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação	sim / não	✓
i)	Testes da segurança às TIC (de intrusão, aos sistemas de alerta e de *backup*, revisões às medidas de segurança)	sim / não	✓
j)	Inventário de todos os ativos essenciais para a prestação dos serviços de segurança das TIC	sim / não	✓
k)	Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada *offline*)	sim / não	✓
l)	Sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar o Organismo sobre as mesmas, excluindo o software antivírus autónomo	sim / não	✓
2	**O Organismo informa o pessoal ao serviço para as suas obrigações em matéria de segurança das TIC, através de:**		
a)	Ações de formação voluntária ou informação interna disponível (Intranet, etc.)	sim / não	✗
b)	Ações de formação obrigatória e/ou consulta obrigatória de informação	sim / não	✗
c)	Disposições contratuais (ex.: políticas de utilização responsável dos equipamentos informáticos que os utilizadores têm de assinar)	sim / não	✗
3	**Quem realiza as atividades relacionadas com a segurança das TIC do Organismo?** (ex.: testes, formação e resolução de incidentes de segurança. Excluem-se as atualizações de software pré-configurado)		
a)	Pessoal da próprio Organismo	sim / não	✓
b)	Fornecedores externos	sim / não	✓
As recomendações sobre segurança TIC não têm que ser obrigatoriamente documentos formais escritos. Podem ser informações/instruções internas e devem incluir temas como: formação para a utilização, medidas de segurança e a sua avaliação, planos para atualização de documentos de segurança, etc.			
4	**O Organismo possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC?**	sim / não	✓
5	**Nessas recomendações são considerados alguns dos seguintes temas?**		
a)	Gestão dos níveis de acesso às TIC (ex.: computadores, redes)	sim / não	✓
b)	Armazenamento, proteção, acesso e processamento de dados	sim / não	✓
c)	Procedimentos e regras para prevenir e/ou reagir a incidentes de segurança (ex.: ataques de *phishing*, *ransomware*, DoS, etc.)	sim / não	✓
d)	Responsabilidade, direitos e deveres no que respeita à utilização das TIC (ex.: uso de e-mails, dispositivos móveis, social media, etc.)	sim / não	✓

e)	Boas práticas para o pessoal ao serviço na utilização segura das TIC	sim / não	✓
6	**Quando foram definidas ou revistas as recomendações sobre medidas, práticas ou procedimentos de segurança TIC?** (ex.: avaliação de riscos, evolução de incidentes, etc.)		
a)	Nos últimos 12 meses	Selecionar apenas uma das opções	✓
b)	Há mais de 12 meses e até 24 meses		
c)	Há mais de 24 meses		
7	**O Organismo detetou problemas de segurança informática?**	sim / não	✓
7.1	**O Organismo sofreu algum incidente de segurança relacionado com as TIC, que tenha tido alguma das seguintes consequências?**		
a)	Indisponibilidade de serviços TIC devido a falhas de hardware ou software	sim / não	✓
b)	Indisponibilidade de serviços TIC devido a ataques do exterior (ex.: ataques de negação de serviço e *ransomware*)	sim / não	✓
c)	Destruição ou corrupção de dados devido a falhas de hardware ou software	sim / não	✓
d)	Destruição ou corrupção de dados devido a infeção de software malicioso ou intrusão não autorizada	sim / não	✓
e)	Divulgação de dados confidenciais devido a ataques de intrusão, *pharming* ou *phishing*, ações intencionais dos próprios funcionários	sim / não	✓
f)	Divulgação de dados confidenciais devido a ações não intencionais dos próprios funcionários	sim / não	✓
g)	Outro(s). Especifique:	sim / não	✗
8	**O Organismo tem seguro contra incidentes de segurança das TIC?**	sim / não	✗
9	**O Organismo tem definida uma estratégia/política para a segurança das redes e da informação?**	sim / não	✓
9.1	**A estratégia/política para a segurança das redes e da informação:**		
a)	Já se encontra implementada no Organismo	sim / não	✓
b)	Encontra-se em fase de implementação no Organismo	sim / não	✓
c)	Prevê avaliar regularmente os resultados das metodologias de segurança de informação colocadas em prática	sim / não	✓
Regulamento Geral de Proteção de Dados (RGPD)			
d)	Já se encontra de acordo com o RGPD	sim / não	✓
e)	Encontra-se em fase de revisão de modo a incorporar o RGPD	sim / não	✓
f)	Prevê avaliar regularmente os resultados das metodologias de segurança de informação colocadas em prática face ao RGPD	sim / não	✓
Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021			
g)	Já se encontra de acordo com o RJSC	sim / não	✓
h)	Encontra-se em fase de revisão de modo a incorporar o RJSC	sim / não	✓
i)	Prevê avaliar regularmente os resultados das metodologias de segurança das redes e da informação colocadas em prática face ao RJSC	sim / não	✓
9.2	**De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), o Organismo:**		
a)	Tem um ponto de contacto permanente com o Centro Nacional de Cibersegurança (CNCS)	sim / não	✓
b)	Designou um responsável de segurança (responsável pela gestão das medidas de segurança como, por exemplo, um CISO - Chief Information Security Officer) junto do CNCS	sim / não	✓
c)	Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços	sim / não	✓
d)	Elaborou e mantém atualizado o plano de segurança, devidamente documentado e assinado pelo responsável de segurança	sim / não	✓
e)	Elaborou o relatório anual de segurança no ano transacto	sim / não	✓
f)	Efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)	sim / não	✓

Tabela 3 - Módulo VII – Segurança das TIC do Inquérito

Fonte: DGEEC, IUTICAP-2023 [75]

Da análise realizada ao primeiro inquérito (IUTICAP-2023), resultou numa seleção de 42 questões com interesse no universo de 49. Foram excluídas 7 questões por serem consideradas como complementares a outras que nesta fase será mais relevante identificar. O principal objetivo foi tentar não construir um inquérito demasiado extenso que poderia inviabilizar a obtenção de uma amostra de respostas significativa.

Inquérito de Autoavaliação da MetaRed Portugal

Relativamente ao inquérito de autoavaliação da MetaRed Portugal, existem duas sessões no inquérito, nomeadamente **Contextualização** e **Autoavaliação**. Para o presente estudo optou-se por selecionar apenas algumas das questões da secção **Contextualização**, e excluiu-se a secção da **Autoavaliação** porque o objetivo não é avaliar apenas um utilizador da instituição de ensino, mas sim o seu contexto global.

Na Tabela 4, são listadas todas as questões da ferramenta de autoavaliação da MetaRed Portugal, bem como a classificação da importância da questão para o estudo de caso.

Id.	Questão	Opções de resposta	Classificação
Contextualização			
1	**Quais dos seguintes dispositivos usa para realizar transações online?**		✕
a)	Computador ou portátil	escolha múltipla	
b)	Dispositivos móveis (*smartphone*, *tablet*, *smartwatch*)		
c)	Não faço pagamentos ou transações online		
Até que ponto concorda com as afirmações:			
2	**Todos os utilizadores têm um papel importante na cibersegurança**	1 – pouco, 2, 3, 4, 5 – muito	✕
3	**A cibersegurança é essencialmente uma preocupação da minha Instituição**	1 – pouco, 2, 3, 4, 5 – muito	✓
4	**Nos últimos 12 meses fui vítima de um dos seguintes tipos de ciberincidentes:**		✕
a)	Publicidade excessiva sempre que visito uma página web	escolha múltipla	
b)	Os meus dados pessoais foram roubados		
c)	Recebi um e-mail com um *link* e coloquei o meu *login* e a minha *password* foi roubada		
d)	Nenhuma das anteriores		
Estou preocupado:			
5	**O meu computador é controlado por *hackers* ilegalmente**	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✕
6	**A minha informação financeira foi obtida por terceiros sem o meu consentimento**	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✕

7	**A minha informação pessoal foi obtida por terceiros sem o meu consentimento**	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✗
8	**Ser vítima de ransomware**	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✓
9	**Ser vítima de *fraud online***	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✓
10	**Ter o computador infetado por vírus ou outro *malware***	1 – nada preocupado, 2, 3, 4, 5 – extremamente preocupado	✗
11	**A engenharia social, é uma das técnicas usadas por criminosos em contextos informáticos para obtenção de informação pessoal e privada, quais as técnicas que já fui alvo?**		✓
a)	*Phishing*	escolha múltipla	
b)	*Smishing*		
c)	*Sextortion*		
d)	*Vishing*		
e)	Não sei se já fui ou não vítima uma vez que não conheço nenhum dos termos acima mencionados		
f)	Nunca fui vítima		
12	**O meu uso de VPN (*Virtual Private Network*):**		✓
a)	Não uso VPN porque a minha informação não necessita desta proteção	escolha múltipla	
b)	Não sei o que é a tecnologia VPN		
c)	Uso sempre VPN quando estou fora da minha instituição		
d)	Não necessito de usar VPN		
e)	A minha instituição não disponibiliza VPN		
13	**Fui (ou no caso de vir a ser) vítima de um ciberincidente, como procedi (vou proceder):**		✓
a)	Alterei a minha *password*	escolha múltipla	
b)	Reportei à Instituição responsável pelo sistema		
c)	Instalei um antivírus em todos os meus dispositivos		
d)	Reportei à polícia		
e)	Reportei ao CSIRT interno ou ao CERT.PT		
f)	Não tomei nenhuma ação		
g)	Tomei outras ações		
Autoavaliação			
14	**Os problemas que afetam a segurança da informação podem ter origem:**		✗
a)	Acidentais	escolha 1 opção	
b)	Propositados por membros da comunidade universitária ou *insiders* (internos)		
c)	Originados por cibercriminosos		
d)	Todas as anteriores		
15	**Quando falamos de segurança da informação, normalmente falamos de:**		✗
a)	Informação está acessível quando precisamos (disponibilidade)	escolha 1 opção	
b)	Informação está livre de alterações e falhas que impliquem alterações no seu conteúdo (integridade)		

c)	Informação não se disponibiliza ou divulga aos particulares, entidades ou processos não autorizados (confidencialidade)	
d)	Todas as anteriores	
16	**Um dado pessoal é:**	✕
a)	Uma fotografia	escolha 1 opção
b)	Um documento de identificação como o CC	
c)	Um correio eletrónico que seja associado a uma pessoa física	
d)	Todas as anteriores	
17	**Quando partilho ficheiros com terceiros usualmente:**	✕
a)	Removo os metadados antes de os partilhar	escolha 1 opção
b)	Os metadados são informação essencial ao ficheiro e não podem ser removidos	
c)	Não sei o que são metadados	
d)	Sei o que são metadados mas não os removo porque não contêm informação pessoal	
18	**Cópias de segurança:**	✕
a)	Faço habitualmente cópias de segurança da minha informação	escolha 1 opção
b)	As cópias de segurança são da responsabilidade da minha Instituição	
c)	Não faço habitualmente cópias de segurança, mas reconheço a importância	
d)	Os discos mais recentes não têm falhas e não é necessário fazer cópias de segurança	
19	**Cuidados com as PENs e Discos Externos:**	✕
a)	Uso sempre as PENs e/ou Discos Externos encriptados	escolha 1 opção
b)	Normalmente uso a PEN e/ou Disco Externo que tem os meus dados para partilhar ficheiros com outros computadores	
c)	As PENs e os discos externos são dispositivos que não permitem encriptação	
d)	Se encontro uma PEN tento verificar se os ficheiros têm informação que permita identificar o seu dono	
20	**Utiliza Duplo Fator de Autenticação (2FA) nas suas contas online?**	✕
a)	Não tenho a certeza se está ativo	escolha 1 opção
b)	Não sei o que isso é	
c)	Não está ativo, mas sei o que é	
d)	Está ativo para algumas contas	
e)	Está ativo para todas as contas	
21	**Tem alguma aplicação de segurança instalado no seu dispositivo móvel?**	✕
a)	Não	escolha 1 opção
b)	Não tenho a certeza	
c)	Sim	
22	**No que respeita a aplicações de segurança no meu dispositivo móvel, considero que:**	✕
a)	Percebo perfeitamente o risco de não ter uma aplicação de segurança	escolha 1 opção
b)	Conheço as funções das aplicações de segurança	
c)	Percebo como usar as aplicações de segurança	
d)	Sei quais as aplicações de segurança a instalar	
23	**Escolheria a password seguinte por ser a mais forte:**	✕
a)	qwetr54321	escolha 1 opção
b)	P@ssw0rd	
c)	AsR0sasD3Atacam@	
d)	1!2"3#4$5%6&	
e)	Indiferente, são todas iguais	

24	**As suas passwords para as contas online (e-mail pessoal e conta institucional):**	✕
a)	Têm entre 8 e 11 caracteres	escolha 1 opção
b)	Têm 12 ou mais caracteres	
c)	São combinação de letras minúsculas, maiúsculas, números e símbolos	
d)	Contêm Informação pessoal	
e)	Incluem palavras ou frases	
f)	Nenhuma das anteriores	
25	**Se alguém me pede ou necessita da minha password:**	✕
a)	Verifico se realmente é importante e, caso seja, partilho-a	escolha 1 opção
b)	Nunca partilho a minha password	
c)	Só partilho a password com pessoas em quem confio	
d)	Só partilho a password com os técnicos do serviço de suporte TIC	
26	***Ransomware*:**	✕
a)	Realizo *backups* regulares da minha informação para dispositivos externos (incluindo a *cloud*) e corro menos riscos	escolha 1 opção
b)	Não me preocupa porque tenho um antivírus instalado	
c)	Podia sempre recuperar a informação desde que pague o resgate	
d)	Não poderei ser vítima porque só abro links/ficheiros vindos dos meus colegas	
27	**Como utilizador de Tecnologias de Informação e Comunicação (TIC), qual considera ser a sua responsabilidade de proteger os recursos tecnológicos ao seu cargo?**	✕
a)	Auxiliar na proteção e uso responsável dos recursos tecnológicos	escolha 1 opção
b)	Conhecer os processos para proteger os recursos tecnológicos	
c)	Aplicar práticas de segurança adequadas	
d)	Todas as anteriores	
28	**Quando recebo um correio eletrónico que não esperava a solicitar-me uma ação:**	✕
a)	Tento responder cordialmente ao solicitado	escolha 1 opção
b)	Verifico com os serviços de suporte da minha Instituição se pode ser alguma fraude	
c)	Verifico sempre os *links* para ver se pode ser algum pedido importante	
d)	Nunca recebi um e-mail deste tipo	
29	**De acordo com o RGPD (Regulamento Geral da Proteção de Dados) quando entrego o meu Curriculum Vitae (CV):**	✕
a)	Sei que tratamento vai ser dado ao meu CV e durante quanto tempo será guardado.	escolha 1 opção
b)	Não tenho conhecimento quais as organizações/empresas que irão ter acesso ao meu CV.	
c)	Não sei durante quanto tempo o meu CV será guardado.	
30	**De acordo com o RGPD (Regulamento Geral da Proteção de Dados), quando alguém grava a minha voz (por exemplo: responder a um inquérito (…).**	✕
a)	Tenho de dar o meu consentimento, ser informado de qual a finalidade de tratamento de dados e durante quanto tempo a gravação será guardada.	escolha 1 opção
b)	Não tenho de dar qualquer consentimento.	
c)	Depois da voz gravada não posso retirar o meu consentimento e solicitar a eliminação da gravação.	
31	**Quando deixo de ser cliente de um banco (...).**	✕
a)	O banco deve guardar sempre todos os meus dados, para que na eventualidade de eu querer ser novamente cliente não ser necessário fornecer novamente todos os meus dados pessoais.	escolha 1 opção
b)	O banco deve guardar sempre todos os meus dados, durante 10 anos, para que na eventualidade de eu vir a ser novamente cliente, não ser necessário fornecer novamente todos os meus dados pessoais.	
c)	Tenho direito ao esquecimento, e terei de fornecer novamente os meus dados pessoais se quiser ser novamente cliente do banco.	

32	**Quais das seguintes frases estão corretas?**	✕
a)	Os *cookies* quanto à sua finalidade podem ser estritamente necessários, cookies de funcionalidade, *cookies* de desempenho e *cookies* de marketing.	escolha 1 opção
b)	Os *cookies* quanto à sua duração podem ser *cookies* temporários e *cookies* persistentes.	
c)	Navegar em modo privado permite navegar sem deixar *cookies* armazenados no seu dispositivo.	
d)	Todas as anteriores.	

Tabela 4 - Inquérito de Autoavaliação

Fonte: MetaRed Portugal [76]

Da análise realizada ao segundo inquérito (Autoavaliação da MetaRed Portugal), resultou numa seleção de 6 questões com interesse no universo de 32. A maioria das questões de autoavaliação foram excluídas porque são demasiado concretas e específicas, e avaliam o utilizador e não a infraestrutura tecnológica.

3.2.2. Plataforma para a realização do questionário

Foram consideradas diversas plataformas para desenvolver e disponibilizar o questionário ao público-alvo do presente caso de estudo, como por exemplo a aplicação QuestionPro Essentials[5] e o Google Forms[6]. No entanto, nos vários testes efetuados às aplicações indicadas não preencheram os requisitos pretendidos, nomeadamente a simplicidade no preenchimento do questionário por parte do utilizador.

A plataforma selecionada para preparar e disponibilizar o questionário consistiu no Microsoft Forms[7], sendo uma aplicação bastante intuitiva e efetiva na realização do que se pretendia apurar pois, para além de uma personalização completa do questionário, permite consultar os resultados diretamente do Excel, permitindo uma análise mais facilitada e estruturada.

Na Figura 22 é apresentada a página inicial do questionário, utilizando a aplicação Microsoft Forms acima mencionada.

[5] QuestionPro - https://www.questionpro.com/
[6] Google Forms - https://docs.google.com/forms
[7] Microsoft Forms - https://forms.office.com/

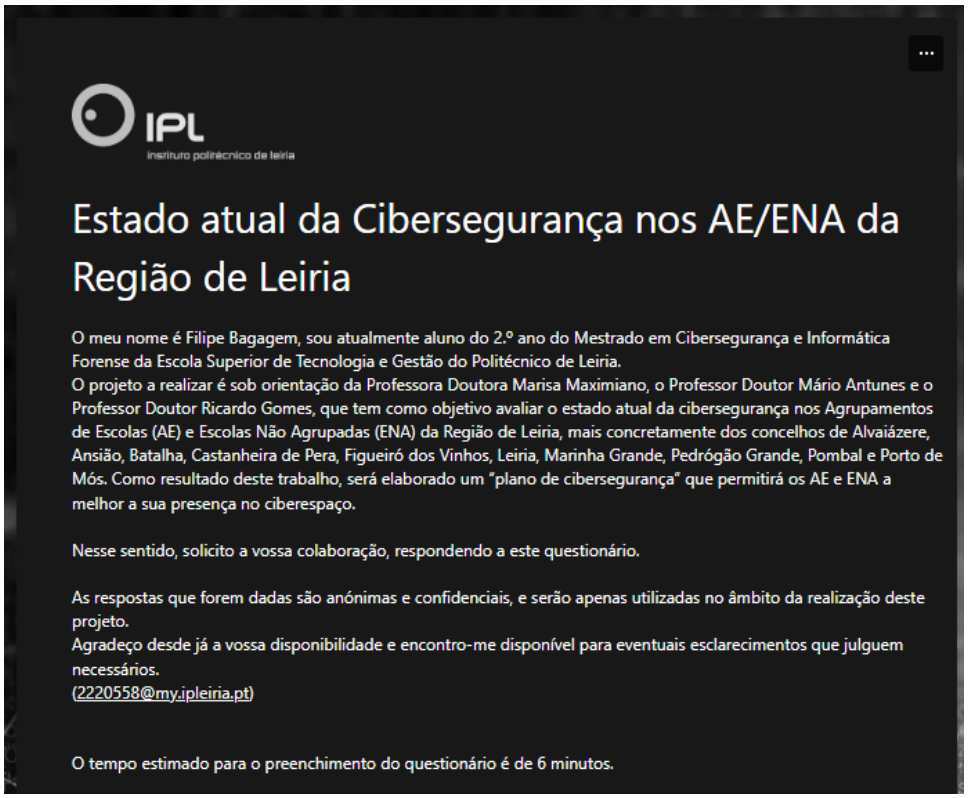


Figura 22 - Ecrã Inicial do Questionário (nota informativa)

No **Anexo B** encontra-se disponível para consulta o questionário final, tal como este foi disponibilizado ao público-alvo do presente caso de estudo.

3.3.Fases do caso de estudo

Neste caso de estudo foram definidas quatro fases, conforme demonstrado na Figura 23. O processo teve início com a caracterização do público-alvo do estudo até recolha e análise dos resultados obtidos.

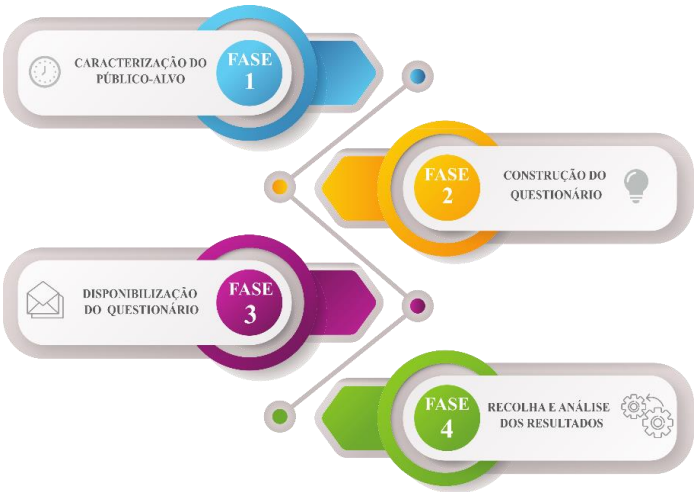


Figura 23 – Processo de Construção e Implementação do Questionário

De seguida são detalhadas as principais atividades envolvidas em cada uma das fases identificadas.

3.3.1. Caracterização do público-alvo

Para a implementação do caso de estudo foram selecionados os Agrupamento de Escolas (AE) e Escolas Não Agrupadas (ENA) que pertencem à região de Leiria, mais concretamente aos concelhos de Alvaiázere, Ansião, Batalha, Castanheira de Pera, Figueiró dos Vinhos, Leiria, Marinha Grande, Pedrógão Grande, Pombal e Porto de Mós, conforme é possível verificar na Figura 24.

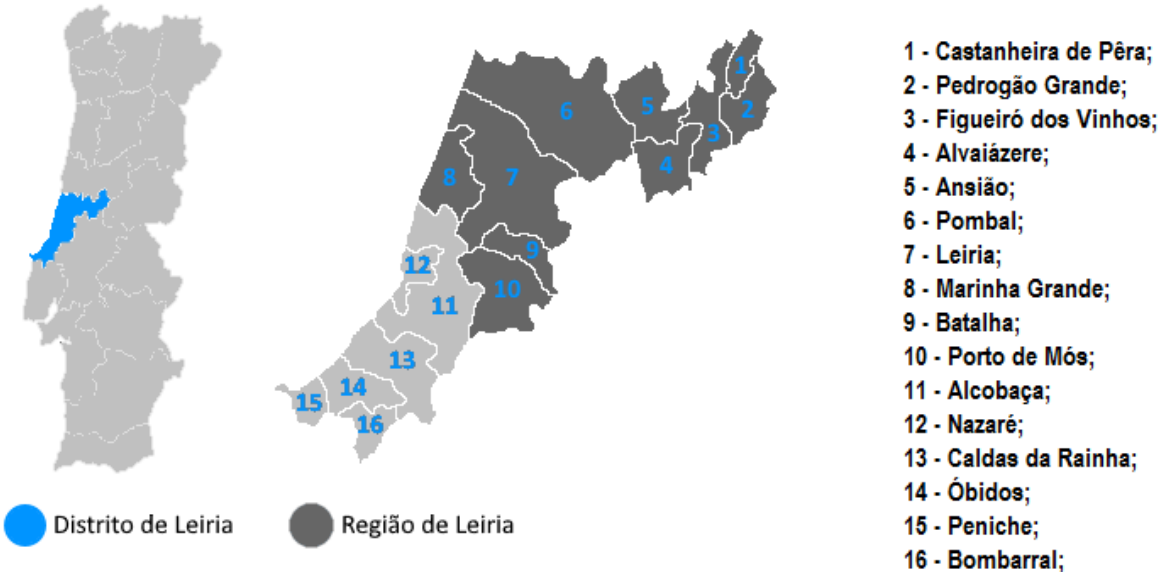


Figura 24 - Concelhos do Distrito de Leiria

De acordo com os últimos dados disponibilizados pelo Instituto de Gestão Financeira da Educação (IGeFE) na plataforma GesEdu [77], na região de Leiria, existem atualmente 23 instituições públicas de ensino (não superior), 21 Agrupamentos de Escolas, e 2 Escolas Não Agrupadas [77], conforme é possível verificar na Tabela 5.

Instituições Públicas de Ensino (não superior)	Concelho	Localidade
Agrup. Escolas de Guia	Pombal	Guia
Agrup. Escolas de Pombal		Pombal
Agrup. Escolas Gualdim Pais		Pombal
Agrup. Escolas de Ansião	Ansião	Ansião
Agrup. Escolas de Alvaiázere	Alvaiázere	Alvaiázere
Agrup. Escolas de Figueiró dos Vinhos	Figueiró dos Vinhos	Figueiró dos Vinhos
Agrup. Escolas de Pedrógão Grande	Pedrogão Grande	Pedrogão Grande
Agrup. Escolas Dr. Bissaya Barreto	Castanheira de Pera	Castanheira de Pera
Escola Secundária Afonso Lopes Vieira	Leiria	Gândara dos Olivais
Escola Secundária Francisco Rodrigues Lobo		Leiria
Agrup. Escolas Caranguejeira – Santa Catarina da Serra		Caranguejeira
Agrup. Escolas D. Dinis		Leiria
Agrup. Escolas de Colmeias		Eira Velha
Agrup. Escolas de Marrazes		Marrazes
Agrup. Escolas Domingos Sequeira		Leiria
Agrup. Escolas Dr. Correia Mateus		Leiria
Agrup. Escolas Henrique Sommer		Maceira
Agrup. Escolas Rainha Santa Isabel		Carreira
Agrup. Escolas de Vieira de Leiria	Marinha Grande	Vieira de Leiria
Agrup. Escolas Marinha Grande Nascente		Marinha Grande
Agrup. Escolas Marinha Grande Poente		Marinha Grande
Agrup. Escolas de Batalha	Batalha	Batalha
Agrup. Escolas de Porto de Mós	Porto de Mós	Porto de Mós

Tabela 5 - Lista de AE e ENA da Região de Leiria

Fonte: IGeFE, GesEdu [77]

Os AE e ENA da região de Leiria contam com 238 estabelecimentos de ensino, conforme é possível verificar na Tabela 6.

Concelho	Estabelecimentos por Nível de Ensino no Ano Letivo 2021/22					Total
	Educação Pré-Escolar	Ensino Básico 1º Ciclo	Ensino Básico 2º Ciclo	Ensino Básico 3º Ciclo	Ensino Secundário / Profissional	
Pombal	26	28	3	4	2	38
Ansião	7	6	2	2	1	11
Alvaiázere	1	1	1	1	1	3
Figueiró dos Vinhos	3	3	1	1	1	7
Pedrogão Grande	2	2	1	1	0	4
Castanheira de Pera	1	1	1	1	0	2
Leiria	63	62	9	10	5	110
Marinha Grande	16	17	3	5	3	29
Batalha	12	10	1	1	1	12
Porto de Mós	16	15	2	2	2	22
Número total de estabelecimentos de ensino						**238**

Tabela 6 - Número de Estabelecimentos de Ensino Públicos na Região de Leiria

Fonte: DGEEC, Educação em Números [9]

De acordo com os dados disponibilizados no relatório designado por "Educação em Números" da DGEEC – Portugal 2023 [9], no ano letivo 2021/22 o número de alunos matriculados na região de Leiria era 42.750. Os três concelhos com um número mais elevado de alunos matriculados, são: Leiria, Pombal e Marinha Grande, com 19.658, 7.486 e 6.428, respetivamente. Os concelhos que ocupam as últimas posições da tabela, são: Castanheira de Pera, Figueiró dos Vinhos e Pedrogão Grande, com 200, 505 e 533, respetivamente. Na Tabela 7 é possível verificar o número de alunos matriculados por Concelho e Nível de Ensino.

Concelho	**Número de Alunos Matriculados no Ano Letivo 2021/22**					**Total**
	Educação Pré-Escolar	**Ensino Básico 1º Ciclo**	**Ensino Básico 2º Ciclo**	**Ensino Básico 3º Ciclo**	**Ensino Secundário**	
Pombal	1231	1660	924	1595	2076	7486
Ansião	229	323	200	353	627	1732
Alvaiázere	99	150	72	145	136	602
Figueiró dos Vinhos	93	126	65	115	106	505
Pedrogão Grande	59	84	43	80	267	533
Castanheira de Pera	39	61	40	60	-	200
Leiria	3489	4842	2573	4162	4592	19658
Marinha Grande	1068	1423	818	1380	1739	6428
Batalha	422	566	304	460	472	2224
Porto de Mós	611	815	452	734	770	3382
Total da Região Leiria	7340	10050	5491	9084	10785	**42750**
Número total de Alunos Matriculados na região de Leiria no ano letivo 2021/22						

Tabela 7 - Número de Alunos Matriculados na Região de Leiria

Fonte: DGEEC, Educação em Números [9]

Dos 42.750 alunos matriculados na região de Leiria, 33.937 são em instituições públicas de ensino que corresponde a uma taxa de 79,38%. No mesmo relatório [9], o número de docentes alocados aos vários níveis de ensino das instituições de ensino da região de Leiria era 4.256, conforme Tabela 8.

Nível de Ensino	**Número de Docentes no Ano Letivo 2021/22**
Educação pré-escolar	460
Ensino básico - 1.º ciclo	832
Ensino básico - 2.º ciclo	556
Ensinos básico (3.º ciclo) e secundário	1 950
Educação especial	257
Formadores (escolas profissionais)	201
Total	**4 256**

Tabela 8 - Número de Docentes nas Instituições de Ensino da Região de Leiria

Fonte: DGEEC, Educação em Números [9]

De acordo com os dados disponibilizados no relatório designado por "Educação em Números" da DGEEC – Portugal 2023 [9], no ano letivo 2021/22 o número de não docentes alocados às instituições de ensino da região de Leiria era 1.869, conforme Tabela 9.

Nível de Ensino	Número de Não Docentes no Ano Letivo 2021/22
Alvaiázere	40
Ansião	98
Batalha	62
Castanheira de Pêra	25
Figueiró dos Vinhos	74
Leiria	828
Marinha Grande	273
Pedrógão Grande	49
Pombal	280
Porto de Mós	140
Total	**1 869**

Tabela 9 - Número de Não Docentes nas Instituições de Ensino na região de Leiria

Fonte: DGEEC, Educação em Números [9]

Dos 1.869 funcionários não docentes na região de Leiria, 1.341 estão alocados às instituições públicas de ensino com uma taxa de 71,75%.

Identificados os tipos de utentes com maior expressão nas instituições de ensino públicas da região de Leiria, nomeadamente os alunos, pessoal docente e não docente, conclui-se que a comunidade escolar nos AE e ENA dos 10 concelhos que compõem esta região está próximo dos 50.000 utentes.

Recursos Tecnológicos das Escolas

De acordo com os dados disponibilizados no relatório designado por "Educação em Números" da DGEEC – Portugal 2023 [9], referente ao ano letivo 2021/22, o número médio é de 1,4 alunos por computador, informação referente às escolas públicas em Portugal Continental, conforme Tabela 10.

N.º médio de alunos/computador	
Ensino básico - 1.º ciclo	1,2
Ensino básico - 2.º ciclo	1,2
Ensino básico - 3.º ciclo	1,2
Ensino Secundário	1,7
Nº médio	**1,4**

Tabela 10 - Nº Médio de Alunos por Computador

Fonte: DGEEC, Boletim informativo Nº4 – Outubro 2023 [78]

Não são conhecidos dados específicos do público-alvo no caso de estudo (AE e ENA da região de Leiria).

Relativamente ao número de computadores com acesso à internet, os números médios mantêm-se em 1,4 alunos por computador, conforme tabela abaixo.

N.º médio de alunos/computador com Internet	
Ensino básico - 1.º ciclo	1,4
Ensino básico - 2.º ciclo	1,2
Ensino básico - 3.º ciclo	1,2
Ensino Secundário	1,8
Nº médio	**1,4**

Tabela 11 - Nº Médio de Alunos por Computador com Internet

Fonte: DGEEC, Boletim informativo Nº4 – Outubro 2023 [78]

O relatório refere ainda que nos estabelecimentos de ensino Público a média de alunos por computador é inferior à dos estabelecimentos de ensino Privado, quer no ensino básico, quer no ensino secundário, conforme é possível verificar na Tabela 12.

Público	**Privado**
Ensino Básico e Secundário	Ensino Básico e Secundário
1,2	**3,4**

Tabela 12 - Nº Médio de Alunos por computador (Público Vs. Privado)

Fonte: DGEEC, Boletim informativo Nº4 – Outubro 2023 [78]

A grande maioria dos equipamentos informáticos existentes nas escolas são para fins pedagógicos. Os computadores portáteis são o tipo de equipamento informático mais frequente, conforme é possível verificar na Figura 25.

De acordo com os dados disponibilizados no relatório designado por "Educação em Números" da DGEEC – Portugal 2023 [9], referente ao ano letivo 2021/22, a grande parte dos equipamentos (computadores de secretária, portáteis e *tablets/iPads*) são para uso pedagógico e destes 23,82% a antiguidade é superior a 3 anos.

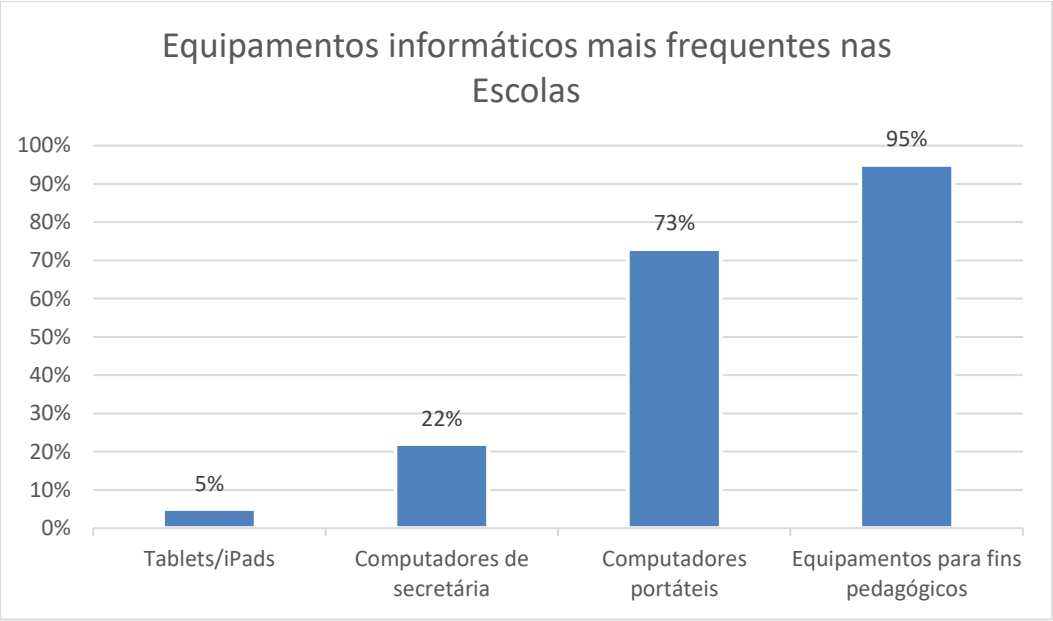


Figura 25 - Equipamentos Informáticos mais Frequentes nas Escolas

Fonte: DGEEC, Boletim informativo Nº4 – Outubro 2023 [78]

Em relação aos equipamentos para fins administrativos, observa-se o oposto, num universo de 43.846 computadores, 72,31% já têm mais de 3 anos de antiguidade, conforme é possível verificar na Tabela 13.

Total de Equipamentos	**Total**	**Inferior ou igual a 3 anos**	**Superior a 3 anos**
	900 556 (100%)	664 769 (100%)	235 787 (100%)
Para fins pedagógicos	856 710 (95%)	652 629 (98%)	204 081 (87%)
Para fins administrativos	43 846 (5%)	12 140 (2%)	31 706 (13%)

Tabela 13 - Total de Equipamentos nas Escolas Públicas, por Antiguidade

Fonte: DGEEC, Boletim informativo Nº4 – Outubro 2023 [78]

Não foram identificados dados sobre outros tipos de equipamentos, como por exemplo os servidores existentes nas instituições de ensino.

3.3.2. Construção do questionário

Nesta 2ª fase foram selecionadas e adaptadas as questões a considerar para a construção do questionário (Estado atual da cibersegurança nos AE/ENA da região de Leiria), com base no trabalho previamente realizado na secção 3.2.1.

Em alguns dos casos, duas e três questões do inquérito IUTIC-2023 deram lugar a uma questão no novo questionário (Estado atual da cibersegurança nos AE/ENA da região de Leiria), conforme o exemplo seguinte.

Origem da questão: Inquérito IUTIC-2023

Módulo: Cibersegurança

Nº da questão: 3

Quem realiza as atividades relacionadas com a segurança das TIC do Organismo? (ex.: testes, formação e resolução de incidentes de segurança. Excluem-se as atualizações de software pré-configurado)		
a)	Pessoal da próprio Organismo	sim / não
b)	Fornecedores externos	sim / não

Questão no novo questionário (Estado atual da cibersegurança nos AE/ENA da região de Leiria)

Nº da questão: 18

Quem realiza as atividades relacionadas com a segurança das TIC da instituição de ensino?		
a)	Pessoal do próprio AE/ENA Técnico(s) de Informática do Município Fornecedores externos	escolha múltipla

Um dos objetivos desta decisão foi o de não tornar o questionário muito extenso para não inviabilizar a obtenção de uma amostra de respostas significativa. Se possível o questionário não deveria de ultrapassar as 30 questões, conforme já indicado anteriormente. A organização do questionário encontra-se descrita em detalhe na secção 3.4 - Questionário.

3.3.3. Disponibilização do questionário

Nesta fase do trabalho (fase 3), tendo em consideração o cronograma definido para o projeto, a disponibilização do questionário teve início no mês de dezembro de 2023, e estendeu-se até meados de janeiro de 2024. A principal razão em disponibilizar o questionário às instituições de ensino da região de Leiria, neste período, prendeu-se com o facto de a interrupção letiva do Natal ocorrer entre o dia 17 de dezembro de 2023, e o dia 2 de janeiro de 2024, conforme é possível verificar no **Anexo E**. Durante este período nas instituições de ensino não decorreram atividades letivas, o que permitiria uma maior disponibilidade tendo em conta que a maioria das Escolas da região de Leiria encontram-se atualmente organizadas por semestres.

Para disponibilizar o questionário aos AE e ENA, foram obtidos primeiramente os e-mails da direção de cada entidade orgânica no próprio website institucional, e no portal GesEdu[8].

Concluído o levantamento de todos os endereços de e-mail, foi realizado o primeiro envio do e-mail (ver **Anexo C**) no dia 2 de dezembro de 2023, no qual a data-limite para o preenchimento do questionário era 31 de dezembro de 2023.

Ainda nesta fase 3, foram realizados contactos com as direções dos AE e ENA para validar a receção do email que tinha sido enviado no dia 2 de dezembro de 2023, com o assunto "Questionário para avaliar o estado atual da cibersegurança nos AE/ENA da região de Leiria - IPLeiria". Em alguns dos casos, foi solicitado o reenvio para outro endereço de e-mail, e o mesmo seguiu de imediato.

3.3.4. **Recolha e análise dos resultados**

Até ao dia 26 de dezembro de 2023 foram rececionadas 7 respostas num universo de 23 possíveis, perfazendo uma taxa de resposta de 30,43%. Tendo em conta que faltavam apenas 5 dias para terminar o período que tinha sido definido para o término do preenchimento do questionário, optou-se por enviar um segundo e-mail com o assunto "Questionário para avaliar o estado atual da cibersegurança nos AE/ENA da Região de Leiria – IPLeiria (2ºPedido)" para relembrar as instituições de ensino da importância na colaboração do estudo (ver **Anexo D**).

Entretanto, até ao dia 31 de dezembro de 2023, foram rececionadas mais 5 respostas perfazendo um total de 12 respostas em 23 possíveis, com uma taxa de resposta de 52,17%.

Já em janeiro de 2024, optou-se por contactar novamente as direções das instituições de ensino, a relembrar que a sua colaboração no seu preenchimento era muito importante e que seria uma enorme contribuição para o presente estudo. Entendeu-se assim alargar o período de resposta ao questionário até ao dia 20 de janeiro de 2024. Neste período alargado foi possível obter mais 5 respostas, terminando o questionário com um total de 17 respostas em 23 possíveis, com uma taxa de resposta de 73,91%.

[8] https://www.gesedu.pt/PesquisaRede/DetalheUO

De uma forma sucinta, resultaram as seguintes marcas temporais:

- **02/12/2023** – Envio do primeiro e-mail "Questionário para avaliar o estado atual da cibersegurança nos AE/ENA da Região de Leiria – IPLeiria;
- **27/12/2023** – Envio do segundo e-mail "Questionário para avaliar o estado atual da cibersegurança nos AE/ENA da Região de Leiria – IPLeiria (2ºPedido);
- **17/12/2023** a **02/01/2024** – Pausa Letiva do Natal;
- **01/01/2024** a **20/01/2024** – Período alargado para obter novas respostas.

Os dados foram recolhidos através da plataforma Microsoft Forms para uma análise estatística. Com recurso ao Excel foi elaborada a análise estatística dos resultados permitindo também a criação de gráficos para uma melhor interpretação dos dados.

3.4. Questionário

O questionário foi organizado em seis secções, com um total de 29 questões, conforme se ilustra na Figura 26 .

Figura 26 - Secções do Questionário

A primeira secção conta apenas com uma questão de resposta opcional, com o objetivo de recolher um endereço de e-mail, que permita no final do estudo enviar o guia de cibersegurança, resultante deste trabalho. A segunda secção é composta por três questões, e tem como principal objetivo caracterizar a entidade orgânica. Na secção 3 são listadas 14 questões para identificar os níveis de segurança das instituições de ensino em relação à

segurança das Tecnologias de Informação e Comunicação (TIC). A secção 4, tem cinco questões para avaliar se as instituições de ensino estão em cumprimento com a legislação em vigor no âmbito da cibersegurança. A secção 5, tem cinco questões que pretende identificar se as instituições de ensino estão a realizar a gestão de incidentes das Tecnologias de Informação (TI). Por último, a secção 6, pretende recolher a opinião pessoal do utilizador que respondeu ao questionário. De seguida, são apresentadas todas as questões, bem como a sua finalidade.

Secção 1	
Nº de questões	**1**
Resposta obrigatória	**Não (resposta opcional)**
Questão 1: Deixe-nos um e-mail caso pretenda receber o "Guia de cibersegurança para as instituições públicas de ensino". A questão 1 é de preenchimento opcional e tem como finalidade recolher o e-mail da entidade interessada em receber posteriormente um exemplar do guia de cibersegurança que será elaborado no âmbito do presente projeto.	

Secção 2	
Caracterização do AE/ENA	
Nº de questões	**3**
Resposta obrigatória	**Sim**
Questão 2: Qual o tipo da Entidade Orgânica? Esta questão tem como propósito identificar o tipo de entidade orgânica para verificar se a sua dimensão tem ou não influência no estado atual de cibersegurança. O universo do público-alvo já é conhecido. Em 23 instituições de ensino, 21 são Agrupamento de Escolas (AE) e 2 são Escolas Não Agrupadas (ENA). **Questão 3: O AE/ENA pertence ao Concelho de _____.** Esta questão tem como finalidade obter os concelhos, aos quais pertencem as instituições de ensino que colaboraram para a realização do presente estudo e mostraram interesse em obter mais informações sobre o mesmo no futuro. Para que as entidades orgânicas possam responder ao questionário, de forma anónima, foi adicionado o tipo de resposta "Prefiro não indicar" porque existiam casos em que o universo em alguns Concelhos era apenas de um Agrupamento de Escolas (AE).	

Questão 4: No AE/ENA realizam campanhas de sensibilização, junto da comunidade escolar, sobre o tema "Cibersegurança"?

A questão 4, tem como objetivo verificar se os AE/ENA realizam campanhas de sensibilização, no âmbito da cibersegurança, junto da comunidade escolar. Para o público-alvo em estudo, era desejável que fosse realizada pelo menos uma campanha de sensibilização sobre o tema cibersegurança por ano letivo. Com a entrada a saída de utentes (alunos, docentes, não docentes, encarregados de educação, etc.) das instituições de ensino todos os anos letivos, é crucial que este tipo de comunicação seja frequente ou muito frequente.

Secção 3	
Estratégia do AE/ENA relativamente à segurança das TIC	
Nº de questões	**14**
Resposta obrigatória	**Sim**

Questão 5: Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores palavras-passe seguras?

Esta questão tem como finalidade identificar se os utilizadores com acesso a informação confidencial, utilizam uma palavra-passe segura. Segundo o *National Institute of Standards and Technology* (NIST), todas as palavras-passe devem ter no mínimo 12 caracteres, com letras maiúsculas e minúsculas, algarismos, caracteres especiais e uma palavra-passe por cada plataforma [79].

Questão 6: Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores Autenticação de Dois Fatores (2FA)?

Esta pergunta tem como objetivo verificar se as instituições de ensino exigem aos utilizadores, com acesso a informação confidencial, um segundo fator de autenticação. Segundo o *National Institute of Standards and Technology* (NIST), o simples utilizador e palavra-passe não é suficiente para garantir a identidade de quem está a fazer o acesso [80].

Questão 7: Para acederem do exterior a recursos internos, utilizam _____.

Esta questão pretende identificar se a política de uso aceitável ou a política de segurança da instituição de ensino permite que determinados utilizadores acedam através da internet (exterior) aos sistemas de informação alojados na própria infraestrutura da instituição de ensino.

Questão 8: No AE/ENA ainda temos equipamentos, em uso, com as seguintes versões do Windows _____.

Esta pergunta tem como finalidade obter se as instituições de ensino ainda dispõem no seu parque tecnológico de Sistemas Operativos Windows com versões descontinuadas, para os quais a Microsoft já deixou de disponibilizar atualizações de segurança. Os equipamentos com sistemas operativos descontinuados apresentam riscos com severidade elevada para as instituições de ensino porque deixaram de ter atualizações de segurança para corrigir vulnerabilidades que, entretanto, foram identificadas. Daqui podem resultar perdas de dados confidenciais, interrupção dos serviços e, claro, prejuízos reputacionais para a instituição de ensino.

Questão 9: As cópias de segurança cumprem a regra 3-2-1?

Pretende-se avaliar se as instituições de ensino seguem as boas práticas relativamente às cópias de segurança. Segundo a *National Institute of Standards and Technology* (NIST), a estratégia de cópias de segurança com a regra 3-2-1 deve ser aplicada para aumentar a probabilidade de recuperação de dados perdidos ou corrompidos. O "3" significa que devem ser realizadas três cópias de qualquer arquivo. O "2" indica que as cópias devem ser mantidas em dois tipos de armazenamentos diferentes. Por fim, o "1" significa que uma das cópias deve ser armazenada num local externo, para evitar que um ataque de *ransomware* possa afetar também as cópias de segurança [81].

Questão 10: As cópias de segurança que são enviadas para locais externos ao servidor são cifradas?

Esta questão tem como propósito verificar se as instituições de ensino estão a cifrar as cópias de segurança que são enviadas para locais externos (internet). Com a cifragem das cópias de segurança é possível garantir a confidencialidade, e só o utilizador com acesso à chave que foi utilizada para cifrar os dados terá acesso à informação protegida [82].

Questão 11: Todas as cópias de segurança dos sistemas em uso pelo AE/ENA são submetidas com regularidade a testes de integridade e recuperação?

Esta pergunta tem como objetivo verificar se as instituições de ensino realizam periodicamente testes de integridade e recuperação das cópias de segurança. Trata-se de uma boa prática para evitar surpresas quando ocorrer um incidente [82].

Questão 12: Dispõem de algum sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar os responsáveis sobre as mesmas?
Esta questão pretende identificar se as instituições de ensino dispõem de sistemas de monitorização e alarmística nos sistemas de TIC. Na resposta não devem considerar como resposta o software de antivírus como sistema de monitorização e alarmística. São várias as soluções existentes no mercado de monitorização da segurança das TIC, como por exemplo o *Nagios*, o *Cacti*, o *SpiceWorks*, o *Observium*, o *Zabbix*, entre outras [83]. Não se pretende aferir especificamente qual a ferramenta, mas sim se dispõem de alguma.

Questão 13: Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a uma Análise de Vulnerabilidades?
Esta questão tem como finalidade verificar se as instituições de ensino realizaram alguma análise das vulnerabilidades dos seus sistemas nos últimos dois anos. É recomendada que esta análise de vulnerabilidades seja realizada com frequência [84].

Questão 14: Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a um Teste de Intrusão?
Esta questão tem como propósito verificar se as instituições de ensino realizam algum teste de intrusão aos seus sistemas nos últimos dois anos. Os testes de intrusão ou penetração (*pentesting*) permitem identificar pontos fracos e avaliar a postura da organização relativamente à segurança dos seus sistemas. De acordo com o *Relatório de Pen Testing de 2023* da FORTRA, a maioria dos profissionais de segurança cibernética (38%) realiza um teste de intrusão, uma ou duas vezes por ano [85].

Questão 15: O AE/ENA possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC?
Esta questão tem como propósito verificar se as instituições de ensino dispõem de documentação sobre as medidas, práticas ou procedimentos no âmbito da segurança das TIC. Alguns dos exemplos, são:

- Política de Segurança Digital: orientações para o uso da internet e dos dispositivos digitais em segurança e como recurso educativo;
- Política de Privacidade e Proteção de Dados;
- Política de Utilização Aceitável (PUA) das TIC – Alunos / Docentes / Não Docentes.

Questão 16: Quando foram definidas ou revistas as recomendações sobre medidas, práticas ou procedimentos de segurança TIC?

A questão número 16 é de preenchimento obrigatório para quem responder "Sim" na questão anterior (15), e tem como finalidade verificar há quanto tempo foi realizada uma revisão às medidas, práticas ou procedimentos de segurança TIC. Com a crescente evolução tecnológica, a documentação terá de ser ajustada com regularidade.

Questão 17: Nas recomendações sobre medidas, práticas ou procedimentos de segurança TIC foram considerados os seguintes temas _____.

A questão número 17 é de preenchimento obrigatório para quem respondeu "Sim" na questão número 15, e tem como finalidade obter quais os planos que fazem parte da documentação de cibersegurança da instituição de ensino, nomeadamente:

- Gestão dos níveis de acesso às TIC (ex.: computadores, redes);
- Procedimentos e regras para prevenir e/ou reagir a incidentes de segurança (ex.: negação de serviço, ataques de *phishing*, *ransomware*, etc.);
- Responsabilidade, direitos e deveres no que respeita à utilização das TIC (ex.: uso de e-mails, dispositivos móveis, *social media*, etc.);
- Boas práticas para o pessoal ao serviço na utilização segura das TIC.

Questão 18: Quem realiza as atividades relacionadas com a segurança das TIC da instituição de ensino?

Esta questão tem como propósito verificar quem realiza as atividades relacionadas com a segurança das TIC na instituição de ensino, com a possibilidade de escolha múltipla:

- Pessoal do próprio AE/ENA;
- Técnico(s) de Informática do Município;
- Fornecedores externos.

O objetivo é tentar perceber se as instituições de ensino recorrem a recursos humanos internos para assumir os riscos relacionados com a segurança das TIC ou se recorrem a recursos externos, transferindo o risco para fora da instituição de ensino.

Secção 4	
Cumprimento da legislação em vigor	
Nº de questões	**5**
Resposta obrigatória	**Sim**

Questão 19: Designou um responsável de segurança junto do CNCS (Centro Nacional de Cibersegurança)?

Esta questão tem como propósito verificar se as instituições de ensino nomearam um responsável de segurança, e se este foi comunicado ao CNCS, de acordo com o Decreto-Lei n.º 65/2021, de 30 de julho [51].

Questão 20: Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços?

Esta questão tem como propósito verificar se as instituições de ensino têm o inventário atualizado com todos os ativos essenciais para a prestação dos seus serviços. Entende-se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços. De acordo com o Decreto-Lei n.º 65/2021, de 30 de julho [51] as organizações devem elaborar e manter o inventário sempre atualizado com todos os ativos essenciais para a prestação dos respetivos serviços, devendo o mesmo ser assinado pelo responsável de segurança, e remetido para o CNCS.

Questão 21: Elaborou e mantém atualizado o plano de (ciber) segurança, devidamente documentado e assinado pelo responsável de segurança?

Esta questão tem como propósito verificar se as instituições de ensino têm um plano de cibersegurança, devidamente documentado e assinado pelo responsável de segurança. O plano de segurança é um documento dinâmico e estruturado que deve descrever como uma entidade aborda todas as suas necessidades de segurança de informação e cibersegurança. As organizações devem elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, que contenha os elementos identificados no Decreto-Lei n.º 65/2021, de 30 de julho [51].

Questão 22: Elaborou o relatório anual de segurança no ano transato?

Esta questão tem como finalidade verificar se as instituições de ensino elaboraram o relatório anual de segurança no ano transato. De acordo com o Decreto-Lei n.º 65/2021,

de 30 de julho [42] as entidades devem fazê-lo todos os anos. Este relatório deve ser assinado pelo responsável de segurança e remetido ao CNCS por meios eletrónicos.

Questão 23: Efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)?
Esta questão tem como propósito verificar se as instituições de ensino comunicaram ao CNCS o ponto de contacto permanente, o responsável de segurança, a lista de ativos e o relatório anual, de acordo com o Regulamento n.º 183/2022 [86].

Secção 5	
Gestão de Incidentes de TI	
Nº de questões	**5**
Resposta obrigatória	**Sim**

Questão 24: No AE/ENA existe um plano de resposta e de recuperação de incidentes?
Esta questão tem como finalidade verificar se as instituições de ensino dispõem de um plano de resposta e de recuperação de incidentes.

Questão 25: O plano de resposta a incidentes do AE/ENA inclui _____.
A questão número 25 é de preenchimento obrigatório para quem respondeu "Sim" na questão anterior (questão 24), e tem como finalidade obter quais os tópicos que fazem parte do plano de resposta a incidentes da instituição de ensino, com a possibilidade de escolha múltipla:

- Plano de continuidade de negócios;
- Plano de contingência;
- Plano de recuperação em caso de desastre;
- Plano de gestão de crise.

O Plano de Resposta a Incidentes (PRI) é um documento que descreve as ações a serem realizadas quando ocorrerem eventos que possam comprometer a segurança dos sistemas, informações ou infraestrutura da organização. O objetivo deste plano é minimizar o impacto do incidente e restaurar a normalidade das operações o mais rápido possível. Os planos devem ser atualizados com frequência.

Questão 26: São realizadas simulações com o plano de resposta a incidentes para verificar da sua eficácia, com que frequência?

A questão número 26 é de preenchimento obrigatório para quem respondeu "Sim" na questão número 24, e tem como finalidade obter se as instituições de ensino que têm um plano de resposta a incidentes realizam simulações para aferir da sua eficácia.

Questão 27: O AE/ENA, nos últimos 24 meses, sofreu algum incidente de segurança nos serviços TIC?

Esta questão tem como propósito verificar se as instituições de ensino sofreram algum incidente de segurança nos últimos 24 meses.

Questão 28: Realizaram a análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam?

Com esta questão pretende-se verificar se as instituições de ensino fazem a análise dos riscos em relação a todos os ativos. A metodologia para realização de análise de riscos encontra-se prevista no artigo 10.º do Decreto-Lei n.º 65/2021, de 30 de julho [51]. Assim, o n.º 1 do referido artigo 10.º determina que as entidades da Administração Pública devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação.

Secção 6	
Opinião pessoal para finalizar	
Nº de questões	**1**
Resposta obrigatória	**Sim**

Questão 29: Na sua opinião e numa escala de 1 a 5, o estabelecimento de ensino ao qual pertence está preparado para os desafios da cibersegurança?

A questão número 29 era de preenchimento obrigatório e tem como finalidade obter qual a opinião pessoal do inquirido sobre a preparação do estabelecimento de ensino para os desafios da cibersegurança.

No **Anexo B** encontra-se para consulta o questionário final, tal como este foi disponibilizado aos AE e ENA da região de Leiria.

3.5.Apresentação e análise dos dados

Esta secção tem como objetivo apresentar os principais resultados do estudo quantitativo resultante da análise estatística dos dados recolhidos através da aplicação do questionário aos AE e ENA da região de Leiria.

Questão 1: E-mail

Das 17 respostas obtidas, 10 AE/ENA indicaram um endereço de e-mail para receberem através deste um exemplar do Guia de Cibersegurança, perfazendo uma taxa de 58,82%, conforme é possível verificar na Figura 27. A maior parte dos utilizadores que responderam ao questionário mostraram interesse em receber o "Guia de Cibersegurança para as instituições públicas de ensino".

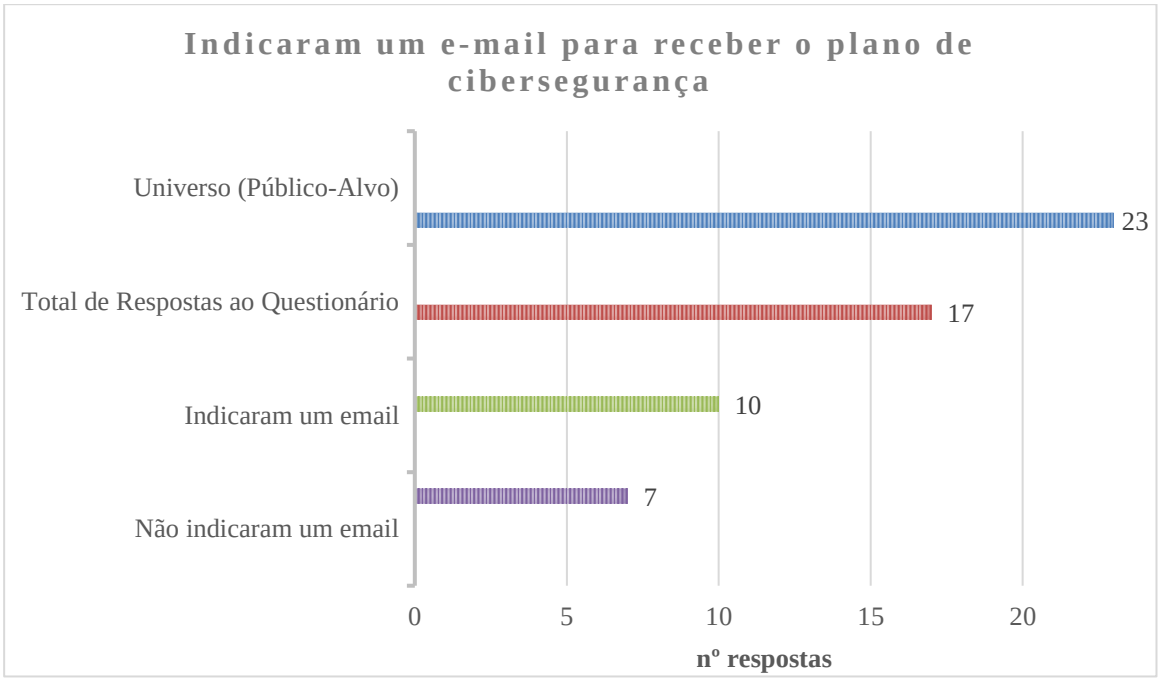


Figura 27 – Questão 1: Recolha do E-mail

Questão 2: Qual o tipo da Entidade Orgânica?

Na Figura 28 é possível verificar que dos Agrupamentos de Escolas (AE), obteve-se uma taxa de resposta ao questionário de 76% (16 respostas em 21 possíveis), e das Escolas Não Agrupadas (ENA), obteve-se uma taxa de resposta ao questionário de 50% (1 resposta em 2 possíveis).

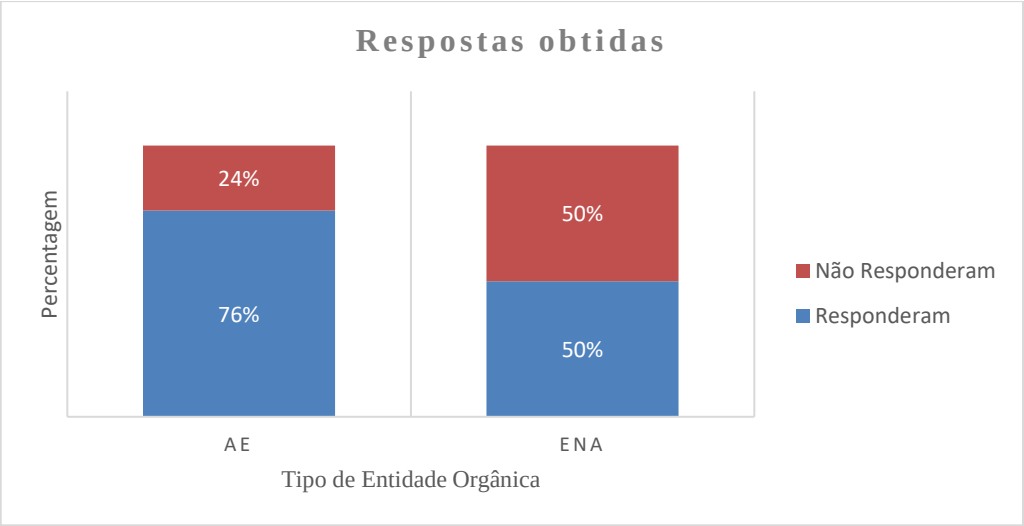


Figura 28 - Questão 2: Respostas Obtidas

Questão 3: O AE/ENA pertence ao Concelho

Uma das entidades orgânicas preferiu não identificar o Concelho a que pertence, porque era dada essa possibilidade de responder de forma anónima. Das respostas obtidas, verifica-se uma taxa de participação de 100% das entidades orgânicas dos Concelhos de Alvaiázere, Ansião, Batalha, Castanheira de Pera, Marinha Grande e Pedrogão Grande. A colaboração das entidades orgânicas do Concelho de Leiria atingiu os 60%, conforme é possível verificar na Figura 29.

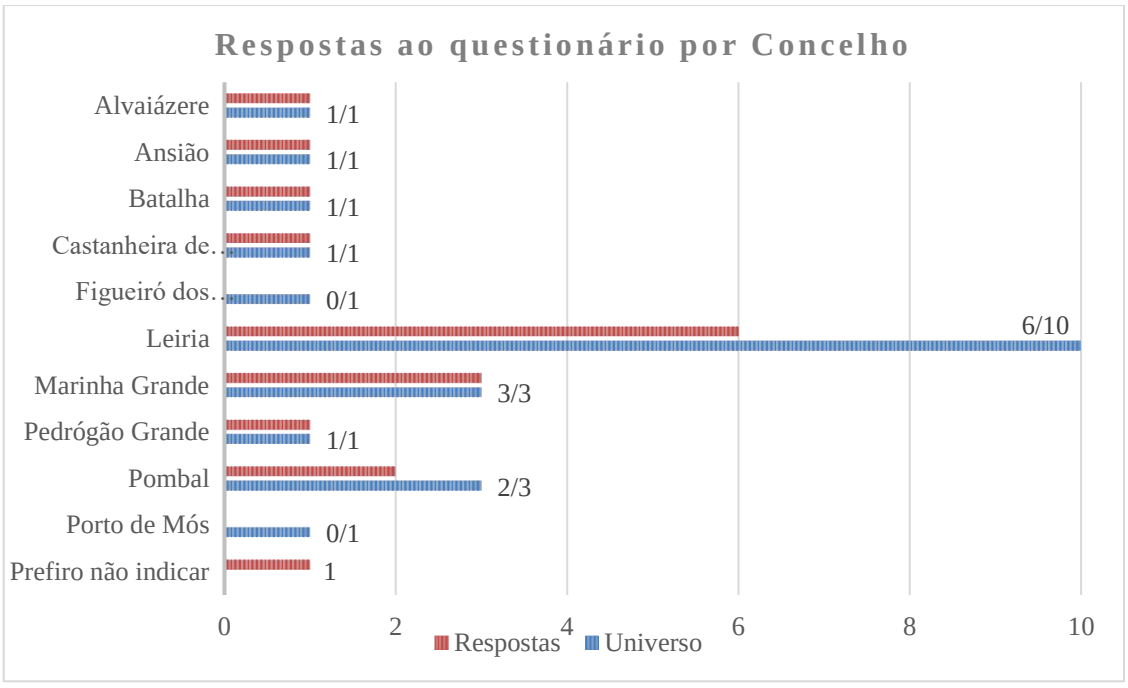


Figura 29 – Questão 3: Respostas por Concelho

Questão 4: No AE/ENA realizam campanhas de sensibilização, junto da comunidade escolar, sobre o tema "Cibersegurança"?

É possível concluir que a maioria das instituições de ensino (58,81%), que responderam ao questionário, não realizam campanhas de sensibilização com a periodicidade que seria desejável, conforme é possível verificar na Figura 30.

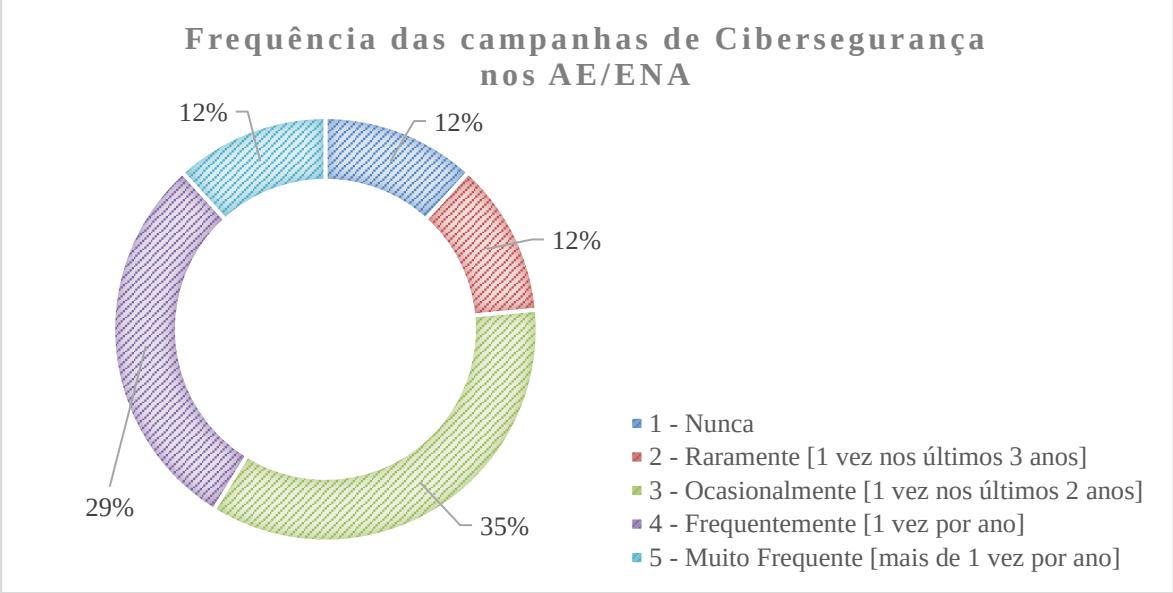


Figura 30 – Questão 4: Frequência das Campanhas de Cibersegurança

Questão 5: Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores palavras-passe seguras?

É possível concluir que a maioria das instituições de ensino (64,71%), que responderam ao questionário, exigem aos utilizadores palavras-passe seguras para acederem a dados confidenciais, conforme é possível verificar na Figura 31.

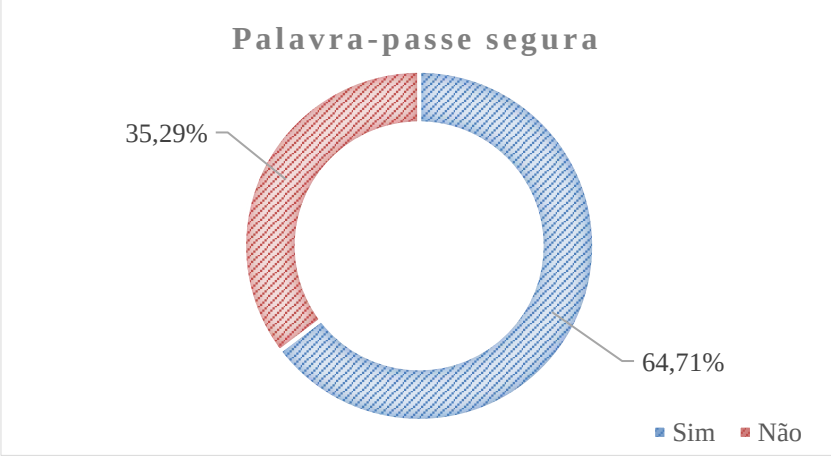


Figura 31 – Questão 5: Palavras-passe Seguras

Questão 6: Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores Autenticação de Dois Fatores (2FA)?

Das respostas obtidas, apenas 11,76% dos inqueridos é que estão a exigir este método de autenticação, conforme é possível verificar na Figura 32.

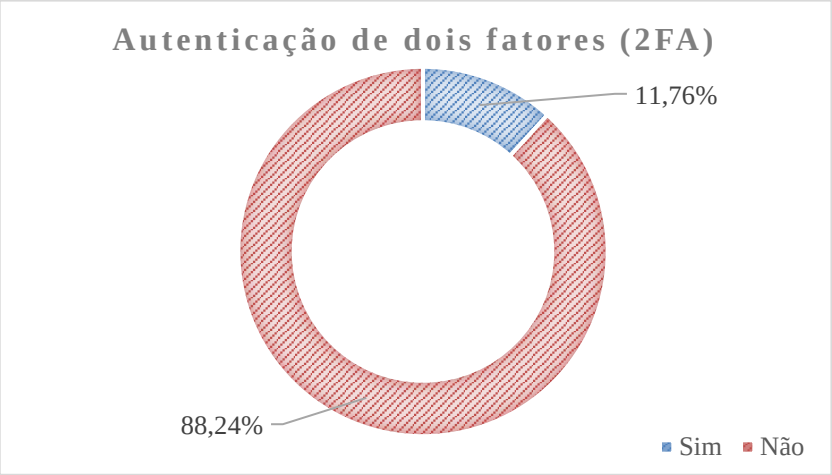


Figura 32 – Questão 6: Autenticação 2FA

Questão 7: Para acederem do exterior a recursos internos, utilizam _____.

A maioria (64,71%) das instituições de ensino recorrem a aplicações de *Remote Desktop*, como o *TeamViewer*[9], o *AnyDesk*[10], entre outras aplicações do género, para acederem aos sistemas internos. Apenas 11,76% das instituições de ensino têm uma política de segurança que não permite este tipo de acesso, conforme é possível verificar na Figura 33.

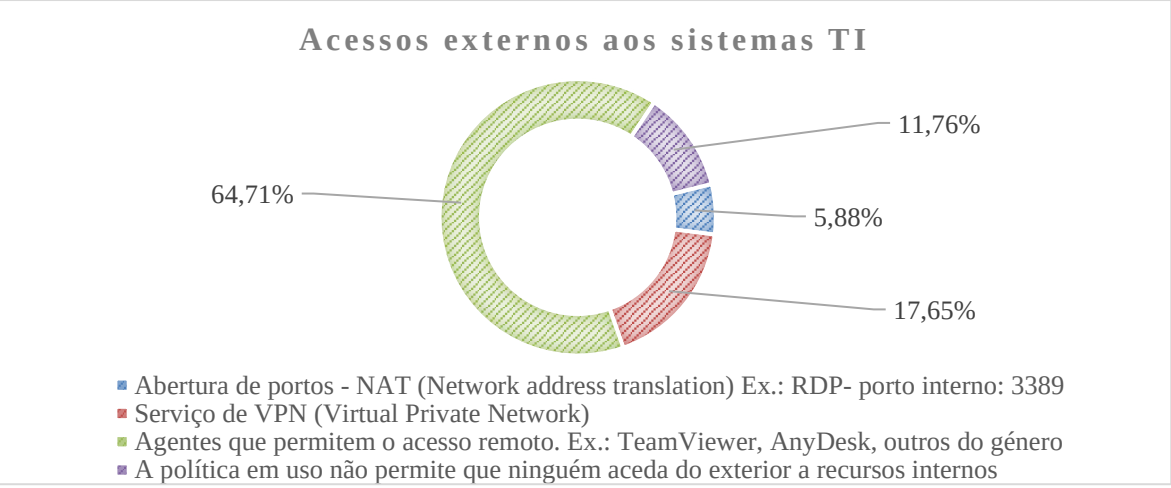


Figura 33 – Questão 7: Acessos Externos aos Sistemas TI

[9] https://www.teamviewer.com
[10] https://anydesk.com

Questão 8: No AE/ENA ainda temos equipamentos, em uso, com as seguintes versões do Windows _____.

Apenas 1 entidade orgânica em 17, que responderam ao questionário, diz não ter sistemas operativos com versões descontinuadas, concluindo-se assim que 94,12% das instituições de ensino ainda têm sistemas operativos descontinuados em funcionamento.

O Windows 7 é o sistema operativo *Workstation* que está presente num maior número de instituições de ensino que foram inquiridas, perfazendo um total de 70,59%, conforme é possível verificar na Figura 34. A Microsoft deixou de prestar suporte a este sistema operativo no dia 14 de janeiro de 2020 [87].

O Windows Server 2012 é o sistema operativo que está presente em mais instituições de ensino que foram inquiridas, perfazendo um total de 58,82%, conforme é possível verificar na Figura 34. A Microsoft deixou de prestar suporte a este sistema operativo no dia 10 de outubro de 2023 [88].

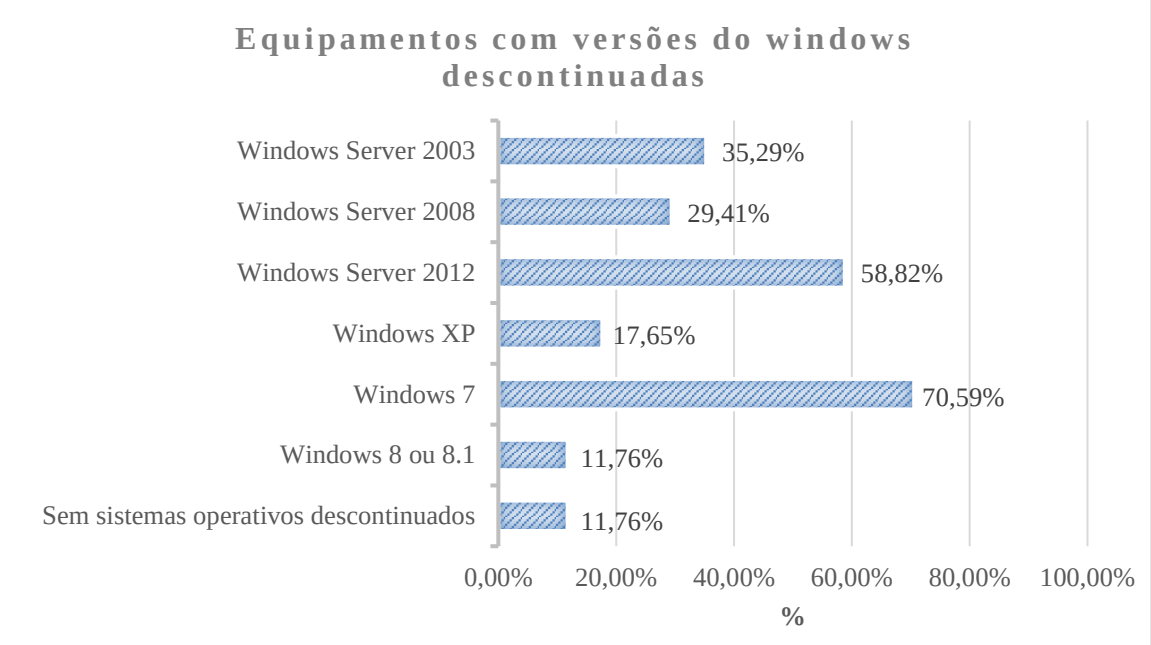


Figura 34 – Questão 8: Equipamentos com Versões do Windows Descontinuadas

Questão 9: As cópias de segurança cumprem a regra 3-2-1?

Das respostas obtidas, só 52,94% dos inqueridos é que está a realizar cópias de segurança para três suportes diferentes, conforme é possível verificar na Figura 35.

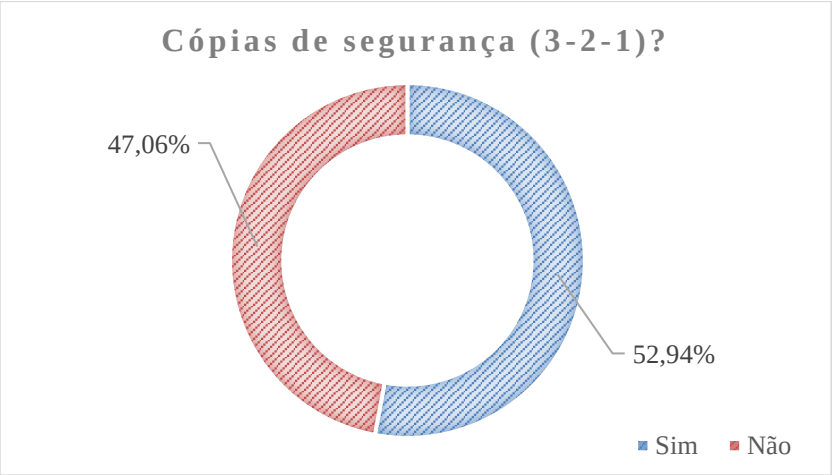


Figura 35 – Questão 9: Cópias de Segurança 3-2-1

Questão 10: As cópias de segurança que são enviadas para locais externos ao servidor são cifradas?

A maioria (70,59%) das instituições de ensino não cifram as cópias de segurança que são enviadas para fora dos servidores, conforme é possível verificar na Figura 36.

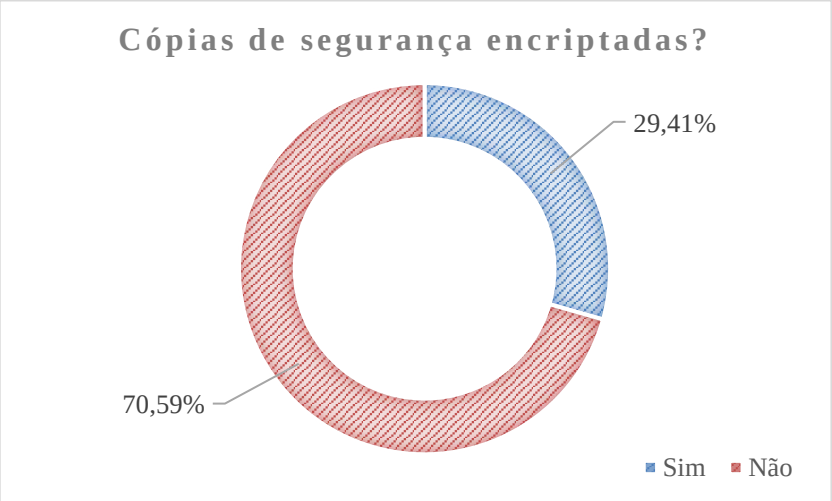


Figura 36 – Questão 10: Cópias de Segurança Cifradas

Questão 11: Todas as cópias de segurança dos sistemas em uso pelo AE/ENA são submetidas com regularidade a testes de integridade e recuperação?

A maioria (64,71%) das instituições de ensino não realizam esta tarefa de verificação das cópias de segurança, conforme é possível verificar na Figura 37.

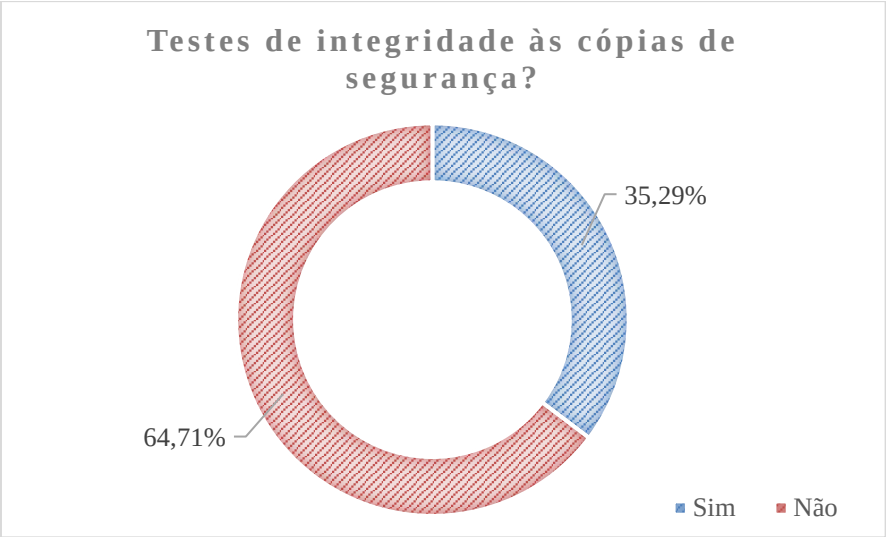


Figura 37 – Questão 11: Testes de Integridade às Cópias de Segurança

Questão 12: Dispõem de algum sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar os responsáveis sobre as mesmas?

Das respostas obtidas, só 47,06% dos inqueridos é que dispõem de sistemas de monitorização e alarmística para detetar atividades suspeitas nos próprios sistemas de TIC, conforme é possível verificar na Figura 38.

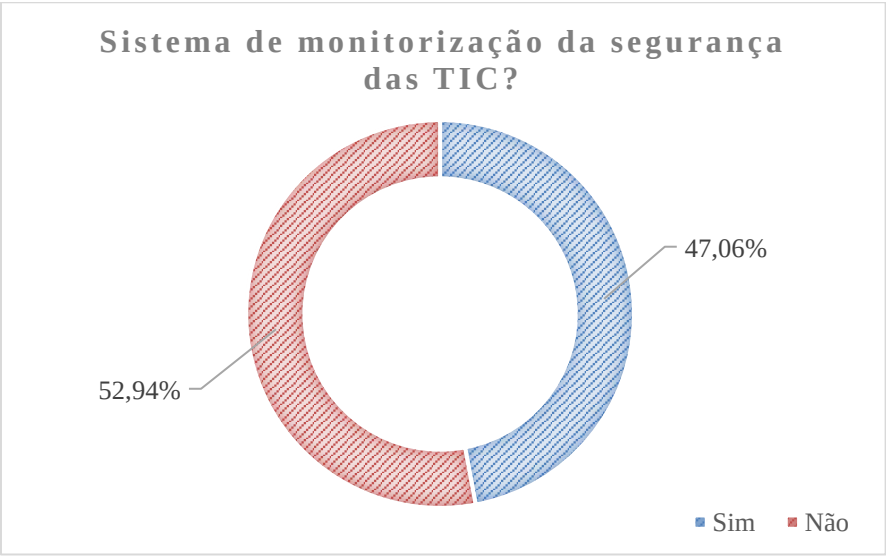


Figura 38 – Questão 12: Sistema de Monitorização da Segurança das TIC

Questão 13: Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a uma Análise de Vulnerabilidades?

A maioria (88,24%) das instituições de ensino não realizou a análise de vulnerabilidades nos seus sistemas nos últimos dois anos, conforme é possível verificar na Figura 39.

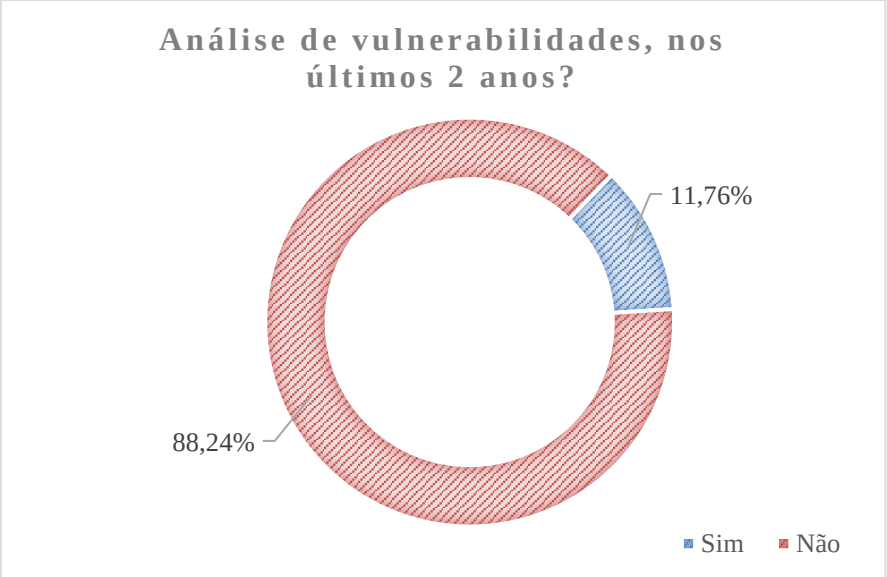


Figura 39 – Questão 13: Análise de Vulnerabilidades nos Últimos 2 Anos

Questão 14: Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a um Teste de Intrusão?

A maioria (82,35%) das instituições de ensino não realizou um teste de intrusão nos seus sistemas nos últimos dois anos, conforme é possível verificar na Figura 40.

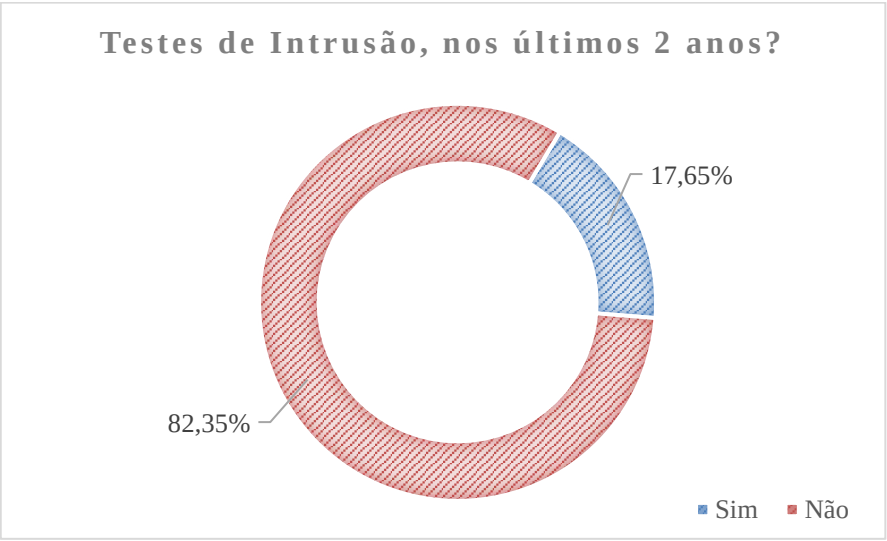


Figura 40 – Questão 14: Testes de Intrusão nos Últimos 2 Anos

Questão 15: O AE/ENA possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC?

Das respostas obtidas, apenas 41,18% dos inqueridos dizem ter documentação sobre a segurança das TIC, conforme é possível verificar na Figura 41.

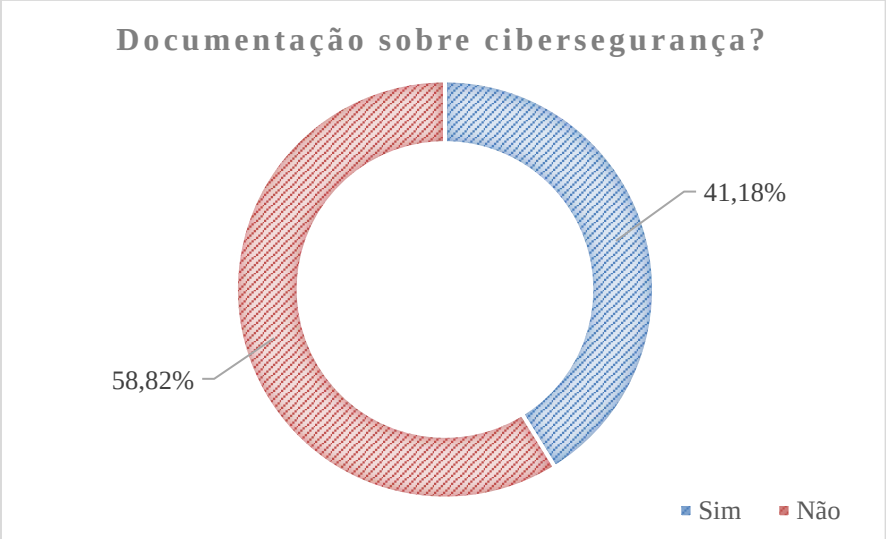


Figura 41 – Questão 15: Documentação Sobre Cibersegurança

Questão 16: Quando foram definidas ou revistas as recomendações sobre medidas, práticas ou procedimentos de segurança TIC?

Das 17 respostas obtidas ao questionário, apenas 7 instituições de ensino (41,18%) possuem documentação sobre cibersegurança. Destas 7 instituições de ensino, 57,14% não atualizaram a documentação sobre a cibersegurança nos últimos 24 meses. Enquanto que 28,57% dizem ter atualizado a documentação sobre a segurança das TIC nos últimos 12 meses, conforme é possível verificar na Figura 42.

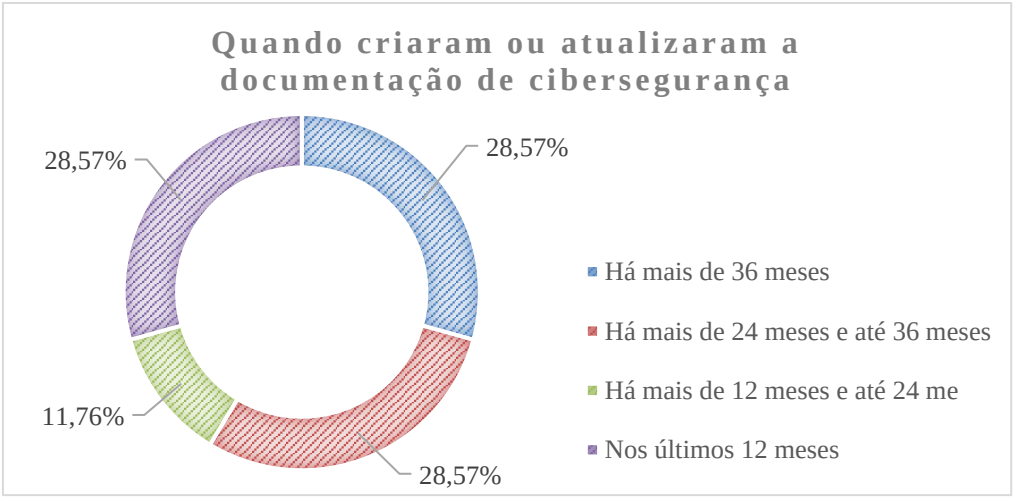


Figura 42 – Questão 16: Criação e Atualização da Documentação de Cibersegurança

Questão 17: Nas recomendações sobre medidas, práticas ou procedimentos de segurança TIC foram considerados os seguintes temas _____.

Das 17 respostas obtidas ao questionário, apenas 7 instituições de ensino (41,18%) possuem documentação sobre cibersegurança. Um dos temas que é abordado por todas as instituições de ensino, com documentação sobre a cibersegurança, é as "Boas práticas para o pessoal ao serviço na utilização segura das TIC". Situação que não se verifica com os restantes temas, como as "Responsabilidade, direitos e deveres no que respeita à utilização das TIC" e a "Gestão dos níveis de acesso às TIC" que apenas surge na documentação de 71,43% das instituições de ensino. O tema "Procedimentos e regras para prevenir e/ou reagir a incidentes de segurança" apenas 57,14% das 7 instituições de ensino dizem abordar este tema na documentação, conforme é possível verificar na Figura 43.

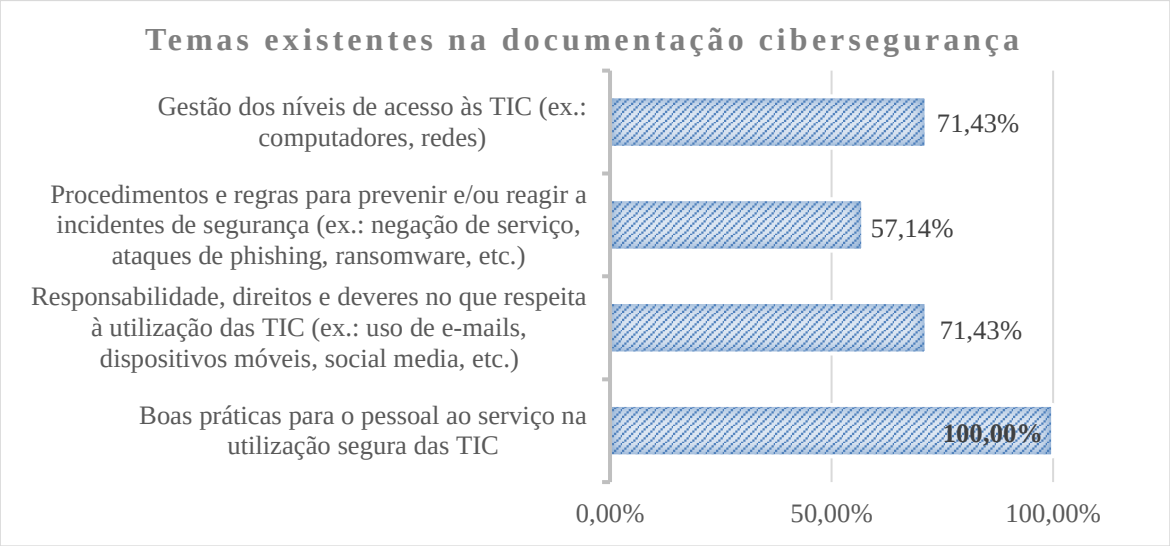


Figura 43 – Questão 17: Temas Existentes na Documentação de Cibersegurança

Questão 18: Quem realiza as atividades relacionadas com a segurança das TIC da instituição de ensino?

Na maioria das instituições de ensino (88,24%), as tarefas relacionadas com a segurança dos sistemas são realizadas por pessoal do próprio AE/ENA. Desta forma, o risco é assumido pela própria instituição de ensino. Apenas 35,29% recorrem a serviços externos passa assegurar as atividades relacionadas com a segurança das TIC, conforme é possível verificar na Figura 44.

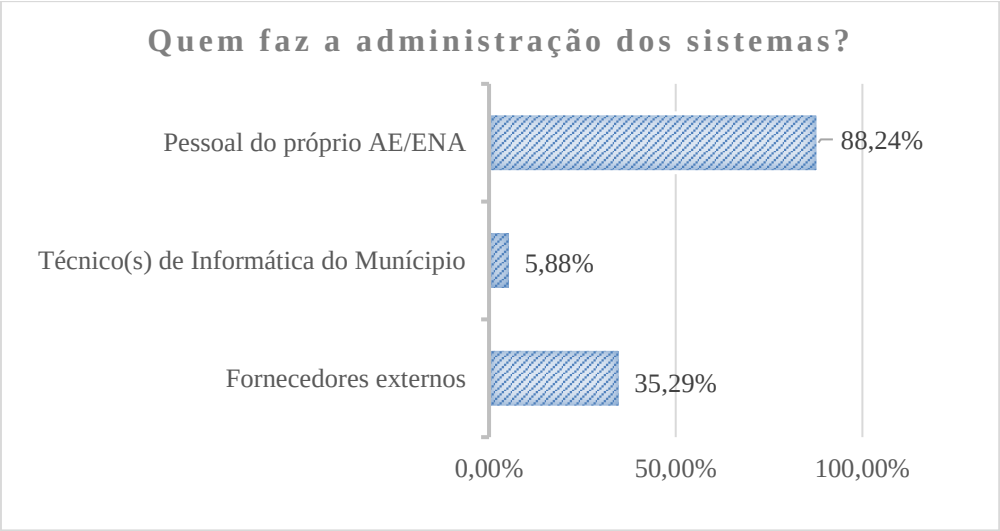


Figura 44 – Questão 18: Quem faz a Administração dos Sistemas

Questão 19: Designou um responsável de segurança junto do CNCS (Centro Nacional de Cibersegurança)?

Apenas 11,76% das instituições de ensino nomearam um responsável de segurança e fizeram a respetiva comunicação ao CNCS, conforme é possível verificar na Figura 45.

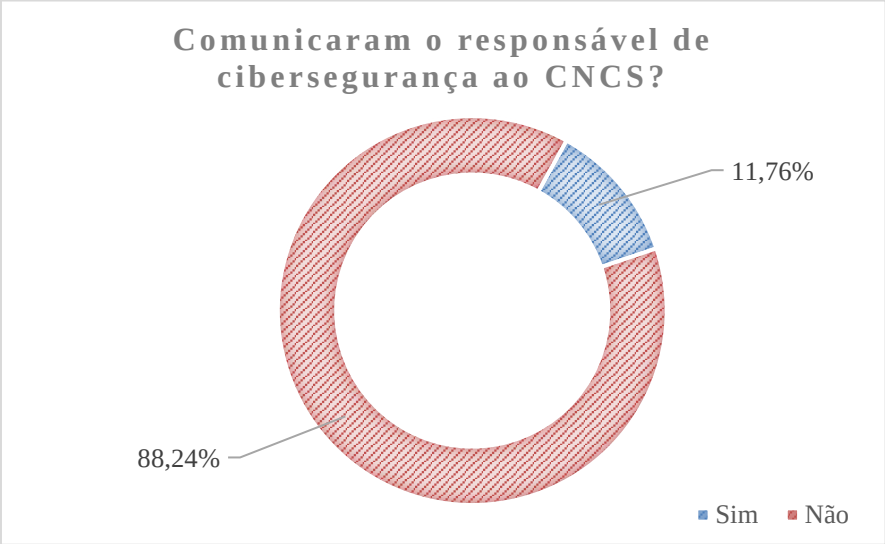


Figura 45 – Questão 19: Comunicaram o Responsável de Cibersegurança ao CNCS

Questão 20: Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços?

Das respostas obtidas, só 52,94% dos inqueridos dizem ter o inventário com todos os ativos essenciais para o desempenho da sua atividade, conforme é possível verificar na Figura 46.

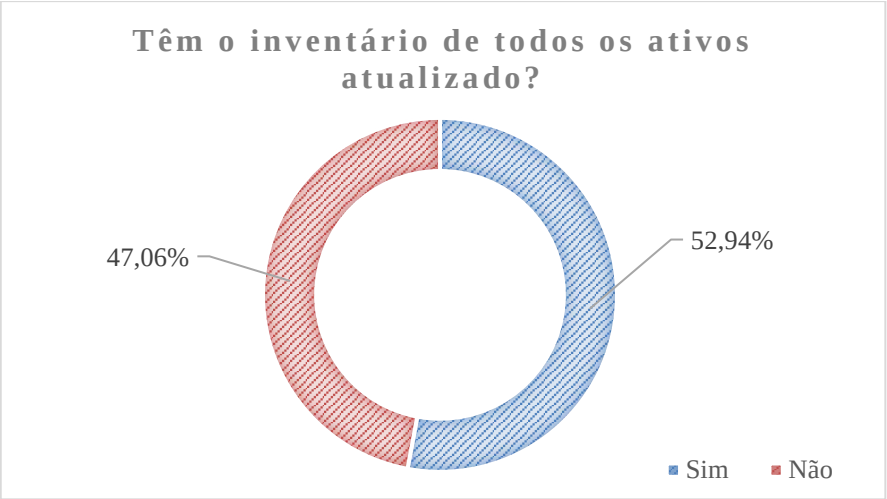


Figura 46 – Questão 20: Existência de Inventário de Todos os Ativos Atualizados

Questão 21: Elaborou e mantém atualizado o plano de (ciber) segurança, devidamente documentado e assinado pelo responsável de segurança?

A maioria das instituições de ensino (94,12%) não dispõem de um plano de cibersegurança, assinado pelo responsável de segurança, conforme é possível verificar na Figura 47.

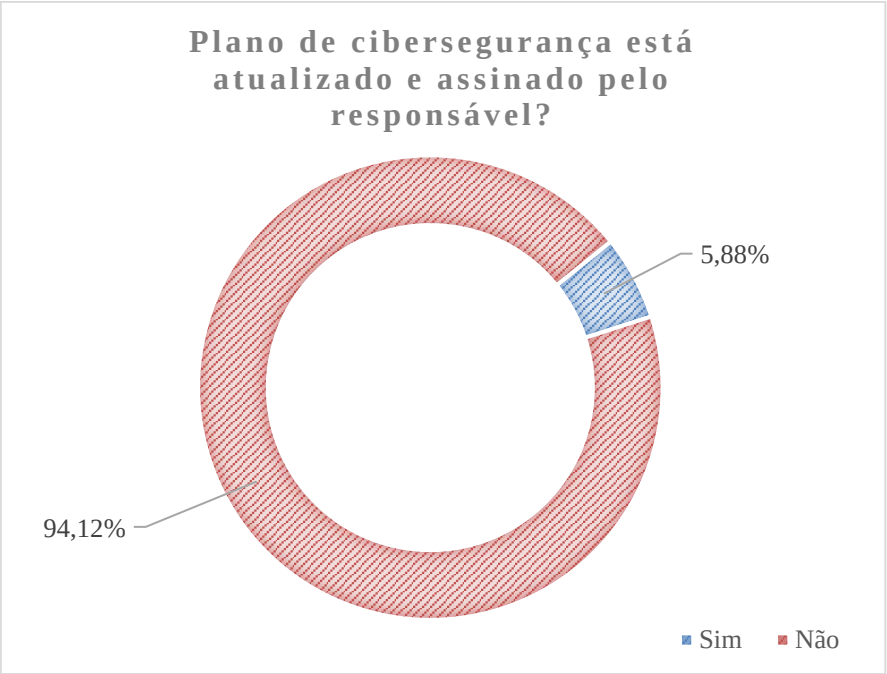


Figura 47 – Questão 21: Plano de Cibersegurança está Atualizado e Assinado pelo Responsável

Questão 22: Elaborou o relatório anual de segurança no ano transato?

A maioria das instituições de ensino (94,12%) não elaboraram o relatório anual de segurança no ano transato, conforme é possível verificar na Figura 48.

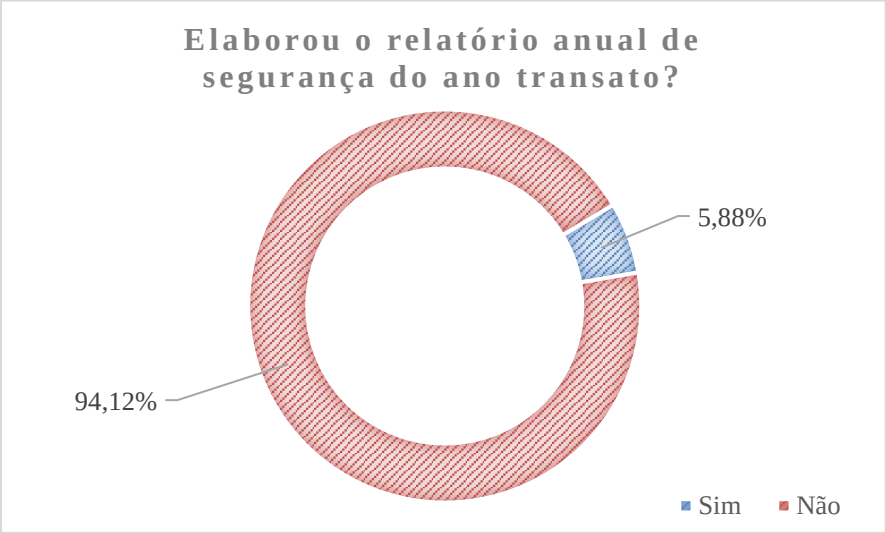


Figura 48 – Questão 22: Elaborou o Relatório Anual de Segurança no Ano Transato

Questão 23: Efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)?

A maioria das instituições de ensino (94,12%) não comunicaram ao CNCS: o ponto de contacto permanente, o responsável de segurança, o inventário de ativos, o relatório anual e a notificação de incidentes, conforme é possível verificar na Figura 49.

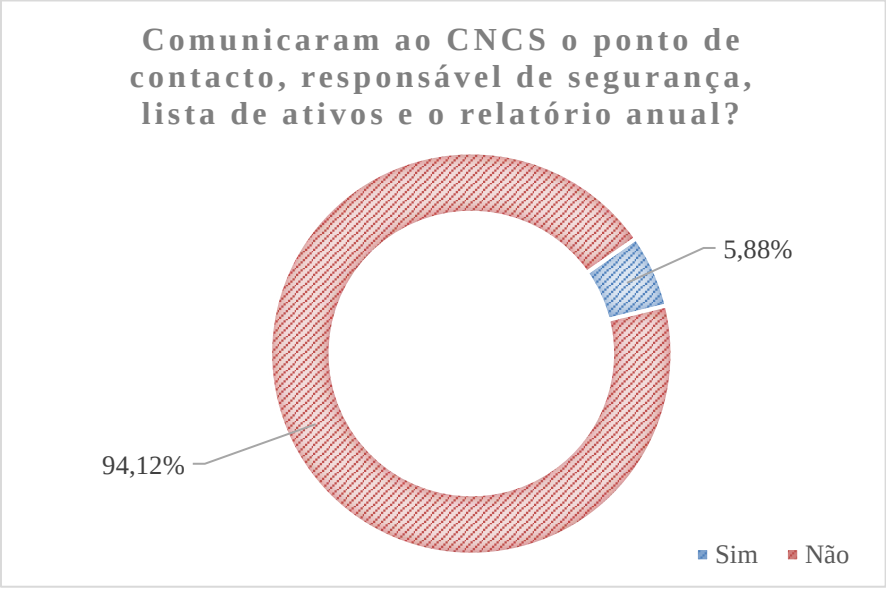


Figura 49 – Questão 23: Comunicações ao CNCS

Questão 24: No AE/ENA existe um plano de resposta e de recuperação de incidentes?

A maioria das instituições de ensino (94,12%) não têm um plano de resposta e de recuperação de incidentes, conforme é possível verificar na Figura 50.

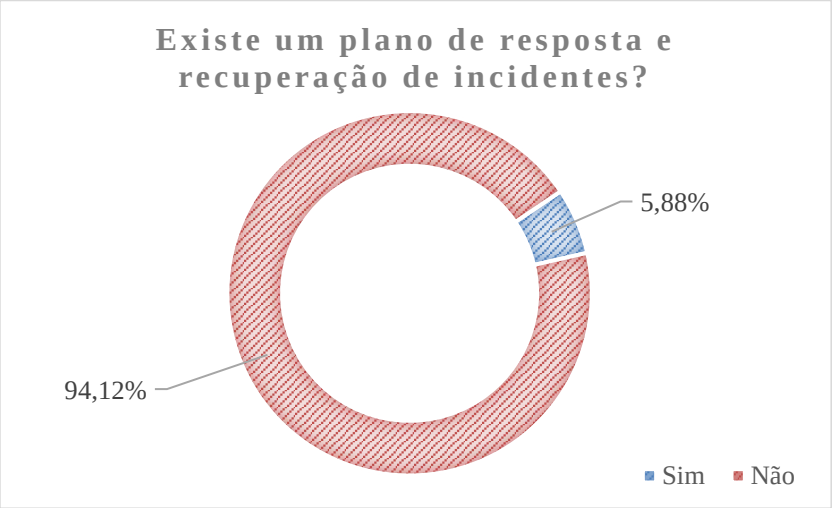


Figura 50 – Questão 24: Existe um Plano de Resposta e Recuperação de Incidentes

Questão 25: O plano de resposta a incidentes do AE/ENA inclui _____.

Das 17 respostas obtidas, só uma instituição de ensino é que possui um plano de resposta e de recuperação de incidentes, conforme é possível verificar na Figura 51. Esta mesma instituição só dispõe do plano de recuperação em caso de desastre. Desta forma, é possível concluir que nenhuma das instituições de ensino que responderam ao questionário têm um plano de continuidade de negócio, um plano de contigência e um plano de gestão de crise.

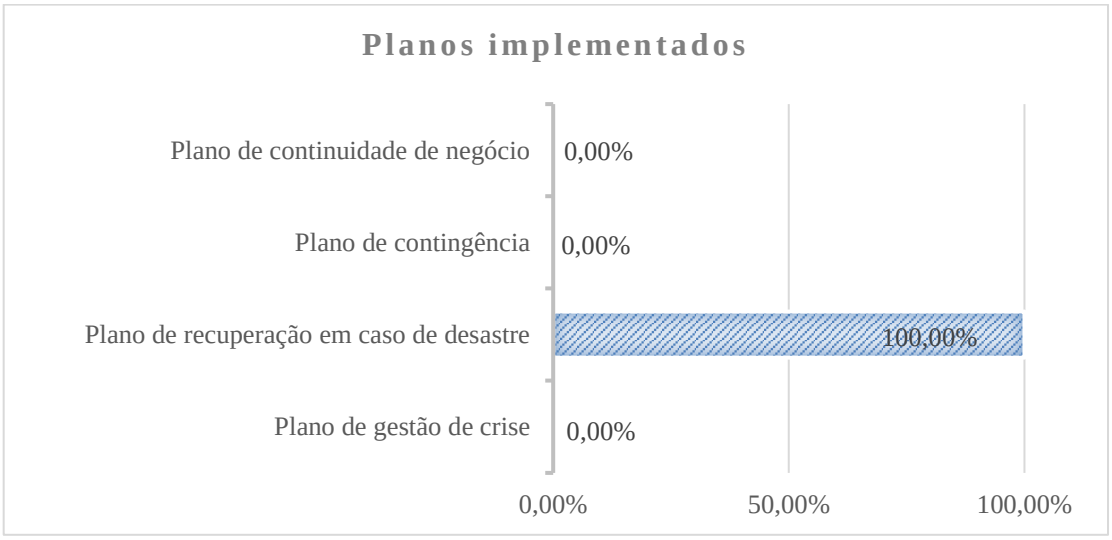


Figura 51 – Questão 25: Planos Implementados

Questão 26: São realizadas simulações com o plano de resposta a incidentes para verificar da sua eficácia, com que frequência?

A única instituição que tem um plano de resposta a incidentes, refere que nunca executou simulações ao seu plano, conforme é possível verificar na Figura 52.

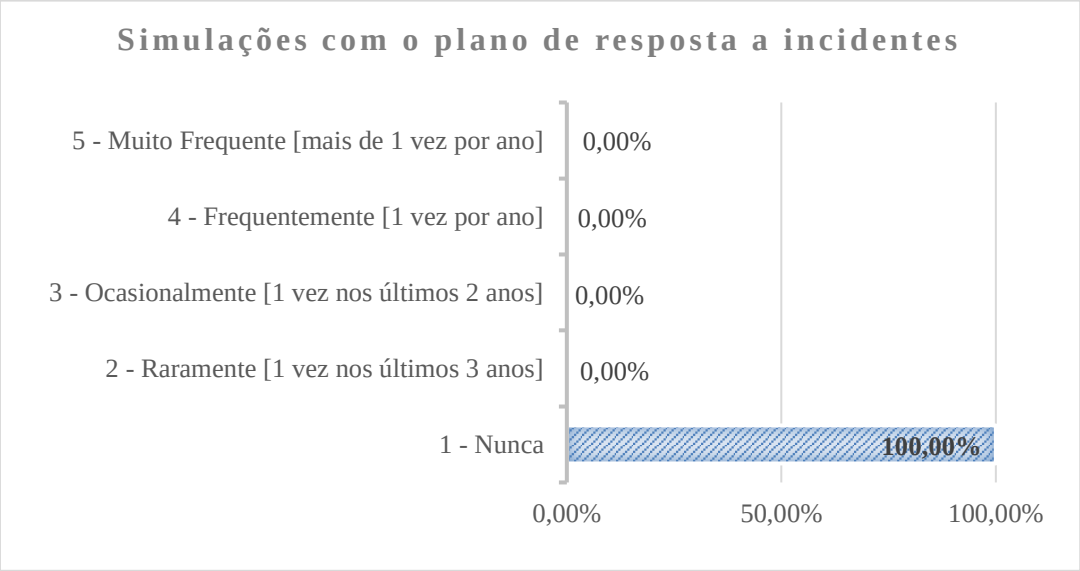


Figura 52 - Questão 26: Simulações ao Plano de Resposta a Incidentes

Questão 27: O AE/ENA, nos últimos 24 meses, sofreu algum incidente de segurança nos serviços TIC?

Apenas 11,76% das instituições de ensino inquiridas tiveram a indisponibilidade de serviços TIC, nos últimos 24 meses, devido a ataques provenientes do exterior, como: ataques *DDoS* [37], *ransomware* , entre outros. Constatou-se que todas as instituições de ensino inquiridas tiveram indisponibilidade de serviços TIC devido a falhas de hardware ou software nos últimos 24 meses, conforme é possível verificar na Figura 53.

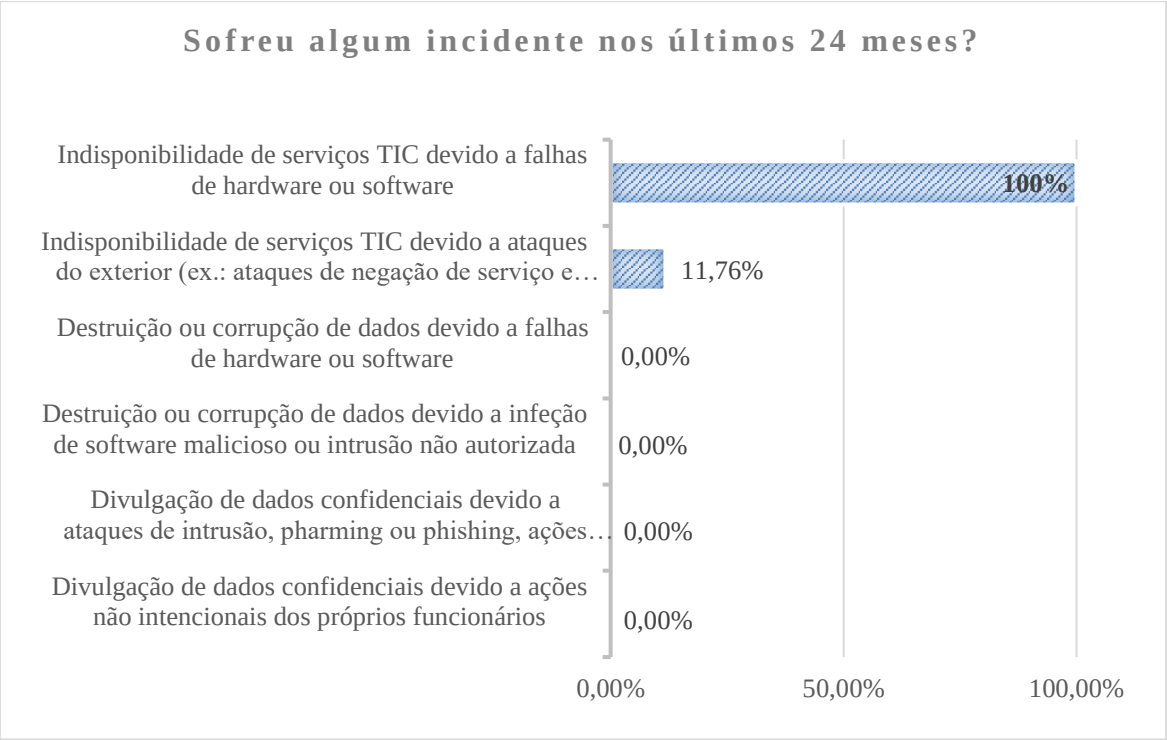


Figura 53 – Questão 27: Sofreu Algum Incidente nos Últimos 24 Meses

Questão 28: Realizaram a análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam?

A maioria das instituições de ensino (88,24%) inquiridas não realizou a análise dos riscos aos seus ativos para garantir a continuidade do funcionamento das redes, e dos sistemas de informação, conforme é possível verificar na Figura 54.

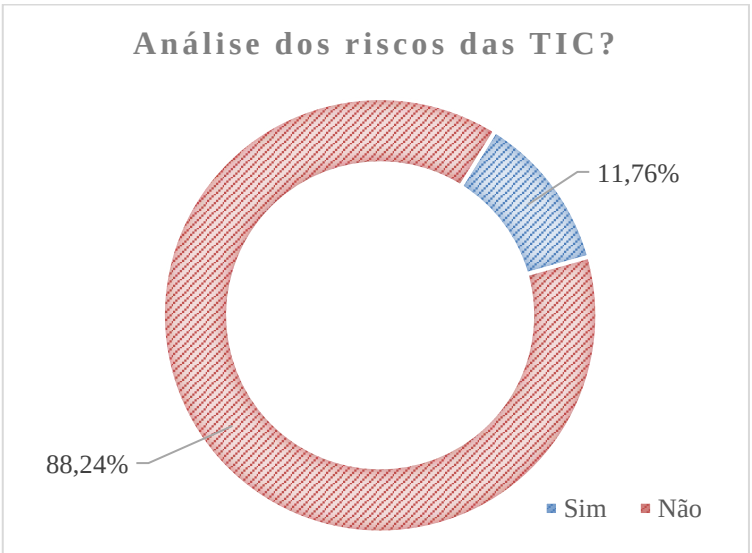


Figura 54 – Questão 28: Análise dos Riscos

Questão 29: Na sua opinião e numa escala de 1 a 5, o estabelecimento de ensino ao qual pertence está preparado para os desafios da cibersegurança?

A maioria dos inquiridos (76,47%) entende que a instituição de ensino à qual pertence tem algum nível de preparação, ou está preparada para os desafios da cibersegurança, conforme é possível verificar na Figura 55. No entanto, 23,53% dos inquiridos têm uma opinião contrária, ou seja, o estabelecimento de ensino ao qual pertence, está muito mal preparado para os desafios da cibersegurança.

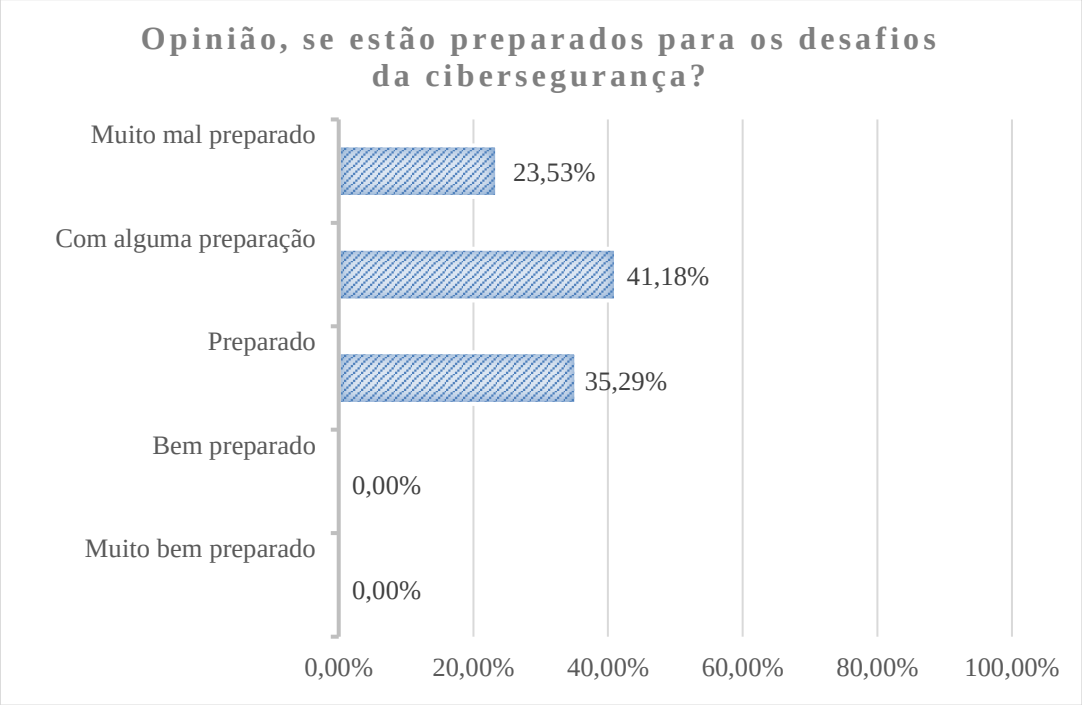


Figura 55 – Questão 29: Opinião sobre os Desafios da Cibersegurança

Concluída a apresentação e análise detalhada dos resultados obtidos com o questionário "Estado atual da cibersegurança nos AE/ENA da região de Leiria", a Figura 56 retrata a percentagem de entidades orgânicas que responderam "Sim" ou "Não", em cada umas das questões do tipo dicotómica, sendo que o "Sim" representa uma maior maturidade em termos de cibersegurança.

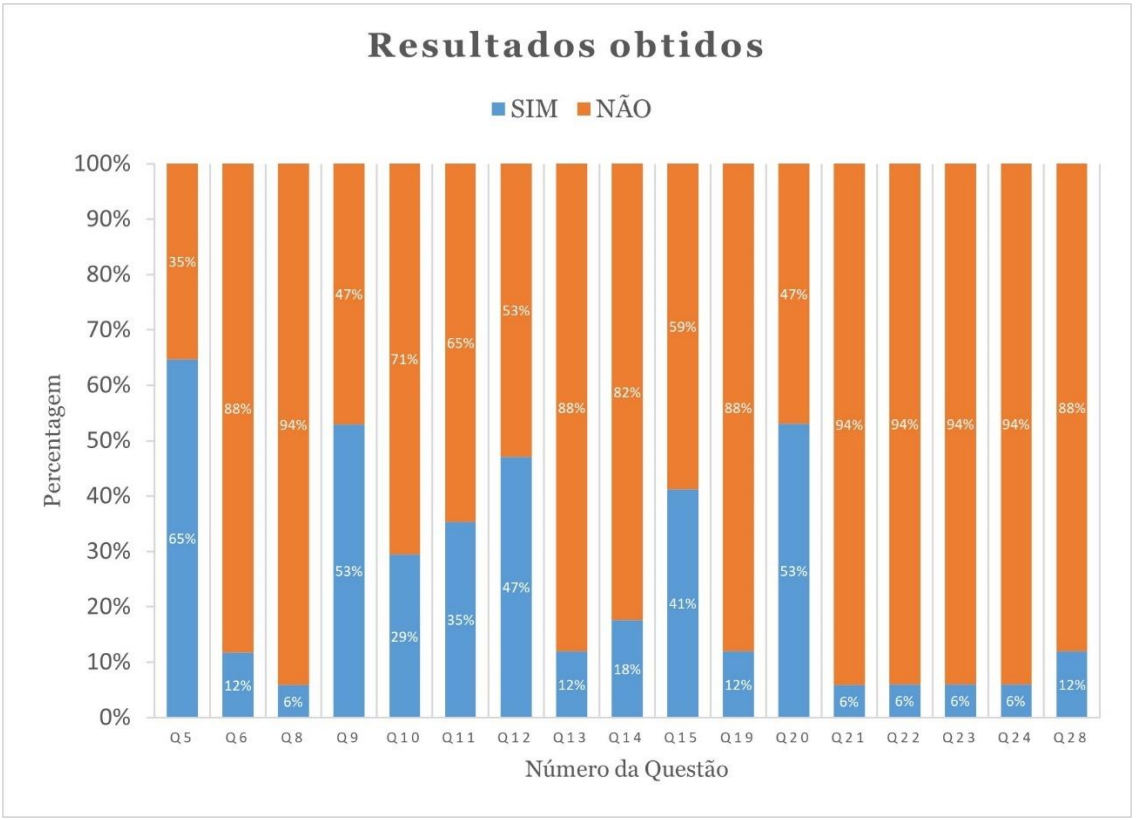


Figura 56 - Resultados Obtidos nas Questões Dicotómicas

Desta forma, comprova-se que há ainda um longo caminho a percorrer, nestas entidades, relativamente aos desafios inerentes à cibersegurança. Por esta razão, pretende-se a construção de um guia de cibersegurança, para auxiliar os responsáveis pelas Tecnologias de Informação e Comunicação (TIC) das instituições de ensino a melhorarem a sua presença no ciberespaço, o qual será abordado no capítulo seguinte.

4. Guia de Cibersegurança para as Escolas

Nesta secção descrevem-se os traços gerais de um guia de cibersegurança dedicado às instituições de ensino, com as recomendações sobre o tema, para auxiliar os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) de Portugal Continental a protegerem-se no ciberespaço.

O guia de cibersegurança proposto é direcionado a vários tipos de utilizadores das instituições de ensino, nomeadamente:

- Direção (Diretor(a), Sub-Diretor(a) ou Adjunto(a) Direção);
- Encarregado de Proteção de Dados;
- Responsável de Segurança;
- Coordenador(a) TIC;
- Técnico(a) Informática;
- Outros que assegurem a segurança da informação na instituição de ensino.

Para a construção do guia, optou-se por abordar conceitos tendo em conta as fragilidades sentidas na análise dos resultados obtidos com a aplicação do questionário, ao público-alvo do caso de estudo, e pretende-se segmentar a informação em cinco secções, conforme elucidado na Figura 57.

Figura 57 - Secções do Guia de Cibersegurança

Na primeira secção do guia, pretende-se abordar os temas gerais da cibersegurança e os principais aspetos que a constituem como, os tipos de ataques e, os seus impactos. A segunda

secção, tem como objetivo apresentar o estado atual da cibersegurança no setor da educação. Na terceira secção do guia, pretende-se explanar a legislação e regulamentos em vigor no âmbito da segurança da informação, bem como dar a conhecer as *frameworks* de cibersegurança mais populares. Na quarta secção, pretende-se elencar algumas das recomendações e boas práticas de cibersegurança que podem ser adotadas pelas instituições de ensino. Por fim, na quinta e última sessão do guia, serão apresentadas as conclusões sobre o tema.

4.1.Secção 1 – Cibersegurança, ameaças e impactos

Nesta primeira secção do guia, pretende-se de uma forma sucinta, responder às seguintes questões:

- O que é a cibersegurança?
- Quais os tipos de ataques e as suas consequências?

Este conteúdo pretende transmitir ao leitor um enquadramento global sobre o tema da cibersegurança.

4.2.Secção 2 – A cibersegurança na educação

Na segunda secção do guia, o objetivo é apresentar ao leitor informação relevante sobre o estado atual da cibersegurança no setor da educação. Um dos principais dados apresentados consiste na quantidade de tentativas de ataques ocorridos semanalmente no setor da educação/investigação, o que torna este setor um dos mais afetados a nível mundial, bem como a falta de estratégia de sensibilização para uma utilização segura e crítica da tecnologia, e dos ambientes digitais nas instituições de ensino [89]. Por fim, nesta secção pretende-se abordar todo o ecossistema de uma instituição de ensino cibersegura, desde os próprios utentes da instituição de ensino, até à tecnologia que sustenta toda a sua atividade.

4.3.Secção 3 – Legislação, regulamentos e normas

Na terceira secção do guia, pretende-se apresentar a legislação e regulamentos em vigor que as instituições se veem obrigadas a cumprir, bem como algumas das normas ou *frameworks* de cibersegurança que podem ser adotadas pelas instituições de ensino para melhorarem a sua presença no ciberespaço.

Legislação e regulamentos, em vigor, aplicável às entidades da Administração Pública:

- **Regulamento Europeu para a proteção de dados pessoais** [(UE) 2016/679] Estabelece as regras a nível europeu para proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, e à livre circulação desses dados [90].
- **Normas para a proteção e tratamento de dados pessoais** [Decreto-Lei 58/2019] Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016 [91], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [92].
- **Orientações técnicas de arquitetura de segurança para a proteção de dados pessoais** [RCM n.º 41/2018]
  Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes/sistemas de informação e procedimentos a adotar de modo a cumprir as normas do RGPD [93].
- **Regime jurídico da segurança do Ciberespaço, transpondo a Diretiva** [(UE) 2016/1148]
  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 [52].
- **Decreto-Lei n.º 65/2021, de 30 de julho**
  Regulamenta o Regime Jurídico da Segurança do Ciberespaço [51] e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.
- **Regulamento n.º 183/2022, de 21 de fevereiro**
  Regulamento que configura a instrução técnica relativa à comunicação e informação para cumprimento das obrigações decorrentes do Regime Jurídico da Segurança do Ciberespaço referentes, a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes [86].

Como normas de segurança, pretende-se apresentar apenas as mais comuns, nomeadamente:

- ISO/IEC 27001
- NIST *Cybersecurity Framework* (CSF)

- *Control Objectives for Information and Related Technologies* (COBIT*)*
- CIS *Controls Framework*
- Quadro Nacional de Referência para a Cibersegurança (QNRCS)

Cada instituição de ensino deverá avaliar as suas necessidades, recursos e cenários de ameaças específicos, e escolher a *framework* ou *frameworks* que mais se ajustam para garantir uma postura de segurança sólida e eficaz.

4.4.Secção 4 – Recomendações e boas práticas

Na quarta secção do guia apresentam-se um conjunto de recomendações e boas práticas que os decisores, e responsáveis pelas soluções TIC nas instituições de ensino, possam seguir para tornar todo o ecossistema mais robusto em relação à cibersegurança.

Após a recolha dos dados e análise dos resultados, optou-se por compilar um conjunto de recomendações e boas práticas para dar resposta às necessidades do público-alvo.

Na Tabela 14 é possível verificar o resumo do mapeamento realizado entre o questionário e as recomendações e boas práticas do guia de cibersegurança.

Questionário		Guia	
Id. Questão	**Resultado obtido**	**Id.**	**Título (Recomendação / Boa Prática)**
4	58,81% dos inquiridos não realizam campanhas de sensibilização	#1	Sensibilizar toda a comunidade escolar
5	35,29% dos inquiridos não estão a exigir aos utilizadores palavras-passe seguras	#3	Criar palavras-passe fortes
6	88,24% dos inqueridos não estão a exigir este método de autenticação aos utilizadores	#4	Ativar a autenticação multifator
8	94,12% dos inqueridos ainda utilizam sistemas operativos descontinuados	#8	Manter os sistemas atualizados
9	47,06% dos inqueridos não realizam cópias de segurança para três suportes diferentes	#6	A importância dos *backups*
10	70,59% dos inqueridos não cifram as cópias de segurança		
11	64,71% dos inqueridos não verificam as cópias de segurança		
12	52,94% dos inqueridos não dispõem de sistemas de monitorização e alarmística	#7	Implementar um sistema centralizado de monitorização de *logs*
13	88,24% dos inqueridos não realizou recentemente uma análise de vulnerabilidades	#9	Identificar e mitigar vulnerabilidades nos sistemas
14	82,35% dos inqueridos não realizou recentemente um teste de intrusão	#10	Realizar testes de intrusão (*pentest*)
15	58,82% dos inqueridos dizem não ter documentação sobre a segurança das TIC	#2	Redigir normativos sobre a cibersegurança
18	35,29% dos inqueridos recorrem a serviços externos	#11	Controlar adequadamente a segurança dos fornecedores
19	88,24% dos inqueridos não nomearam um responsável de segurança	#13	Nomear os responsáveis pela segurança da informação
20	47,06% dos inqueridos não dispõem do inventário dos ativos	#14	Criar e manter atualizado o inventário dos ativos
21	99,12% dos inqueridos não dispõem de um plano de cibersegurança	#15	Criar e executar um plano de resposta a ciberincidentes
24	94,12% dos inqueridos não têm um plano de resposta e de recuperação de ciberincidentes		

Tabela 14 - Mapeamento do Questionário com o Guia elaborado

De seguida, são apresentadas as questões do questionário onde se verificou uma maior fragilidade, por parte das instituições de ensino e, que devem ser mitigadas com as boas práticas de cibersegurança.

#1 Sensibilizar toda a comunidade Escolar		
Questionário	Questão 4	No AE/ENA realizam campanhas de sensibilização, junto da comunidade escolar, sobre o tema "Cibersegurança"?
	Resposta obtida	58,81% dos inquiridos não realizam campanhas de sensibilização junto da comunidade escolar com a periodicidade que seria desejável.
Guia	Sensibilizar a comunidade escolar (incluindo pais e encarregados de educação) para a adoção das boas práticas de cibersegurança, de modo a aumentar a resiliência da instituição de ensino relativamente às ameaças no ciberespaço. As questões de segurança digital são responsabilidade de todos e, para isso, é necessário sensibilizar toda a comunidade. Aos funcionários (docentes e não docentes) e colaboradores, deve ser ministrada formação mínima no domínio de práticas básicas de segurança da informação e comportamento defensivo.	

#2 Redigir normativos sobre a cibersegurança		
Questionário	Questão 15	O AE/ENA possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC?
	Resposta obtida	58,82% dos inqueridos dizem não ter documentação sobre a segurança das TIC.
Guia	Devem ser definidos normativos, com o objetivo de regular a cibersegurança e a segurança de informação. Estes documentos devem, no mínimo, contemplar os requisitos básicos de segurança da informação na instituição de ensino. Devem, igualmente, ser redigidos numa linguagem acessível, tendo em conta que todos os funcionários (docentes e não docentes) da instituição de ensino devem ter conhecimento dos mesmos.	

#3 Criar palavras-passe fortes		
Questionário	Questão 5	Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores Palavras-passe seguras?
	Resposta obtida	35,29% dos inquiridos não estão a exigir aos utilizadores palavras-passe seguras para acederem a dados confidenciais.
Guia	Quanto mais robusta for a palavra-passe, mais resistente se torna a ataques de força bruta. Crie palavra-passes com, pelo menos, 14 carateres e inclua uma combinação de letras maiúsculas e minúsculas, números e símbolos, se permitido.	

#4 Ativar a autenticação multifator		
Questionário	Questão 6	Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores Autenticação de Dois Fatores (2FA)?
	Resposta obtida	88,24% dos inqueridos não estão a exigir este método de autenticação aos utilizadores que têm acesso a informação confidencial.
Guia	A Autenticação MultiFator (MFA) é uma medida de segurança que protege o utilizador e a própria instituição de ensino, exigindo que os utilizadores forneçam, dois ou mais fatores de autenticação para aceder a informação confidencial que está alojada nas Tecnologias da Informação (TI), como aplicações, websites, e-mail, entre outros.	

#7 Implementar sistema centralizado de monitorização de *logs*		
Questionário	Questão 12	Dispõem de algum sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar os responsáveis sobre as mesmas?
	Resposta obtida	52,94% dos inqueridos não dispõem de sistemas de monitorização e alarmística para detetar atividades suspeitas nos próprios sistemas de TIC.
Guia	A monitorização de *logs* de sistema é de extrema importância na gestão da segurança de sistemas de informação. Os *logs* são registos detalhados de atividades que ocorrem em sistemas, redes, aplicações e dispositivos. Para uma visão centralizada dos *logs* é recomendado a utilização de uma plataforma de Gestão de Informações e Eventos de Segurança (SIEM).	

#6 A importância dos backups		
Questionário	Questão 9	As cópias de segurança cumprem a regra 3-2-1?
	Resposta obtida	47,06% dos inqueridos não realizam cópias de segurança para três suportes diferentes.
	Questão 10	As cópias de segurança que são enviadas para locais externos ao servidor são cifradas?
	Resposta obtida	70,59% das instituições de ensino não cifram as cópias de segurança que são enviadas para fora dos servidores.
	Questão 11	Todas as cópias de segurança dos sistemas em uso pelo AE/ENA são submetidas com regularidade a testes de integridade e recuperação?
	Resposta obtida	64,71% das instituições de ensino não realizam esta tarefa de verificação das cópias de segurança.
Guia	Para proteger os dados, por exemplo de ataques de *ransomware,* é importante criar e manter uma estratégia de cópias de segurança robusta. A regra 3-2-1 aumenta consideravelmente as possibilidades de recuperação de dados perdidos ou corrompidos. Para garantir a confidencialidade, só o utilizador com acesso à chave que foi utilizada para cifrar os dados terá acesso à informação protegida. As cópias de segurança devem ser submetidas periodicamente a testes de integridade e recuperação.	

#8 Manter os sistemas atualizados		
Questionário	Questão 8	No AE/ENA ainda temos equipamentos, em uso, com as seguintes versões do Windows: Windows Server 2003/2008/2012 e Windows XP/7/8/8.1.
	Resposta obtida	A maioria (94,12%) das instituições de ensino ainda têm sistemas operativos descontinuados em funcionamento.
Guia	Muitos incidentes de segurança ocorrem porque as atualizações de segurança, disponibilizadas pelo fornecedor do software, estão por instalar. Não é recomendado utilizar equipamentos com sistemas operativos descontinuados porque estes sistemas deixaram de ter atualizações de segurança para corrigir vulnerabilidades que, entretanto, foram identificadas.	

#9 Identificar e mitigar vulnerabilidades nos sistemas		
Questionário	Questão 13	Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a uma Análise de Vulnerabilidades?
	Resposta obtida	A maioria (88,24%) das instituições de ensino não realizou a análise de vulnerabilidades nos seus sistemas nos últimos dois anos.
Guia	As instituições de ensino devem assumir uma postura mais proativa no domínio da identificação, avaliação, priorização e mitigação de vulnerabilidades de software e sistema que podem ser exploradas por atacantes. O objetivo é reduzir o risco de um ciberataque bem-sucedido e manter a informação confidencial segura.	

#10 Realizar testes de intrusão (*pentest*)		
Questionário	Questão 14	Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a um Teste de Intrusão?
	Resposta obtida	A maioria (82,35%) das instituições de ensino não realizou um teste de intrusão nos seus sistemas nos últimos dois anos.
Guia	O teste de intrusão é um tipo de avaliação de segurança que envolve a simulação de um ataque cibernético a um sistema, rede ou aplicação web para identificar falhas e avaliar a segurança de um sistema, além de medir a maturidade de segurança da instituição de ensino.	

#11 Controlar adequadamente a segurança dos fornecedores		
Questionário	Questão 18	Quem realiza as atividades relacionadas com a segurança das TIC da instituição de ensino?
	Resposta obtida	35,29% das instituições de ensino recorrem a serviços externos para assegurar as atividades relacionadas com a segurança das TIC.
Guia	É comum as instituições de ensino recorrerem à subcontratação de serviços de manutenção para os seus sistemas informáticos, pelo que é necessário tomar providências, em sede contratual, junto dos seus fornecedores de Tecnologias de Informação (TI).	

#13 Nomear os responsáveis pela segurança da informação		
Questionário	Questão 19	Designou um responsável de segurança junto do CNCS (Centro Nacional de Cibersegurança)?
	Resposta obtida	88,24% das instituições de ensino não nomearam um responsável de segurança e fizeram a respetiva comunicação ao Centro Nacional de Cibersegurança (CNCS).
Guia	De acordo com a legislação em vigor, as instituições de ensino devem nomear pelo menos um responsável pela segurança da informação e, cabe a este adotar as medidas técnicas e organizacionais.	

#14 Criar e manter atualizado o inventário dos ativos		
Questionário	Questão 20	Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços?
	Resposta obtida	47,06% das instituições de ensino não dispõem do inventário dos ativos.
Guia	De acordo com a legislação em vigor, as instituições de ensino devem criar e manter o inventário de ativos (equipamentos e aplicações) atualizado e este deve ser comunicado ao Centro Nacional de Cibersegurança (CNCS).	

#15 Criar e executar um plano de resposta a ciberincidentes		
Questionário	Questão 21	Elaborou e mantém atualizado o plano de (ciber) segurança, devidamente documentado e assinado pelo responsável de segurança?
	Resposta obtida	94,12% das instituições de ensino não dispõem de um plano de cibersegurança.
	Questão 24	No AE/ENA existe um plano de resposta e de recuperação de incidentes?
	Resposta obtida	94,12% não têm um plano de resposta e de recuperação de ciberincidentes.

Guia	Os responsáveis pela instituição de ensino precisam de saber como responder a incidentes de segurança, e como recuperar caso ocorram eventos adversos. O Plano de Resposta a Incidentes (PRI) deve definir o que a instituição de ensino terá de realizar antes, durante e depois de um incidente de segurança. Este plano deve também incluir quais as funções e responsabilidades dos envolvidos para responder a um incidente.

Para além das questões acima referenciadas, para as quais as instituições de ensino inquiridas mostraram maior nível de fragilidade, optou-se por incluir também mais cinco recomendações e boas práticas tendo em consideração a última questão do questionário: "*Na sua opinião e numa escala de 1 a 5, o Estabelecimento de Ensino ao qual pertence está preparado para os desafios da cibersegurança?"*, onde foi obtida uma classificação média de 2,12, numa escala de 1 a 5.

Outras recomendações e boas práticas consideradas no guia

- **#5 Utilizar um gestor de palavras-passe**

  Um gestor de palavras-passe é uma forma conveniente e segura de proteger as credenciais de acesso. Existem vários gestores de palavras-passe gratuitos, de qualidade e intuitivos de utilizar, como por exemplo: *KeePass*[11],*KeePassXC*[12], *LastPass*[13], *NordPass*[14], *Bitwarden*[15], entre outros. O gestor permite criar palavras-passe fortes e mantêm-nas em segurança.

- **#12 Controlo de acessos aos sistemas informáticos**

  O reforço das medidas de controlo de acesso aos sistemas de informação é assim urgente e devem ter em conta tanto os utilizadores internos (docentes e não docentes) como os externos (técnicos de informática, fornecedores, entre outros), bem como os utilizadores da instituição de ensino com privilégios máximos, nomeadamente os elementos da direção.

[11] https://keepass.info/
[12] https://keepassxc.org/
[13] https://www.lastpass.com/pt
[14] https://nordpass.com/
[15] https://bitwarden.com/

- **#16 Criar e executar um plano de auditorias à segurança**
  As instituições de ensino devem estabelecer um plano de auditorias à segurança dos sistemas considerados mais críticos para avaliar se os processos, princípios e políticas de cibersegurança estão a ser respeitados. Existem diversas *frameworks* de Cibersegurança que podem auxiliar neste processo.
- **#17 Proteger toda a infraestrutura tecnológica**
  Adotar medidas proativas pode ajudar a proteger adequadamente a infraestrutura tecnológica (equipamentos e sistemas), nomeadamente: Controlo do acesso à/da Internet; Configurações e acessos por omissão; Proteção dos equipamentos terminais; Sistemas descontinuados; Definição de uma política *Bring Your Own Device* (BYOD) [94].
- **#18 Proteger os domínios (*registrars*)**
  Implementar os principais *standards* de segurança nas vertentes web e e-mail para melhorar a presença da instituição de ensino no ciberespaço, nomeadamente: *Sender Policy Framework* (SPF) [95], o *DomaimKeys Identified Mail* (DKIM) [96] e o *Domain-based Message Authentication, Reporting and Conformance* (DMARC) [97].

Por último, ainda nesta secção 4, incluiu-se o procedimento e os contactos que as instituições de ensino devem utilizar para reportar um incidente ou um cibercrime.

4.5. Secção 5 – Conclusões

Na quinta e última secção do guia apresentam-se as conclusões ao documento "Guia de Boas Práticas para as Escolas". Recomenda-se assim a leitura do guia de cibersegurança, resultante deste trabalho, de forma a obter uma visão geral dos contributos alcançados pelo mesmo.

4.6. Disponibilização do guia de cibersegurança

Concluída a versão final do guia de cibersegurança - **Anexo G**, optou-se por disponibilizar publicamente o ficheiro em formato digital (PDF) num repositório do GitHub[16] para que o mesmo ficasse acessível ao público em geral, conforme é possível verificar na Figura 58.

[16] https://github.com/filbag/Ciberseguranca--Guia-de-Boas-Praticas.git

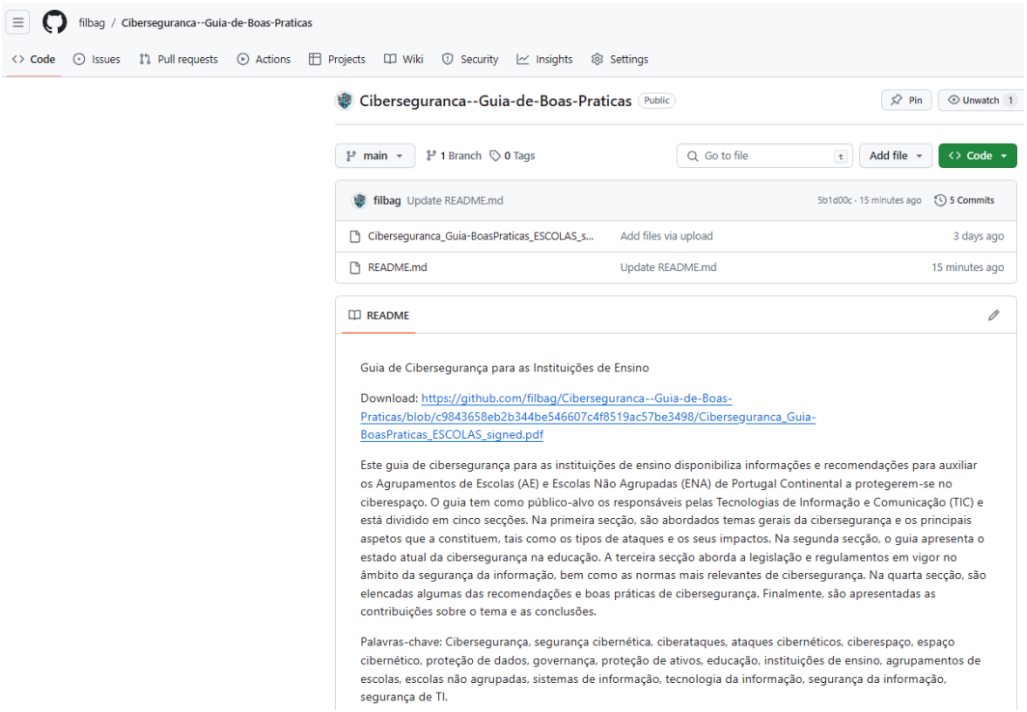


Figura 58 - Repositório do GitHub

Reforça-se que as instituições de ensino que colaboraram, com o preenchimento do questionário, receberam via e-mail, em forma de agradecimento pelo imprescindível contributo que deram ao presente trabalho. Nesta mesma comunicação, foi divulgado o guia de cibersegurança para que estas possam melhorar a sua presença no ciberespaço. No **Anexo F** é possível verificar o e-mail que foi enviado às instituições de ensino, neste contexto.

5. Conclusões

Neste capítulo apresentam-se as conclusões e uma reflexão sobre o trabalho realizado, assim como algumas ideias para trabalho futuro.

5.1. Conclusões gerais

A segurança das Tecnologias da Informação (TI) na educação é uma realidade que nos rodeia já há algum tempo e que teve um incremento considerável com o contexto criado pela pandemia Covid-19. Não só pela quantidade de sistemas digitais disponíveis no meio, mas também pelo interesse de toda a comunidade escolar em utilizar a tecnologia a partir de qualquer lugar, privilegiando a qualidade, a acessibilidade e a simplicidade do acesso à informação.

Contudo, esta transformação digital impõe alguns desafios aos utilizadores e aos responsáveis pelas Tecnologias de Informação e Comunicação (TIC) na instituição de ensino, porque está a atrair cada vez mais cibercriminosos.

A cibersegurança, é efetivamente um tema que preocupa cada vez mais os responsáveis pelas instituições de ensino em todo o mundo, uma vez que estas armazenam informação confidencial valiosa, e os estudos recentes confirmam isso mesmo, ou seja, que o setor do ensino/investigação está no topo dos mais visados. Contudo, as instituições públicas de ensino têm uma grande dependência financeira do Estado, porque um dos pilares da cibersegurança é efetivamente a tecnologia, e quando os recursos tecnológicos são escassos, ou já se encontram descontinuados, torna-se mais difícil proteger todo o ecossistema destas instituições. Porém, com as limitações já identificadas, cabe às instituições encontrar outras soluções para mitigar ou reduzir o risco de um ciberataque bem-sucedido e manter a informação confidencial o mais segura possível.

Considerando que em Portugal Continental, existem mais de 8.190 estabelecimentos de ensino (privado e público) do pré-escolar ao secundário, onde o total de alunos inscritos/matriculados corresponde a 1.586.453, 150.649 docentes e 77.032 não docentes [9]. Num setor cada vez mais digitalizado e dependente dos sistemas de comunicação altamente informatizados, é fundamental avaliar a maturidade para as matérias da cibersegurança e a capacidade de mitigação do cibercrime nestas instituições de ensino.

O foco do estudo empírico do presente trabalho incidiu sobre as instituições de ensino da região de Leiria, considerando a dificuldade técnica de aplicar esta investigação a todas as instituições de ensino a nível nacional, nomeadamente o tempo necessário para a realização do projeto dessa envergadura demorará consideravelmente mais que um ano, e não era viável realizá-lo nos prazos determinados para a elaboração deste projeto.

É neste âmbito que foram traçados os seus principais objetivos, tendo o caso de estudo como estratégia de investigação para os alcançar:

- Estudar e analisar o estado da arte da cibersegurança, nomeadamente a legislação em vigor, os *standards* existentes e as boas práticas de segurança digital;
- Avaliar o estado atual de cibersegurança, através de dados obtidos por meio de um questionário, nas instituições de ensino da região de Leiria;
- Elaborar um guia de cibersegurança que permitisse ajudar os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) a melhorar a sua presença no ciberespaço.

Alcançados os objetivos supramencionados, reuniam-se as condições para responder à questão: "*Qual é o estado atual nos Agrupamentos de Escolas e Escolas Não Agrupadas da Região de Leiria?*".

O público-alvo do caso de estudo correspondeu a 23 entidades orgânicas da região de Leiria, embora só tenham sido obtidas 17 respostas, num universo de 23, sendo que a taxa de resposta ao questionário foi positiva (73,91%).

Os resultados obtidos com o questionário revelam que ainda existe um caminho longo a percorrer em matéria de cibersegurança, nomeadamente:

- 94,12% das instituições de ensino não estão em conformidade com a legislação, normas e regulamentos em vigor no âmbito da segurança da informação;
- 94,12% das instituições de ensino ainda integram sistemas operativos descontinuados em funcionamento;
- 94,12% das instituições de ensino não dispõem de um plano de cibersegurança;
- 94,12% das instituições de ensino não comunicaram ao CNCS o ponto de contacto permanente, o responsável de segurança, a lista de ativos e o seu relatório anual;
- 88,24% das instituições de ensino não exigem aos utilizadores com acesso a informação confidencial a autenticação de multifator;

- 58,81% das instituições de ensino assumem não realizar campanhas de sensibilização, junto da comunidade escolar, sobre o tema cibersegurança, pelo menos uma vez por ano;
- 64,71% dos responsáveis pelas TIC, reconhecem de uma forma geral que a instituição de ensino à qual pertence, não está bem preparada para os desafios da cibersegurança.

Concluída a recolha e análise dos dados obtidos no questionário, foi desenvolvido o guia de cibersegurança dedicado às instituições de ensino contendo este informações e recomendações para auxiliar os AE e ENA de Portugal Continental a protegerem-se no ciberespaço. Este guia destina-se aos responsáveis pelas Tecnologias de Informação e Comunicação das instituições de ensino e tem como principal foco, dar a conhecer:

- temas gerais da cibersegurança e os principais aspetos que a constituem, tais como os tipos de ataques e os seus impactos;
- o estado atual da cibersegurança na educação;
- a legislação e regulamentos em vigor no âmbito da segurança da informação, bem como as normas mais relevantes de cibersegurança;
- algumas das recomendações e boas práticas de cibersegurança.

Sendo que a adoção de recomendações e boas práticas de cibersegurança, pode reduzir o risco e os custos associados a violações de dados ou intrusões, e que na maioria das instituições de ensino (88,24%), as tarefas relacionadas com a segurança dos sistemas são realizadas por pessoal do próprio AE/ENA, é essencial aumentar o nível de literacia em cibersegurança de todos os utilizadores em geral, com maior incidência nos funcionários (docentes e não docentes) e nos responsáveis pelas TIC, para elevar o grau de consciencialização para a cibersegurança. Uma boa estratégia para o sucesso são os próprios utilizadores da comunidade escolar sentirem que são parte da solução e que têm um papel não só ativo, como também determinante neste processo. Independentemente do investimento que as instituições de ensino venham a fazer em ferramentas tecnológicas de cibersegurança, os utilizadores continuam a ser uma peça fundamental na segurança da informação.

Como reflexão final considero que os objetivos a que me propus, no início deste projeto, foram atingidos, tendo contribuído academicamente para a segurança dos sistemas de Tecnologias de Informação e Comunicação (TIC) das instituições de ensino.

5.2. Trabalho futuro

Com base no trabalho desenvolvido, surgiram novas sugestões e orientações que poderão ser desenvolvidas em termos de trabalhos futuros. Em alguns casos, o trabalho futuro poderá servir como modelo comparativo com o presente estudo.

Sugere-se a elaboração de um estudo semelhante às mesmas instituições de ensino, num outro momento temporal de modo a permitir comparar os resultados, para aferir se existem melhorias entre os diferentes períodos temporais.

Considera-se pertinente efetuar o mesmo tipo de estudo a todas as instituições públicas de ensino de Portugal, de modo a obter o estado atual da cibersegurança a nível nacional e compreender as discrepâncias entre os diferentes concelhos/distritos.

Outro trabalho relevante a realizar é a aplicação de uma *framework* de cibersegurança, como ISO27001, NIST *Cybersecurity Framework 2.0* ou até mesmo o Quadro Nacional de Referência para a Cibersegurança (QNRCS) a uma instituição de ensino.

Por último, deverá equacionar-se a aplicação da mesma metodologia, contexto e abordagem noutros casos de estudo, como estabelecimentos de ensino particular e cooperativo, como por exemplo: Colégios, Externatos, Institutos, Conservatórios, entre outras instituições de ensino de nível não superior.

5.3. Considerações finais

Este caso de estudo revelou-se numa mais-valia para mim, tanto a nível pessoal, como a nível profissional, pois possibilitou-me uma visão mais abrangente sobre o conceito de Cibersegurança, a sua importância e aplicabilidade no contexto institucional.

É de realçar que com a realização do caso estudo, foi possível colocar em prática os conhecimentos adquiridos ao longo do Mestrado de Cibersegurança e Informática Forense, no contexto de trabalho de pesquisa, preparação, execução e análise de dados, como também, me proporcionou um enriquecimento desses conhecimentos.

Como complemento ao presente estudo, foi submetido um artigo científico, intitulado de "Análise da Cibersegurança em Instituições de Ensino da região de Leiria, em Portugal" na Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI), estando o mesmo em processo de revisão.

Bibliografia

[1] C. R. Junior, I. Becker, e S. Johnson, «Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity». arXiv, 29 de setembro de 2023. Disponível em: http://arxiv.org/abs/2309.17186. [Acedido: 31 de janeiro de 2024]

[2] D. Kim e M. Solomon, *Fundamentals of information systems security*, Fourth edition. Burlington, Massachusetts: Jones & Bartlett Learning, 2023.

[3] CNCS, «CNCS - Boletim de maio, nº 2/2020», maio de 2020. Disponível em: https://www.cncs.gov.pt/en/boletim-may-2020/#qNumber. [Acedido: 31 de março de 2024]

[4] Check Point, «Check Point's 2023 Mid-Year Cyber Security Report», *Check Point's 2023 Mid-Year Cyber Security Report*. Disponível em: https://go.checkpoint.com/2023-mid-year-security-report/. [Acedido: 31 de janeiro de 2024]

[5] European Union Agency for Cybersecurity., *ENISA threat landscape 2023: July 2022 to June 2023*. LU: Publications Office, 2023. Disponível em: https://data.europa.eu/doi/10.2824/782573. [Acedido: 31 de janeiro de 2024]

[6] «Using the CIA and AAA Models to Explain Cybersecurity Activities». Disponível em: https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf. [Acedido: 31 de março de 2024]

[7] DGEEC, «Direção-Geral de Estatísticas da Educação e Ciência - DGEEC», *Sumários estatísticos*. Disponível em: https://www.dgeec.medu.pt/art/64ad21f98e5ca5b1c8676271/64ad2e478e5ca5b1c8676284/65413240fa6563985a785832/65438e5fdc5370e4ed6816b5. [Acedido: 31 de janeiro de 2024]

[8] Metared, «O que é MetaRed», *O que é a MetaRed Portugal?* Disponível em: https://www.metared.org/pt/que-e-metared.html. [Acedido: 31 de janeiro de 2024]

[9] DGEEC, «DGEEC - Educacao Em Numeros 2023.pdf». Disponível em: https://pessoas2030.gov.pt/wp-content/uploads/sites/19/2023/08/EducacaoEmNumeros_2023.pdf. [Acedido: 31 de janeiro de 2024]

[10] Assembleia da República, «Lei n.º 46/86, de 14 de Outubro», *LEI DE BASES DO SISTEMA EDUCATIVO*, 14 de outubro de 1986. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1744&tabela=leis&so_miolo=. [Acedido: 31 de janeiro de 2024]

[11] Ministério da Ciência, Inovação e Ensino Superior, «Decreto-Lei n.º 42/2005, de 22 de fevereiro», *Decreto-Lei n.º 42/2005, de 22 de fevereiro*, 22 de fevereiro de 2005. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/42-2005-606304. [Acedido: 31 de janeiro de 2024]

[12] DGEEC, «DGEEC - Educacao E Formacao Em Portugal_2021.pdf». Disponível em: https://www.dgeec.medu.pt/api/ficheiros/6595938c74d2e1f2f79ecc63. [Acedido: 31 de janeiro de 2024]

[13] DGEEC, «75 Anos Estatísticas Educação Portugal», *75 Anos Estatísticas Educação Portugal*, 1 de julho de 2023. Disponível em: https://info.dgeec.medu.pt/75anos-estatisticas-educacao-portugal/8/. [Acedido: 31 de janeiro de 2024]

[14] Direção Geral de Estatísticas da Educação e Ciência (DGEEC), Direção de Serviços de Estatísticas da Educação (DSEE), e Divisão de Estatísticas dos Ensinos Básico e Secundário (DEEBS), «Recursos Tecnológicos das escolas 2021/2022», p. 29, jul. 2024, Disponível em: http://www.dgeec.mec.pt. [Acedido: 20 de novembro de 2023]

[15] Portugal Digital, «Conhecer a Escola Digital», *Portugal Digital*, 21 de junho de 2022. Disponível em: https://portugaldigital.gov.pt/formar-pessoas-para-o-digital/conhecer-a-escola-digital/. [Acedido: 31 de janeiro de 2024]

[16] DGEEC, «Projeto RAE - Rede Alargada da Educação», *Rede Alargada da Educação*. Disponível em: https://projetorae.dgeec.mec.pt/. [Acedido: 31 de janeiro de 2024]

[17] FCCN, «Rede alargada de educação aumenta capacidade», *Rede alargada de educação aumenta capacidade*, 14 de maio de 2019. Disponível em: https://www.fccn.pt/noticias/rede-alargada-de-educacao-aumenta-capacidade/. [Acedido: 31 de janeiro de 2024]

[18] DGEEC, «Direção-Geral de Estatísticas da Educação e Ciência - preservada pelo Arquivo.pt», *Procedimentos de Segurança*, 13 de novembro de 2014. Disponível em: https://arquivo.pt/wayback/20211021052043/https://www.dgeec.mec.pt:80/np4/psegdigital/. [Acedido: 31 de janeiro de 2024]

[19] Seguranet, «Selo de Segurança Digital (eSafety Label) | SeguraNet», *Selo de Segurança Digital (eSafety Label)*, 17 de janeiro de 2024. Disponível em: https://www.seguranet.pt/esafetylabel. [Acedido: 24 de março de 2024]

[20] Assembleia da República, «Lei n.º 50/2018, de 16 de agosto», *Lei n.º 50/2018, de 16 de agosto*, 16 de agosto de 2018. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/50-2018-116068877. [Acedido: 20 de março de 2024]

[21] CCDR Norte, «Transferência de competências para as autarquias locais e entidades intermunicipais», *Transferência de competências para as autarquias locais e entidades intermunicipais*. Disponível em: https://www.ccdr-n.pt/pagina/servicos/administracao-local/transferencia-de-competencias. [Acedido: 31 de janeiro de 2024]

[22] Assembleia da República, «Transferência de competências para os órgãos municipais e para as entidades intermunicipais no domínio da educação - Artigo 12.º | DR», *Decreto-Lei n.º 21/2019*, 30 de janeiro de 2019. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2019-118872841-118872954. [Acedido: 20 de março de 2024]

[23] Assembleia da República, «Diário da República n.º 251/2018, Série I de 2018-12-31», *Diário da República n.º 251/2018, Série I de 2018-12-31*, 31 de dezembro de 2018. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/71-2018-117537583. [Acedido: 20 de março de 2024]

[24] Clara Guerra, «*Proteção de dados em contexto escolar | Clara Guerra*», (24 de outubro de 2014). Disponível em: https://www.youtube.com/watch?v=XuiTCDemoSg. [Acedido: 31 de janeiro de 2024]

[25] Presidência do Conselho de Ministros, «Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho», *Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho*, 5 de junho de 2019. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962. [Acedido: 31 de janeiro de 2024]

[26] NIST, «information security - Glossary | CSRC», *information security*, NT. Disponível em: https://csrc.nist.gov/glossary/term/information_security. [Acedido: 31 de janeiro de 2024]

[27] CISCO, «What Is a Cyberattack?», *Cisco*. Disponível em: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. [Acedido: 31 de janeiro de 2024]

[28] H. Ahmetoglu e R. Das, «A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions», *Internet Things*, vol. 20, p. 100615, nov. 2022, doi: 10.1016/j.iot.2022.100615. Disponível em: https://www.sciencedirect.com/science/article/pii/S254266052200097X. [Acedido: 31 de janeiro de 2024]

[29] E. Gandotra, D. Bansal, e S. Sofat, «Malware Analysis and Classification: A Survey», *J. Inf. Secur.*, vol. 05, n.º 02, pp. 56–64, 2014, doi: 10.4236/jis.2014.52006. Disponível em: http://www.scirp.org/journal/doi.aspx?DOI=10.4236/jis.2014.52006. [Acedido: 31 de janeiro de 2024]

[30] Kaspersky, «What is a Trojan Horse Virus? Types and How to Remove it», *www.kaspersky.com*, 12 de março de 2024. Disponível em: https://www.kaspersky.com/resource-center/threats/trojans. [Acedido: 24 de março de 2024]

[31] Mário Antunes e Baltazar Rodrigues, *Introdução à Cibersegurança*, 2.ª ed., vol. 1, 1 vols. em 2, no. 2, vol. 1. FCA. Disponível em: https://www.almedina.net/introdu-o-ciberseguran-a-a-internet-os-aspetos-legais-e-a-an-lise-digital-forense-1668440717.html

[32] Kaspersky, «What is Cryptocurrency and how does it work?», *What is Cryptocurrency and how does it work?*, 27 de fevereiro de 2024. Disponível em: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency. [Acedido: 24 de março de 2024]

[33] Z. Alkhalil, C. Hewage, L. Nawaf, e I. Khan, «Phishing Attacks: A Recent Comprehensive Study and a New Anatomy», *Front. Comput. Sci.*, vol. 3, 2021, Disponível em: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060. [Acedido: 31 de janeiro de 2024]

[34] Cloudflare, «What is a phishing attack?», *What is a phishing attack?* Disponível em: https://www.cloudflare.com/learning/access-management/phishing-attack/. [Acedido: 31 de janeiro de 2024]

[35] Veracode, «Man in the Middle (MITM) Attack», *Veracode*. Disponível em: https://www.veracode.com/security/man-middle-attack. [Acedido: 31 de janeiro de 2024]

[36] A. B. de Neira, B. Kantarci, e M. Nogueira, «Distributed denial of service attack prediction: Challenges, open issues and opportunities», *Comput. Netw.*, vol. 222, p. 109553, fev. 2023, doi: 10.1016/j.comnet.2022.109553. Disponível em: https://www.sciencedirect.com/science/article/pii/S1389128622005874. [Acedido: 31 de janeiro de 2024]

[37] Cloudflare, «What is a DDoS attack?», *What is a DDoS attack?* Disponível em: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Acedido: 31 de janeiro de 2024]

[38] V. Abdullayev e Dr. A. S. Chauhan, «SQL Injection Attack: Quick View», *Mesopotamian J. Cyber Secur.*, pp. 30–34, fev. 2023, doi: 10.58496/MJCS/2023/006. Disponível em: https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/50. [Acedido: 31 de janeiro de 2024]

[39] PortSwigger, «What is SQL Injection?», *What is SQL Injection?* Disponível em: https://portswigger.net/web-security/sql-injection. [Acedido: 31 de janeiro de 2024]

[40] R. Ahmad, I. Alsmadi, W. Alhamdani, e L. Tawalbeh, «Zero-day attack detection: a systematic literature review», *Artif. Intell. Rev.*, vol. 56, n.º 10, pp. 10733–10811, out. 2023, doi: 10.1007/s10462-023-10437-z. Disponível em: https://link.springer.com/10.1007/s10462-023-10437-z. [Acedido: 14 de janeiro de 2024]

[41] H. M. Reddy e N. Subramanian, «DNS tunnelling attack and detection», apresentado na CHEMISTRY BEYOND BORDERS: INTERNATIONAL CONFERENCE ON PHYSICAL CHEMISTRY: The 1st Annual Meeting of the Physical Chemistry Division of the Indonesian Chemical Society, Malang, Indonesia, 2023, p. 020021. doi: 10.1063/5.0166736. Disponível em: http://aip.scitation.org/doi/abs/10.1063/5.0166736. [Acedido: 15 de janeiro de 2024]

[42] Infoblox, «What is DNS Tunneling?», *What is DNS Tunneling?* Disponível em: https://www.infoblox.com/glossary/dns-tunneling/. [Acedido: 31 de janeiro de 2024]

[43] CNCS, «CNCS - Relatorio Politicas Publicas 2021 - observatorio ciberseguranca.pdf». Disponível em: https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs.pdf. [Acedido: 31 de janeiro de 2024]

[44] Assembleia da República, «Lei n.º 27/2021», *Lei n.º 27/2021*, 17 de maio de 2021. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244. [Acedido: 30 de março de 2024]

[45] Parlamento Europeu e do Conselho, *Regulamento (UE) 2019/881*, vol. 151. 2019. Disponível em: http://data.europa.eu/eli/reg/2019/881/oj/por. [Acedido: 1 de abril de 2024]

[46] ENISA, «Sobre a ENISA — Agência da União Europeia para a Cibersegurança», *ENISA*, 2004. Disponível em: https://www.enisa.europa.eu/about-enisa/about/pt. [Acedido: 1 de abril de 2024]

[47] Resolução do Conselho de Ministros, «DL n.º 69/2014, de 09 de Maio», *DL n.º 69/2014, de 09 de Maio*, 9 de maio de 2014. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=2100&pagina=1&ficha=1. [Acedido: 2 de abril de 2024]

[48] Presidência e da Modernização Administrativa, «DL n.º 136/2017, de 06 de Novembro», *DL n.º 136/2017, de 06 de Novembro*, 6 de novembro de 2017. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=selected&nid=2803&tabela=leis&pagina=1&ficha=1&nversao=. [Acedido: 2 de abril de 2024]

[49] PORTUGAL GOV, «Relatório Anual de Segurança Interna 2022», *Relatório Anual de Segurança Interna 2022*, 31 de março de 2023. Disponível em: https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2022-. [Acedido: 21 de março de 2024]

[50] Parlamento Europeu, «Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016», *Jornal Oficial da União Europeia, L 194, 19 de julho de 2016*, 19 de julho de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL%3A2016%3A194%3ATOC. [Acedido: 31 de janeiro de 2024]

[51] Presidência do Conselho de Ministros, «Decreto-Lei n.º 65/2021, de 30 de julho», *Decreto-Lei n.º 65/2021, de 30 de julho*, 30 de julho de 2021. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988. [Acedido: 31 de janeiro de 2024]

[52] Assembleia da República, «Lei n.º 46/2018, de 13 de agosto», *Lei n.º 46/2018, de 13 de agosto*, 13 de agosto de 2018. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384. [Acedido: 31 de janeiro de 2024]

[53] CNCS, «Quadro Nacional de Referência para a Cibersegurança (QNRCS)», *Quadro Nacional de Referência para a Cibersegurança (QNRCS)*. Disponível em: https://www.cncs.gov.pt/pt/quadro-nacional/. [Acedido: 21 de março de 2024]

[54] CNCS, «CNCS - Roteiro Capacidades Minimas Ciberseguranca.pdf». Disponível em: https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf. [Acedido: 1 de fevereiro de 2024]

[55] ISO, «ISO/IEC 27001:2022», *ISO/IEC 27001:2022*, 2022. Disponível em: https://www.iso.org/standard/27001. [Acedido: 1 de fevereiro de 2024]

[56] NIST, «The NIST Cybersecurity Framework (CSF) 2.0», National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, fev. 2024. doi: 10.6028/NIST.CSWP.29. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Acedido: 11 de março de 2024]

[57] COBIT, «COBIT | Control Objectives for Information Technologies», *COBIT An ISACA Framework*, 2019. Disponível em: https://www.isaca.org/resources/cobit. [Acedido: 1 de fevereiro de 2024]

[58] CIS, «CIS Critical Security Controls Version 7», *CIS Critical Security Controls Version 7*, 19 de março de 2018. Disponível em: https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/. [Acedido: 1 de fevereiro de 2024]

[59] H. Taherdoost, «Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview», *Electronics*, vol. 11, n.º 14, p. 2181, jul. 2022, doi: 10.3390/electronics11142181. Disponível em: https://www.mdpi.com/2079-9292/11/14/2181. [Acedido: 1 de fevereiro de 2024]

[60] NIST, «Cybersecurity Framework», *NIST*, nov. 2013, Disponível em: https://www.nist.gov/cyberframework. [Acedido: 21 de março de 2024]

[61] NIST, «Framework for Improving Critical Infrastructure Cybersecurity (1.0)», *1.0*, 2014, Disponível em: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[62] NIST, «Framework for Improving Critical Infrastructure Cybersecurity (1.1)», National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, abr. 2018. doi: 10.6028/NIST.CSWP.04162018. Disponível em:

http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Acedido: 1 de fevereiro de 2024]

[63] I. T. L. Computer Security Division, «Informative Reference Catalog - National Online Informative References Program | CSRC | CSRC», *CSRC | NIST*, 8 de setembro de 2020. Disponível em: https://csrc.nist.gov/projects/olir/informative-reference-catalog. [Acedido: 20 de março de 2024]

[64] NIST, «Navigating NIST's CSF 2.0 Quick Start Guides», *NIST*, dez. 2023, Disponível em: https://www.nist.gov/quick-start-guides. [Acedido: 20 de março de 2024]

[65] K12 SIX, «Protecting the U.S. K12 Education Sector from Emerging Cybersecurity Threats», *K12 SIX*. Disponível em: https://www.k12six.org/about. [Acedido: 1 de fevereiro de 2024]

[66] K12 SIX, «K12 SIX - The State of K12 Cybersecurity 2022 Anual Report.pdf». Disponível em: https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/6228bfe3f412c818293e16e1/1646837732368/StateofK12Cybersecurity2022.pdf. [Acedido: 1 de fevereiro de 2024]

[67] F. M. F. Marques, «ESTRATÉGIA INTEGRADA DE AVALIAÇÃO E CONSCIENCIALIZAÇÃO CIBERNÉTICA EM CONTEXTO ESCOLAR», masterThesis, 2021. Disponível em: https://iconline.ipleiria.pt/handle/10400.8/6651. [Acedido: 1 de fevereiro de 2024]

[68] Bruno Daniel Monte Pereira, «Ciberexercícios na Comunidade Académica», p. 79, 2022, Disponível em: https://recipp.ipp.pt/handle/10400.22/21344

[69] CSIRT.UPORTO, Bruno Pereira, e Sara Andrade, «CyberLab - CYBERSECURITY INNOVATION LAB FOR PUBLIC ADMINISTRATION», Jornadas FCCN, 2023. Disponível em: https://indico.fccn.pt/event/26/sessions/299/attachments/378/735/04%20CyberLab.pdf

[70] Metared, «MetaRed Portugal lança campanha #ProtegeOTeuCampus para sensibilização em cibersegurança», *MetaRed Portugal lança campanha #ProtegeOTeuCampus para sensibilização em cibersegurança*, 1 de outubro de 2021. Disponível em: https://www.metared.org/pt/novidades/MetaRed-portugal-lanza-campanha-protegeoteucampus-.html. [Acedido: 1 de fevereiro de 2024]

[71] Metared, «Outras Entidades Aderentes», *Outras Entidades Aderentes*. Disponível em: https://www.metared.org/pt/outras-entidades-aderentes.html. [Acedido: 1 de fevereiro de 2024]

[72] Assembleia da República, «Lei n.º 22/2008, de 13 de maio», *Lei n.º 22/2008, de 13 de maio*, 13 de maio de 2008. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/22-2008-249237. [Acedido: 24 de março de 2024]

[73] DGEEC, «Direção-Geral de Estatísticas da Educação e Ciência - DGEEC», *IUTIC - Inquérito à Utilização das Tecnologias da Informação e da Comunicação*, 12 de outubro de 2023. Disponível em: https://www.dgeec.medu.pt/art/u/u/u/652834def28299a6babd74a3. [Acedido: 2 de fevereiro de 2024]

[74] DGEEC, «Principais resultados 2022», vol. 1, n.º 1, p. 11, dez. 2023, Disponível em: https://www.dgeec.medu.pt/api/ficheiros/658eb977f85d439ae0dbce60

[75] DGEEC, «DGEEC - Inquérito à utilização das tecnologias da informação e comunicação - Admin. Pública Central e Regional». Disponível em: https://www.dgeec.medu.pt/api/ficheiros/6528355cf28299a6babd74a4. [Acedido: 2 de fevereiro de 2024]

[76] FCT/FCCN, «Cibersegurança - Ferramenta de Autoavaliação», *Cibersegurança - Ferramenta de Autoavaliação*. Disponível em: https://survey.fccn.pt/index.php/188449. [Acedido: 2 de fevereiro de 2024]

[77] IGeFE, «Pesquisa Rede Escolar - GesEdu», *Pesquisa da Rede Escolar*. Disponível em: https://www.gesedu.pt/PesquisaRede. [Acedido: 2 de fevereiro de 2024]

[78] DGEEC, «Info DGEEC N.º 4», *Info DGEEC N.º 4*, 1 de outubro de 2023. Disponível em: https://info.dgeec.medu.pt/4/9/. [Acedido: 2 de fevereiro de 2024]

[79] NIST, «NCNR Information Management System», *NIST Center for Neutron Research*. Disponível em: https://www-s.nist.gov/NCNR-IMS/passwordTips.jsp. [Acedido: 20 de fevereiro de 2024]

[80] NIST, «NIST - Multi-Factor Authentication». Disponível em: https://www.nist.gov/system/files/documents/2024/02/15/MFA-SMB_2024_Final.pdf. [Acedido: 20 de fevereiro de 2024]

[81] NIST, «NIST - Protecting Data From Ransomware.pdf». Disponível em: https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf. [Acedido: 20 de fevereiro de 2024]

[82] TechTarget, «The 7 critical backup strategy best practices to keep data safe | TechTarget», *Data Backup*, 18 de janeiro de 2023. Disponível em: https://www.techtarget.com/searchdatabackup/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe. [Acedido: 21 de fevereiro de 2024]

[83] Carlos Almeida, «Sistema de monitorização e alarmística de ativos de rede». Disponível em: https://recipp.ipp.pt/bitstream/10400.22/8034/1/DM_CarlosAlmeida_2015_MEI.pdf. [Acedido: 21 de fevereiro de 2024]

[84] K. A. Scarfone, M. P. Souppaya, A. Cody, e A. D. Orebaugh, «Technical guide to information security testing and assessment.», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. [Acedido: 4 de fevereiro de 2024]

[85] Fortra, «2023 Penetration Testing Report.pdf». Disponível em: https://static.fortra.com/core-security/pdfs/guides/cs-2023-pen-testing-report-gd.pdf. [Acedido: 21 de março de 2024]

[86] Presidência do Conselho de Ministros - Gabinete Nacional de Segurança - Centro Nacional de Cibersegurança, «Regulamento n.º 183/2022, de 21 de fevereiro», *Regulamento n.º 183/2022, de 21 de fevereiro*, 21 de fevereiro de 2022. Disponível em: https://diariodarepublica.pt/dr/detalhe/regulamento/183-2022-179325870. [Acedido: 21 de março de 2024]

[87] Microsoft, «Windows 7 support ended on January 14, 2020», *Windows 7 support ended on January 14, 2020*. Disponível em: https://support.microsoft.com/en-

us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962. [Acedido: 4 de fevereiro de 2024]

[88] Microsoft, «Windows Server 2012 and 2012 R2 reaching end of support», *Windows Server 2012 and 2012 R2 reaching end of support*, 5 de maio de 2023. Disponível em: https://learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support. [Acedido: 4 de fevereiro de 2024]

[89] DGEEC, «Selo de Segurança Digital (eSafety Label) 2022 - Escolas Certificadas | Direção-Geral da Educação», *Selo de Segurança Digital (eSafety Label) 2022 - Escolas Certificadas*, 12 de dezembro de 2022. Disponível em: https://www.dge.mec.pt/noticias/selo-de-seguranca-digital-esafety-label-2022-escolas-certificadas. [Acedido: 15 de março de 2024]

[90] Parlamento Europeu, «Regulamento Geral sobre a Proteção de Dados (RGPD)», *Regulamento Geral sobre a Proteção de Dados (RGPD)*, 7 de janeiro de 2022. Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html. [Acedido: 21 de março de 2024]

[91] Parlamento Europeu, «REGULAMENTO (UE) 2016/679», *2016-04-27*, p. 88, abr. 2016, Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

[92] Assembleia da República, «Lei n.º 58/2019, de 8 de agosto», *Lei n.º 58/2019, de 8 de agosto*, 8 de agosto de 2019. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982. [Acedido: 11 de março de 2024]

[93] Presidência do Conselho de Ministros, «Resolução do Conselho de Ministros n.º 41/2018», *Resolução do Conselho de Ministros n.º 41/2018, de 28 de março*, 28 de março de 2018. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034. [Acedido: 11 de março de 2024]

[94] Fortinet, «What is BYOD? Bring Your Own Device Meaning and Policies», *Fortinet*. Disponível em: https://www.fortinet.com/resources/cyberglossary/byod?utm_source=blog&utm_medium=blog&utm_campaign=blog-byod. [Acedido: 28 de maio de 2024]

[95] S. Kitterman, «Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1», Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc7208, Request for Comments RFC 7208, abr. 2014. doi: 10.17487/RFC7208. Disponível em: https://datatracker.ietf.org/doc/rfc7208. [Acedido: 25 de março de 2024]

[96] DKIM, «DomainKeys Identified Mail (DKIM)», *DomainKeys Identified Mail (DKIM)*. Disponível em: https://www.dkim.org/. [Acedido: 25 de março de 2024]

[97] A. Brotman, «DMARC Aggregate Reporting», Internet Engineering Task Force, Internet Draft draft-ietf-dmarc-aggregate-reporting-14, fev. 2024. Disponível em: https://datatracker.ietf.org/doc/draft-ietf-dmarc-aggregate-reporting. [Acedido: 25 de março de 2024]

Anexos

Anexo A – Inquérito sobre a utilização das TIC na Administração Pública Central (DGEEC)

VII - SEGURANÇA DAS TIC (CIBERSEGURANÇA)

Segurança das TIC - medidas, controlos e procedimentos aplicados em sistemas das TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados e dos sistemas.

1. O Organismo utiliza alguma das seguintes medidas de segurança das TIC?

	Sim	Não
a) Autenticação dos utilizadores através de uma palavra passe segura (mínimo de doze caracteres com letras maiúsculas e minúsculas, algarismos, caracteres especiais, uma palavra-passe por cada plataforma)	☐	☐
b) Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação (i.e. combinação de palavra-passe definida pelo utilizador, palavra-passe de uso único (OTP), código gerado por token de segurança ou recebido via smartphone, métodos biométricos (impressões digitais, reconhecimento de voz, reconhecimento facial))	☐	☐
c) Autenticação do utilizador através de métodos biométricos (impressões digitais, voz, rostos)	☐	☐
d) Atualização regular do software (incluído sistemas operativos)	☐	☐
e) Técnicas de proteção por método criptográfico de dados, documentos ou/ e-mail	☐	☐
f) Controlo de acessos remotos à rede do Organismo (acesso dos dispositivos e dos utilizadores, ex.: VPN)	☐	☐
g) Conservação de registos (histórico) para análise depois da ocorrência de incidentes de segurança	☐	☐
h) Análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação	☐	☐
i) Testes de segurança às TIC (de intrusão, aos sistemas de alerta e de backup, revisões às medidas de segurança)	☐	☐
j) Inventário de todos os ativos essenciais para a prestação dos serviços de segurança das TIC	☐	☐
k) Cópias de segurança cumprindo a regra 3-2-1 (realização de três cópias: duas em suportes diferentes e a terceira guardada offline)	☐	☐
l) Sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar o Organismo sobre as mesmas, excluindo o software antivírus autónomo	☐	☐

2. O Organismo informa o pessoal ao serviço para as suas obrigações em matéria de segurança das TIC, através de:

	Sim	Não
a) Ações de formação voluntária ou informação interna disponível (Intranet, etc.)	☐	☐
b) Ações de formação obrigatória e/ou consulta obrigatória de informação	☐	☐
c) Disposições contratuais (ex.: políticas de utilização responsável dos equipamentos informáticos que os utilizadores têm de assinar)	☐	☐

3. Quem realiza as atividades relacionadas com a segurança das TIC do Organismo?
(ex.: testes, formação e resolução de incidentes de segurança. Excluem-se as atualizações de software pré-configurado)

	Sim	Não
a) Pessoal do próprio Organismo	☐	☐
b) Fornecedores externos	☐	☐

As recomendações sobre segurança TIC não têm que ser obrigatoriamente documentos formais escritos. Podem ser informações/instruções internas e devem incluir temas como: formação para a utilização, medidas de segurança e a sua avaliação, planos para atualização de documentos de segurança, etc.

4. O Organismo possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC?

Sim	Não
☐	☐

SE RESPONDEU "NÃO" PASSE PARA A QUESTÃO 7.

5. Nessas recomendações são considerados alguns dos seguintes temas?

	Sim	Não
a) Gestão dos níveis de acesso às TIC (ex.: computadores, redes)	☐	☐
b) Armazenamento, proteção, acesso e processamento de dados	☐	☐
c) Procedimentos e regras para prevenir e/ou reagir a incidentes de segurança (ex.: negação de serviço, ataques de phishing, ransomware, etc.)	☐	☐
d) Responsabilidade, direitos e deveres no que respeita à utilização das TIC (ex.: uso de e-mails, dispositivos móveis, social media, etc.)	☐	☐
e) Boas práticas para o pessoal ao serviço na utilização segura das TIC	☐	☐

6. Quando foram definidas ou revistas as recomendações sobre medidas, práticas ou procedimentos de segurança TIC?
(ex.: avaliação de riscos, evolução de incidentes, etc.)

(escolha apenas uma opção)

a) Nos últimos 12 meses	☐
b) Há mais de 12 meses e até 24 meses	☐
c) Há mais de 24 meses	☐

7. O Organismo detetou problemas de segurança informática?

Sim	Não
☐	☐

SE RESPONDEU "NÃO" PASSE PARA A QUESTÃO 8.

7.1. O Organismo sofreu algum incidente de segurança relacionado com as TIC, que tenha tido alguma das seguintes consequências?

	Sim	Não
a) Indisponibilidade de serviços TIC devido a falhas de hardware ou software	☐	☐
b) Indisponibilidade de serviços TIC devido a ataques do exterior (ex.: ataques de negação de serviço e ransomware)	☐	☐
c) Destruição ou corrupção de dados devido a falhas de hardware ou software	☐	☐
d) Destruição ou corrupção de dados devido a infeção de software malicioso ou intrusão não autorizada	☐	☐
e) Divulgação de dados confidenciais devido a ataques de intrusão, pharming ou phishing , ações intencionais dos próprios funcionários	☐	☐
f) Divulgação de dados confidenciais devido a ações não intencionais dos próprios funcionários	☐	☐
g) Outro(s). Especifique: _____	☐	☐

8. O Organismo tem seguro contra incidentes de segurança das TIC?

Sim	Não
☐	☐

9. O Organismo tem definida uma estratégia/política para a segurança das redes e da informação?

Sim	Não
☐	☐

SE RESPONDEU "NÃO" PASSE PARA O MÓDULO VIII-INTELIGÊNCIA ARTIFICIAL.

9.1. A estratégia/política para a segurança das redes e da informação:

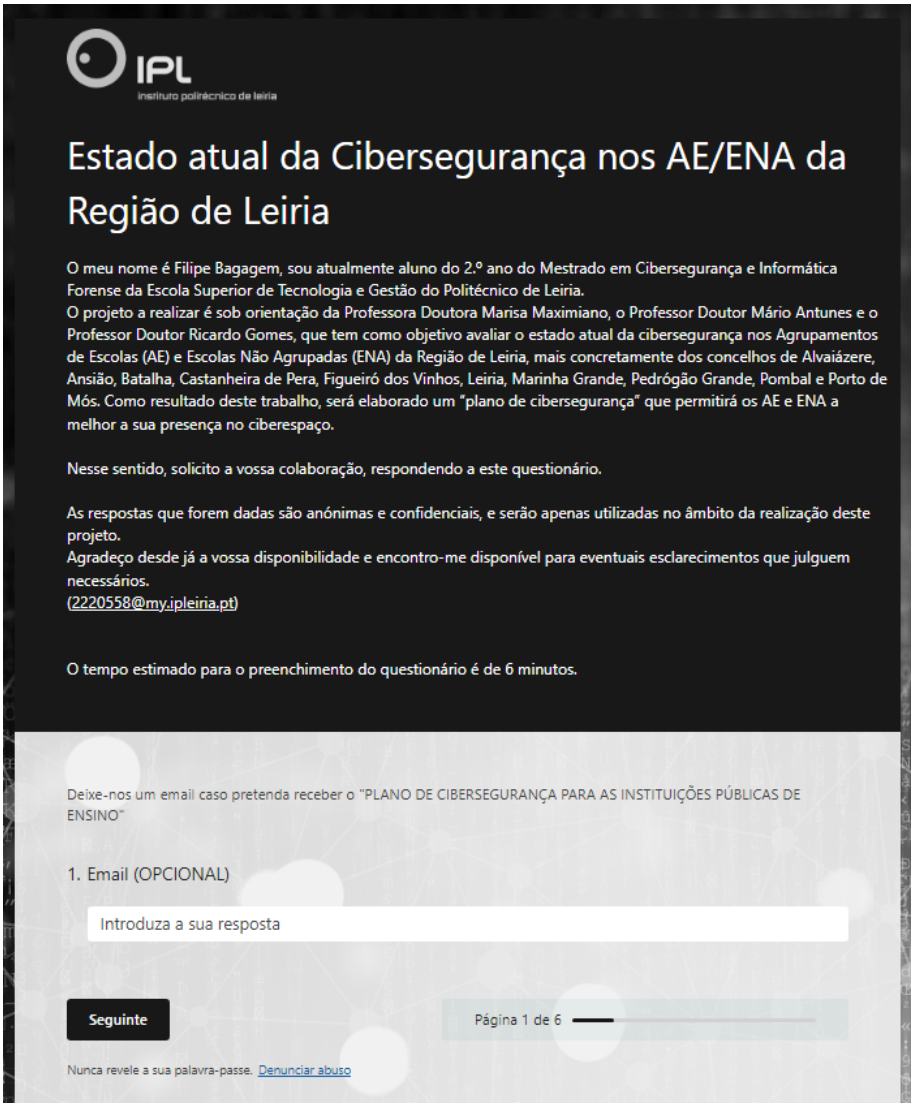
	Sim	Não
a) Já se encontra implementada no Organismo	☐	☐
b) Encontra-se em fase de implementação no Organismo	☐	☐
c) Prevê avaliar regularmente os resultados das metodologias de segurança de informação colocadas em prática	☐	☐
Regulamento Geral de Proteção de Dados (RGPD)		
d) Já se encontra de acordo com o RGPD	☐	☐
e) Encontra-se em fase de revisão de modo a incorporar o RGPD	☐	☐
f) Prevê avaliar regularmente os resultados das metodologias de segurança de informação colocadas em prática face ao RGPD	☐	☐
Regime Jurídico da Segurança do Ciberespaço (RJSC) - Decreto-Lei n.º 65/2021		
g) Já se encontra de acordo com o RJSC	☐	☐
h) Encontra-se em fase de revisão de modo a incorporar o RJSC	☐	☐
i) Prevê avaliar regularmente os resultados das metodologias de segurança das redes e da informação colocadas em prática face ao RJSC	☐	☐

SE RESPONDEU "SIM" NAS ALINEAS G) OU H) PASSE PARA A QUESTÃO 9.2.

9.2. De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), o Organismo:

	Sim	Não
a) Tem um ponto de contacto permanente com o Centro Nacional de Cibersegurança (CNCS)	☐	☐
b) Designou um responsável de segurança (responsável pela gestão das medidas de segurança como, por exemplo, um CISO - Chief Information Security Officer) junto do CNCS	☐	☐
c) Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços	☐	☐
d) Elaborou e mantém atualizado o plano de segurança, devidamente documentado e assinado pelo responsável de segurança	☐	☐
e) Elaborou o relatório anual de segurança no ano transacto	☐	☐
f) Efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)	☐	☐

Anexo B - Questionário disponibilizado aos AE/ENA através do Microsoft Forms



IPL
instituto politécnico de leiria

Estado atual da Cibersegurança nos AE/ENA da Região de Leiria

O meu nome é Filipe Bagagem, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.
O projeto a realizar é sob orientação da Professora Doutora Marisa Maximiano, o Professor Doutor Mário Antunes e o Professor Doutor Ricardo Gomes, que tem como objetivo avaliar o estado atual da cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da Região de Leiria, mais concretamente dos concelhos de Alvaiázere, Ansião, Batalha, Castanheira de Pera, Figueiró dos Vinhos, Leiria, Marinha Grande, Pedrógão Grande, Pombal e Porto de Mós. Como resultado deste trabalho, será elaborado um "plano de cibersegurança" que permitirá os AE e ENA a melhor a sua presença no ciberespaço.

Nesse sentido, solicito a vossa colaboração, respondendo a este questionário.

As respostas que forem dadas são anónimas e confidenciais, e serão apenas utilizadas no âmbito da realização deste projeto.
Agradeço desde já a vossa disponibilidade e encontro-me disponível para eventuais esclarecimentos que julguem necessários.
(2220558@my.ipleiria.pt)

O tempo estimado para o preenchimento do questionário é de 6 minutos.

Deixe-nos um email caso pretenda receber o "PLANO DE CIBERSEGURANÇA PARA AS INSTITUIÇÕES PÚBLICAS DE ENSINO"

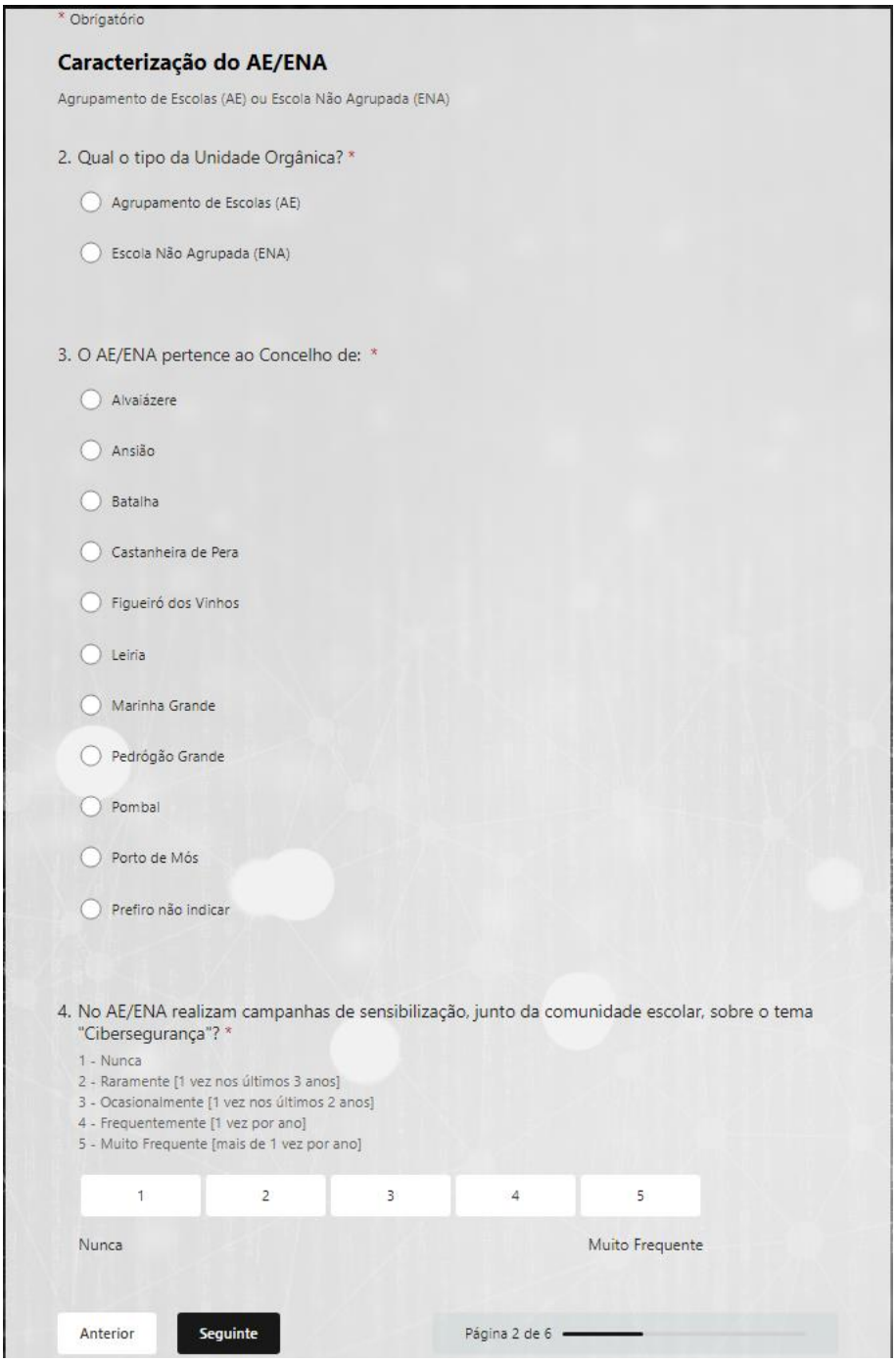
1. Email (OPCIONAL)

Introduza a sua resposta

Seguinte

Página 1 de 6

Nunca revele a sua palavra-passe. Denunciar abuso



* Obrigatório

Caracterização do AE/ENA

Agrupamento de Escolas (AE) ou Escola Não Agrupada (ENA)

2. Qual o tipo da Unidade Orgânica? *

- ◯ Agrupamento de Escolas (AE)
- ◯ Escola Não Agrupada (ENA)

3. O AE/ENA pertence ao Concelho de: *

- ◯ Alvaiázere
- ◯ Ansião
- ◯ Batalha
- ◯ Castanheira de Pera
- ◯ Figueiró dos Vinhos
- ◯ Leiria
- ◯ Marinha Grande
- ◯ Pedrógão Grande
- ◯ Pombal
- ◯ Porto de Mós
- ◯ Prefiro não indicar

4. No AE/ENA realizam campanhas de sensibilização, junto da comunidade escolar, sobre o tema "Cibersegurança"? *

1 - Nunca
2 - Raramente [1 vez nos últimos 3 anos]
3 - Ocasionalmente [1 vez nos últimos 2 anos]
4 - Frequentemente [1 vez por ano]
5 - Muito Frequente [mais de 1 vez por ano]

1	2	3	4	5

Nunca Muito Frequente

Anterior Seguinte Página 2 de 6

* Obrigatório

Estratégia do AE/ENA relativamente à segurança das TIC

Segurança das TIC - medidas, controlos e procedimentos aplicados em sistemas das TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados e dos sistemas.

5. Para o acesso a plataformas digitais com informação confidencial, exigem aos utilizadores Palavras-passe seguras: *

Palavra-passe segura: mínimo de doze caracteres com letras maiúsculas e minúsculas, algarismos, caracteres especiais e uma palavra-passe por cada plataforma.

- ◯ Sim
- ◯ Não

6. Para o acesso a plataformas digitais com informação confidencial, exigem aos Utilizadores Autenticação de dois fatores (2FA)? *

Autenticação de dois fatores (2FA): combinação de palavra-passe definida pelo utilizador, palavra-passe de uso único (OTP), código gerado por token de segurança ou recebido/consultado na App móvel (Google Authenticator, Microsoft Authenticator ou outro do género).

- ◯ Sim
- ◯ Não

7. Para acederem do exterior a recursos internos, utilizam: *

Não considerar na resposta os protocolos HTTP e HTTPS, que habitualmente são utilizados para associar a plataformas web que estão alojadas na rede interna do AE/ENA.

- ◯ Abertura de portos - NAT (Network address translation) Ex.: RDP- porto interno: 3389
- ◯ Serviço de VPN (Virtual Private Network)
- ◯ Agentes que permitem o acesso remoto. Ex.: TeamViewer, AnyDesk, outros do género
- ◯ A política em uso não permite que ninguém aceda do exterior a recursos internos

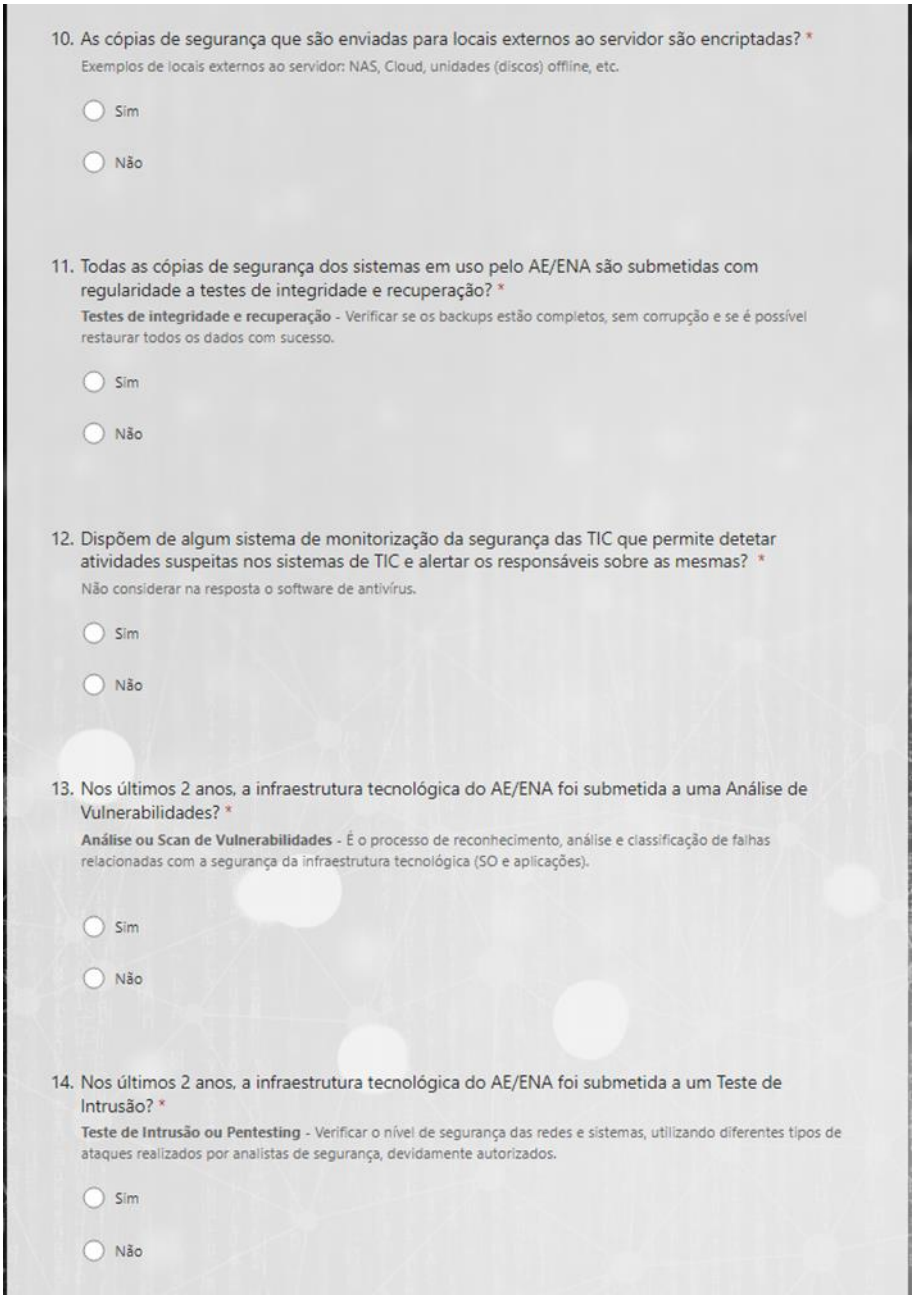
8. No AE/ENA ainda temos equipamentos, em uso, com as seguintes versões do Windows: *

- ☐ Windows Server 2003
- ☐ Windows Server 2008
- ☐ Windows Server 2012
- ☐ Windows XP
- ☐ Windows 7
- ☐ Windows 8 ou 8.1
- ☐ Todos os equipamentos, em uso, têm versões do Windows superiores às listadas acima

9. As cópias de segurança cumprem a regra 3-2-1? *

3-2-1: realização de três cópias de segurança em locais distintos. Uma no próprio servidor, outra num local externo ao servidor (NAS, Cloud, outro servidor, etc) e uma terceira cópia guardada numa unidade offline.

- ◯ Sim
- ◯ Não



10. As cópias de segurança que são enviadas para locais externos ao servidor são encriptadas? *

Exemplos de locais externos ao servidor: NAS, Cloud, unidades (discos) offline, etc.

- ◯ Sim
- ◯ Não

11. Todas as cópias de segurança dos sistemas em uso pelo AE/ENA são submetidas com regularidade a testes de integridade e recuperação? *

Testes de integridade e recuperação - Verificar se os backups estão completos, sem corrupção e se é possível restaurar todos os dados com sucesso.

- ◯ Sim
- ◯ Não

12. Dispõem de algum sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar os responsáveis sobre as mesmas? *

Não considerar na resposta o software de antivírus.

- ◯ Sim
- ◯ Não

13. Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a uma Análise de Vulnerabilidades? *

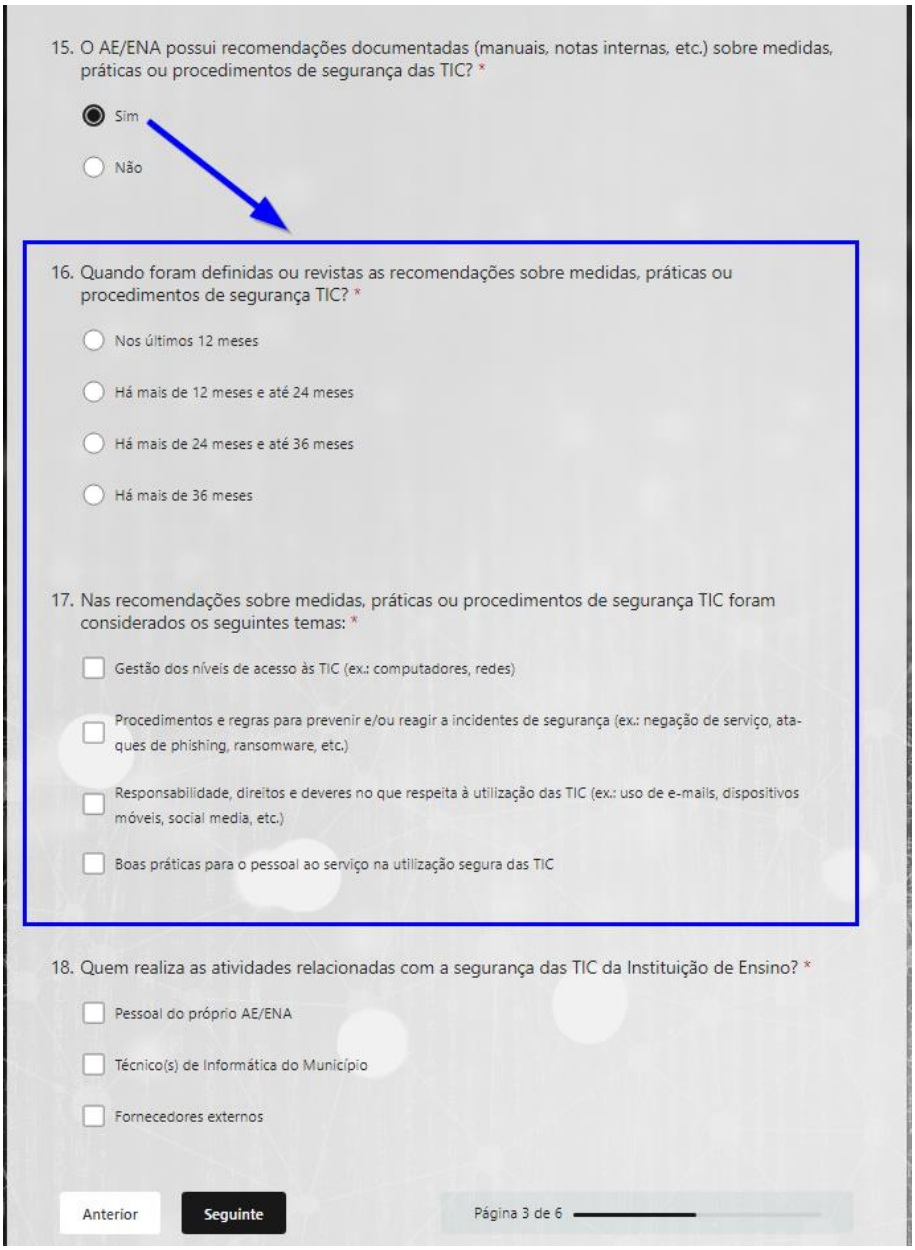
Análise ou Scan de Vulnerabilidades - É o processo de reconhecimento, análise e classificação de falhas relacionadas com a segurança da infraestrutura tecnológica (SO e aplicações).

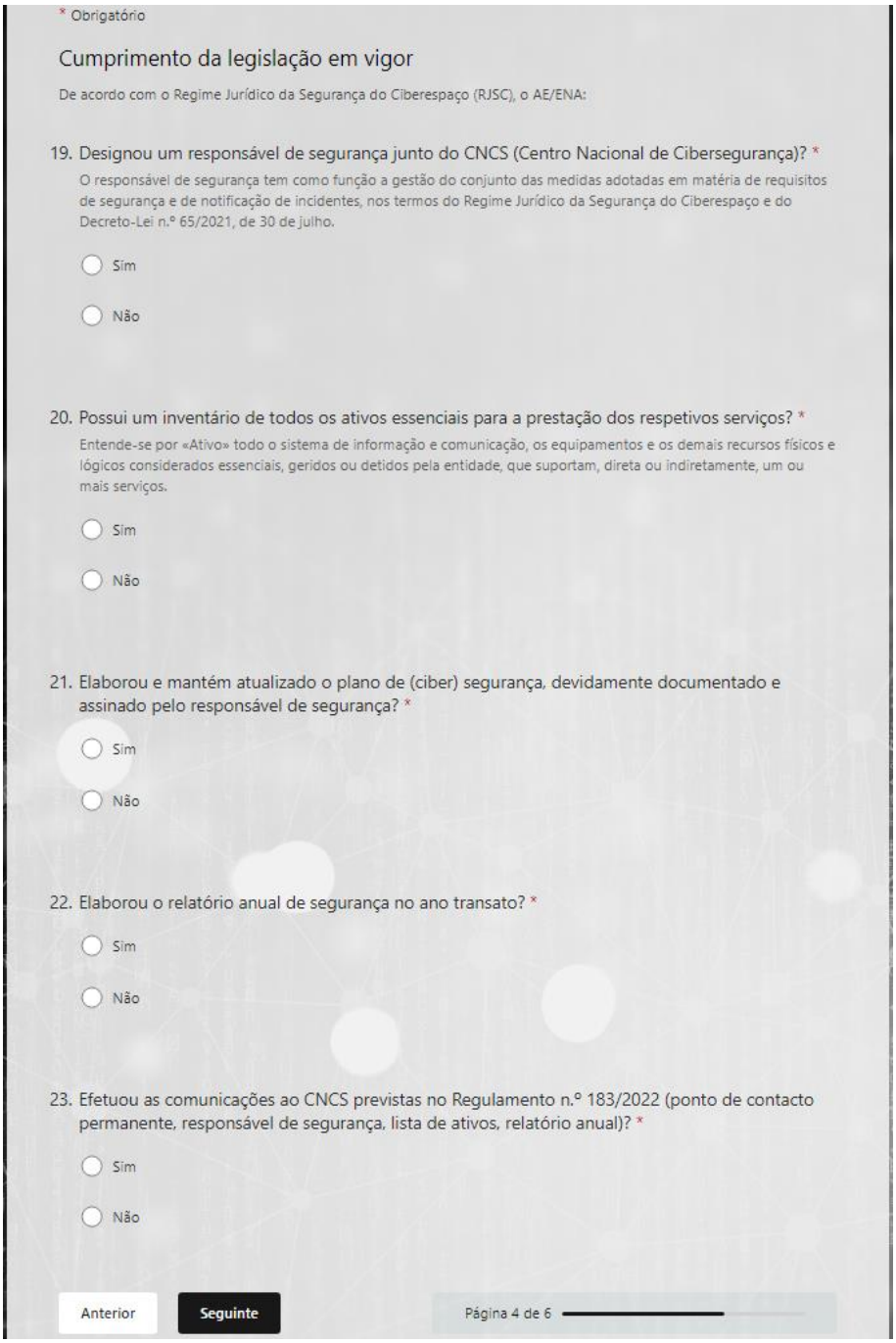
- ◯ Sim
- ◯ Não

14. Nos últimos 2 anos, a infraestrutura tecnológica do AE/ENA foi submetida a um Teste de Intrusão? *

Teste de Intrusão ou Pentesting - Verificar o nível de segurança das redes e sistemas, utilizando diferentes tipos de ataques realizados por analistas de segurança, devidamente autorizados.

- ◯ Sim
- ◯ Não


15. O AE/ENA possui recomendações documentadas (manuais, notas internas, etc.) sobre medidas, práticas ou procedimentos de segurança das TIC? *
Sim
Não
16. Quando foram definidas ou revistas as recomendações sobre medidas, práticas ou procedimentos de segurança TIC? *
Nos últimos 12 meses
Há mais de 12 meses e até 24 meses
Há mais de 24 meses e até 36 meses
Há mais de 36 meses
17. Nas recomendações sobre medidas, práticas ou procedimentos de segurança TIC foram considerados os seguintes temas: *
Gestão dos níveis de acesso às TIC (ex.: computadores, redes)
Procedimentos e regras para prevenir e/ou reagir a incidentes de segurança (ex.: negação de serviço, ataques de phishing, ransomware, etc.)
Responsabilidade, direitos e deveres no que respeita à utilização das TIC (ex.: uso de e-mails, dispositivos móveis, social media, etc.)
Boas práticas para o pessoal ao serviço na utilização segura das TIC
18. Quem realiza as atividades relacionadas com a segurança das TIC da Instituição de Ensino? *
Pessoal do próprio AE/ENA
Técnico(s) de Informática do Município
Fornecedores externos
Anterior
Seguinte
Página 3 de 6



* Obrigatório

Cumprimento da legislação em vigor

De acordo com o Regime Jurídico da Segurança do Ciberespaço (RJSC), o AE/ENA:

19. Designou um responsável de segurança junto do CNCS (Centro Nacional de Cibersegurança)? *

O responsável de segurança tem como função a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto-Lei n.º 65/2021, de 30 de julho.

- ◯ Sim
- ◯ Não

20. Possui um inventário de todos os ativos essenciais para a prestação dos respetivos serviços? *

Entende-se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.

- ◯ Sim
- ◯ Não

21. Elaborou e mantém atualizado o plano de (ciber) segurança, devidamente documentado e assinado pelo responsável de segurança? *

- ◯ Sim
- ◯ Não

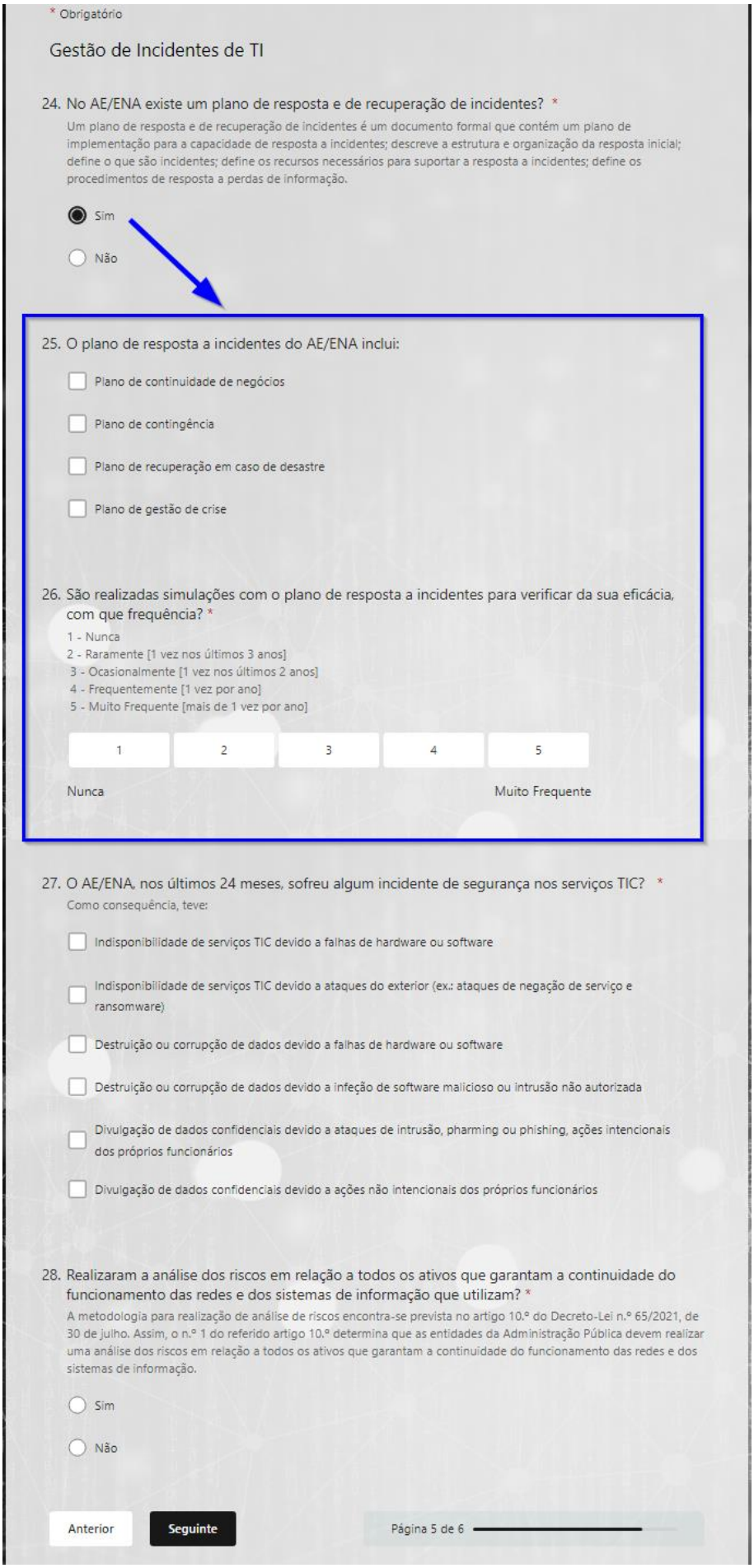
22. Elaborou o relatório anual de segurança no ano transato? *

- ◯ Sim
- ◯ Não

23. Efetuou as comunicações ao CNCS previstas no Regulamento n.º 183/2022 (ponto de contacto permanente, responsável de segurança, lista de ativos, relatório anual)? *

- ◯ Sim
- ◯ Não

Anterior | Seguinte | Página 4 de 6



* Obrigatório

Gestão de Incidentes de TI

24. No AE/ENA existe um plano de resposta e de recuperação de incidentes? *

Um plano de resposta e de recuperação de incidentes é um documento formal que contém um plano de implementação para a capacidade de resposta a incidentes; descreve a estrutura e organização da resposta inicial; define o que são incidentes; define os recursos necessários para suportar a resposta a incidentes; define os procedimentos de resposta a perdas de informação.

- (●) Sim
- ( ) Não

25. O plano de resposta a incidentes do AE/ENA inclui:

- [ ] Plano de continuidade de negócios
- [ ] Plano de contingência
- [ ] Plano de recuperação em caso de desastre
- [ ] Plano de gestão de crise

26. São realizadas simulações com o plano de resposta a incidentes para verificar da sua eficácia, com que frequência? *

1 - Nunca
2 - Raramente [1 vez nos últimos 3 anos]
3 - Ocasionalmente [1 vez nos últimos 2 anos]
4 - Frequentemente [1 vez por ano]
5 - Muito Frequente [mais de 1 vez por ano]

1	2	3	4	5

Nunca — Muito Frequente

27. O AE/ENA, nos últimos 24 meses, sofreu algum incidente de segurança nos serviços TIC? *

Como consequência, teve:

- [ ] Indisponibilidade de serviços TIC devido a falhas de hardware ou software
- [ ] Indisponibilidade de serviços TIC devido a ataques do exterior (ex.: ataques de negação de serviço e ransomware)
- [ ] Destruição ou corrupção de dados devido a falhas de hardware ou software
- [ ] Destruição ou corrupção de dados devido a infeção de software malicioso ou intrusão não autorizada
- [ ] Divulgação de dados confidenciais devido a ataques de intrusão, pharming ou phishing, ações intencionais dos próprios funcionários
- [ ] Divulgação de dados confidenciais devido a ações não intencionais dos próprios funcionários

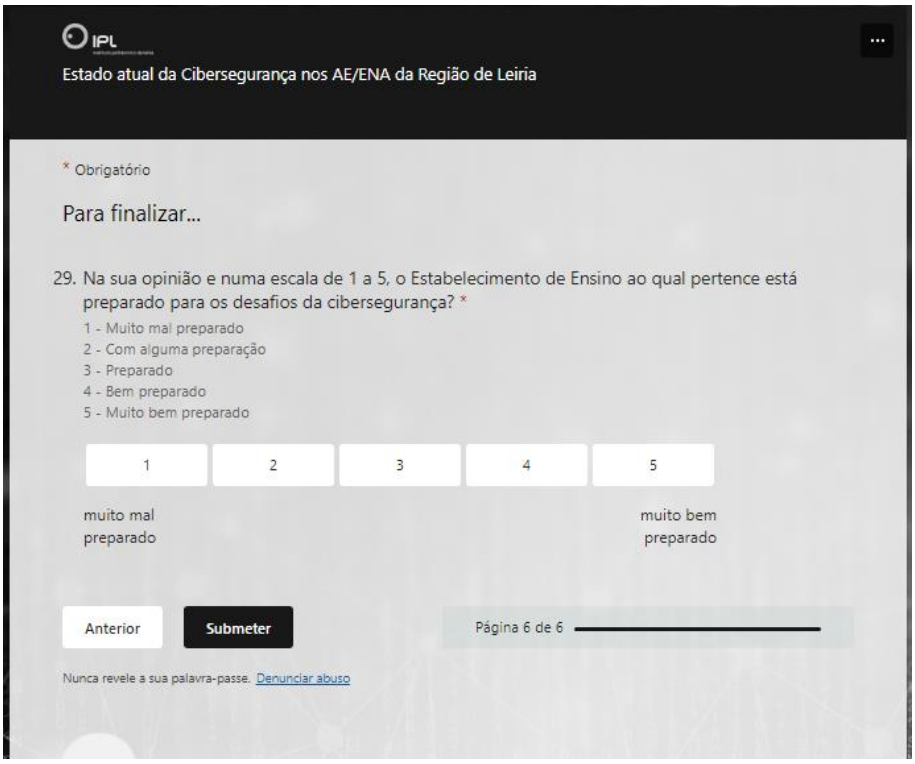
28. Realizaram a análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam? *

A metodologia para realização de análise de riscos encontra-se prevista no artigo 10.º do Decreto-Lei n.º 65/2021, de 30 de julho. Assim, o n.º 1 do referido artigo 10.º determina que as entidades da Administração Pública devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação.

- ( ) Sim
- ( ) Não

Anterior | Seguinte

Página 5 de 6


IPL
Estado atual da Cibersegurança nos AE/ENA da Região de Leiria
* Obrigatório
Para finalizar...
29. Na sua opinião e numa escala de 1 a 5, o Estabelecimento de Ensino ao qual pertence está preparado para os desafios da cibersegurança? *
1 - Muito mal preparado
2 - Com alguma preparação
3 - Preparado
4 - Bem preparado
5 - Muito bem preparado
1
2
3
4
5
muito mal preparado
muito bem preparado
Anterior
Submeter
Página 6 de 6
Nunca revele a sua palavra-passe. Denunciar abuso

Anexo C - E-mail enviado aos AE/ENA (1º envio)

Data do envio: 2 de dezembro de 2023

Questionário para avaliar o estado atual da Cibersegurança nos AE/ENA da Região de Leiria - IPLeiria

Filipe André Pereira Bagagem <2220558@my.ipleiria.pt>

sáb, 02/12/2023 14:47

[redacted]

Exmº/ª. Srº/ª. Diretor(a),

O meu nome é Filipe Bagagem, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense na Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.

No âmbito da tese de Mestrado, que estou a realizar sob orientação da Professora Doutora Marisa Maximiano, o Professor Doutor Mário Antunes e o Professor Doutor Ricardo Gomes, intitulada "**O Estado Atual da Cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da Região de Leiria**", venho pelo presente solicitar a colaboração de V. Exa.

Este estudo tem como objetivo avaliar o estado atual da cibersegurança no setor da educação, mais concretamente nos AE e ENA da região de Leiria e como resultado deste trabalho, será elaborado um "plano de cibersegurança" que permitirá os AE e ENA a melhorar a sua presença no ciberespaço.

Deste modo, foi construído um questionário que está a ser disponibilizado a todos os AE e ENA da região de Leiria.

A informação recolhida é anónima e o tratamento dos dados respeitará o princípio da confidencialidade.

A participação é voluntária, mas possui grande contribuição para o presente estudo.

Neste sentido, agradecemos o preenchimento de um breve questionário utilizando para o efeito o link abaixo ou o QRCode.

Link de acesso: https://forms.office.com/e/pESMEvb9Ew

QRCode:

Contamos, assim, com a vossa colaboração, solicitando a resposta ao questionário até ao dia **31 de dezembro de 2023**.

Estimamos que o preenchimento deste questionário demore cerca de **6 minutos**.

Para o esclarecimento de qualquer dúvida poderá considerar o seguinte e-mail 2220558@my.ipleiria.pt

Agradeço desde já a vossa atenção e disponibilidade.

Com os melhores cumprimentos,

Filipe Bagagem

IPL instituto politécnico de leiria

Anexo D – E-mail enviado aos AE/ENA (2º envio)

Data do envio: 27 de dezembro de 2023

Questionário para avaliar o estado atual da Cibersegurança nos AE/ENA da Região de Leiria - IPLeiria (2º Pedido)

Filipe André Pereira Bagagem <2220558@my.ipleiria.pt>

qua, 27/12/2023 14:49

[redacted]

Exmº/ª. Srº/ª. Diretor(a),

Caso já tenha respondido ao questionário ignore, por favor, este segundo pedido. Aproveito para agradecer a sua participação e pedir desculpa pelo incómodo de uma nova mensagem.

O meu nome é Filipe Bagagem, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense na Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.
No âmbito da tese de Mestrado, que estou a realizar sob orientação da Professora Doutora Marisa Maximiano, o Professor Doutor Mário Antunes e o Professor Doutor Ricardo Gomes, intitulada "**O Estado Atual da Cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da Região de Leiria**", venho pelo presente solicitar a colaboração de V. Exa.

Este estudo tem como objetivo avaliar o estado atual da cibersegurança no setor da educação, mais concretamente nos AE e ENA da região de Leiria e como resultado deste trabalho, será elaborado um "plano de cibersegurança" que permitirá os AE e ENA a melhorar a sua presença no ciberespaço.

Deste modo, foi construído um questionário que está a ser disponibilizado a todos os AE e ENA da região de Leiria.

A informação recolhida é anónima e o tratamento dos dados respeitará o princípio da confidencialidade.

A participação é voluntária, mas possui grande contribuição para o presente estudo.

Neste sentido, agradecemos o preenchimento de um breve questionário utilizando para o efeito o link abaixo ou o QRCode.

Link de acesso: https://forms.office.com/e/pESMEvb9Ew

QRCode:

Contamos, assim, com a vossa colaboração, solicitando a resposta ao questionário até ao dia **31 de dezembro de 2023**.

Estimamos que o preenchimento deste questionário demore cerca de **6 minutos**.

Para o esclarecimento de qualquer dúvida poderá considerar o seguinte e-mail 2220558@my.ipleiria.pt

Agradeço desde já a vossa atenção e disponibilidade.

Com os melhores cumprimentos,

Filipe Bagagem

IPL
instituto politécnico de leiria

Anexo E – Calendário com as tarefas para a disponibilização do questionário

Mês	Dom	Seg	Ter	Qua	Qui	Sex	Sáb
						1	2 Dispobilização do Questionário Envio do 1º E-MAIL
Dez 2023	3	4	5	6	7	8	9
	10	11	12	13	14	15	16
	17 Pausa Letiva	18 Pausa Letiva	19 Pausa Letiva	20 Pausa Letiva	21 Pausa Letiva	22 Pausa Letiva	23 Pausa Letiva
	24 Pausa Letiva	25 Pausa Letiva	26 Pausa Letiva	27 Pausa Letiva Envio do 2º E-MAIL	28 Pausa Letiva	29 Pausa Letiva	30 Pausa Letiva
	31 Pausa Letiva Fim Questionário	1 Pausa Letiva Período alargado	2 Pausa Letiva Período alargado	3 Período alargado	4 Período alargado	5 Período alargado	6 Período alargado
Jan 2024	7 Período alargado	8 Período alargado	9 Período alargado	10 Período alargado	11 Período alargado	12 Período alargado	13 Período alargado
	14 Período alargado	15 Período alargado	16 Período alargado	17 Período alargado	18 Período alargado	19 Período alargado	20 Período alargado Fim do Período Alargado
	21	22	23	24	25	26	27
	28	29	30	31			

Tabela 15 – Calendário – Disponibilização do Questionário

Anexo F – Disponibilização do guia de cibersegurança às instituições de ensino

Data do envio: 2 de maio de 2024

Cibersegurança – Guia de Boas Práticas para as Escolas [IPLeiria]

Filipe André Pereira Bagagem <2220558@my.ipleiria.pt>

qui, 02/05/2024 12:32

[redacted]

Exmº/ª. Srº/ª. Professor(a) e/ou Técnico(a) Informática,

O meu nome é Filipe Bagagem, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense na Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.
No âmbito da tese de Mestrado, em curso sob a orientação da Prof. Dr. Marisa Maximiano, o Prof. Dr. Mário Antunes e o Prof. Ricardo Gomes, intitulada "O Estado Atual da Cibersegurança nos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da Região de Leiria", elaborei um guia de cibersegurança, destinado às instituições de ensino, que partilho agora V. Ex.ª.

Este guia de cibersegurança disponibiliza informações e recomendações para auxiliar as instituições de ensino a protegerem-se no ciberespaço. O presente guia é direcionado a vários tipos de utilizadores das instituições de ensino, tais como:

- Direção (Diretor(a), Sub-Diretor(a) ou Adjunto(a) Direção);
- Encarregado de Proteção de Dados;
- Responsável de Segurança;
- Coordenador(a) TIC;
- Técnico(a) Informática;
- Entre outros que assegurem a segurança da informação na instituição de ensino.

Aproveito o momento para prestar um especial agradecimento a todos os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da região de Leiria que participaram neste estudo que serviu de base para elaborar o presente guia de cibersegurança.

O Guia de Boas Práticas para as Escolas pode ser descarregado através do link ou QRCode abaixo.
Link: https://github.com/filbag/Ciberseguranca--Guia-de-Boas-Praticas
QRCode:

Para o esclarecimento de qualquer dúvida poderá considerar o seguinte email 2220558@my.ipleiria.pt

Agradeço desde já a vossa atenção e disponibilidade.

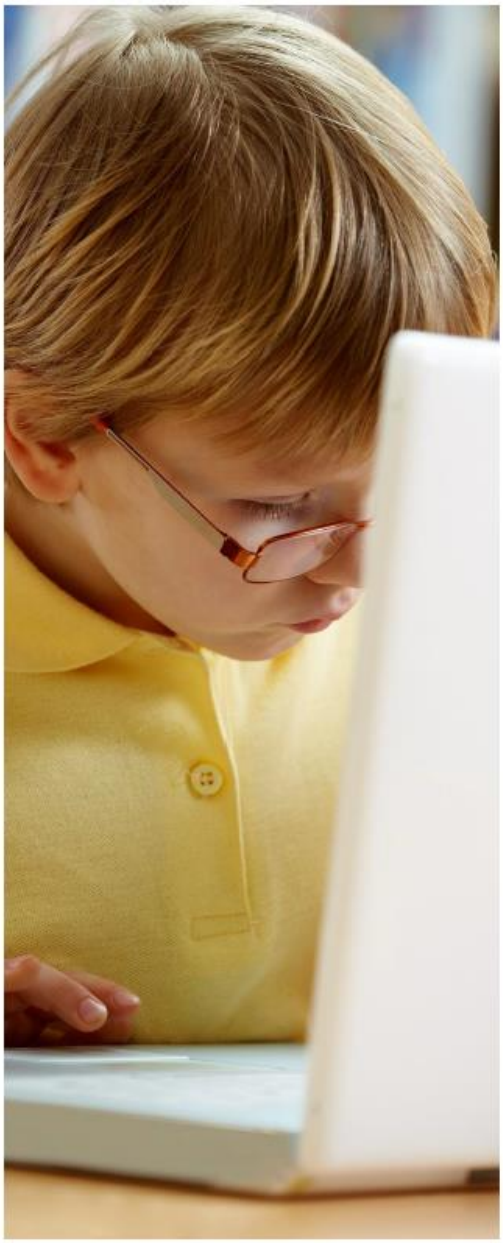
Com os melhores cumprimentos,
Filipe Bagagem

IPL
instituto politécnico de leiria

Anexo G – Guia de Boas Práticas para as Escolas

Este guia de cibersegurança para as instituições de ensino disponibiliza informações e recomendações para auxiliar os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) de Portugal Continental a protegerem-se no ciberespaço. O guia tem como público-alvo os responsáveis pelas Tecnologias de Informação e Comunicação (TIC) e está dividido em cinco secções. Na primeira secção, são abordados temas gerais da cibersegurança e os principais aspetos que a constituem, tais como os tipos de ataques e os seus impactos. Na segunda secção, o guia apresenta o estado atual da cibersegurança na educação. A terceira secção aborda a legislação e regulamentos em vigor no âmbito da segurança da informação, bem como as normas mais relevantes de cibersegurança. Na quarta secção, são elencadas algumas das recomendações e boas práticas de cibersegurança. Finalmente, são apresentadas as contribuições sobre o tema e as conclusões.

Palavras-chave: Cibersegurança, segurança cibernética, ciberataques, ataques cibernéticos, ciberespaço, espaço cibernético, proteção de dados, governança, proteção de ativos, educação, instituições de ensino, agrupamentos de escolas, escolas não agrupadas, sistemas de informação, tecnologia da informação, segurança da informação, segurança de TI.



SUMÁRIO

Prefácio

Este guia de cibersegurança para as instituições de ensino visa disponibilizar um conjunto de informações e acrescentar valor para se entender melhor o que é a cibersegurança, riscos, potenciais impactos e a necessidade de agir proactivamente para proteger as Tecnologias de Informação e Comunicação (TIC) e os dados contidos nestas.

Prólogo

Este guia teve origem num trabalho académico, mais concretamente numa tese de mestrado de Cibersegurança e Informática Forense ministrada pelo Instituto Politécnico de Leiria, intitulada de "Estado atual da Cibersegurança nos AE/ENA da Região de Leiria" sobe a orientação da Prof. Dr. Marisa Maximiano, do Prof. Ricardo Gomes e o do Prof. Dr. Mário Antunes.

Agradecimentos

Um especial agradecimento a todos os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da região de Leiria que participaram no estudo intitulado de "Estado atual da Cibersegurança nos AE/ENA da Região de Leiria" que serviu de base para elaborar o presente documento.

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

INTRODUÇÃO

Apresenta-se este guia com o objetivo de promover a conscientização e a compreensão da cibersegurança ou segurança da tecnologia de informação, bem como os possíveis riscos e resultados dos ataques cibernéticos às operações das instituições de ensino. O guia permite visualizar os possíveis riscos, impactos e a necessidade de proteger a infraestrutura tecnológica das instituições de ensino contra ataques mal-intencionados.

A Administração Pública é uma peça fundamental na cibersegurança do país
Não só porque deve dar o exemplo às outras organizações, como porque presta serviços muito importantes para o funcionamento da sociedade, a Administração Pública (e a sua cibersegurança) afeta todos os cidadãos, direta ou indiretamente. Fonte: CNCS

O que é o Guia de Boas Práticas de Cibersegurança para as Escolas?

Este guia de cibersegurança oferece conhecimento às instituições de ensino sobre a cibersegurança, os riscos digitais, os possíveis impactos e a necessidade de uma ação mais proactiva.

A quem se destina este guia?

O Guia de Boas Práticas de Cibersegurança para as Escolas é direcionado a vários tipos de utilizadores das instituições de ensino, tais como:

- Direção (Diretor(a), Sub-Diretor(a) ou Adjunto(a) Direção);
- Encarregado de Proteção de Dados;
- Responsável de Segurança;
- Coordenador(a) TIC;
- Técnico(a) Informática;
- Entre outros que assegurem a segurança da informação na instituição de ensino.

1

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Quais são os objetivos deste guia?

Os objetivos do guia são:

1. **Ajudar toda a comunidade Escolar** a proteger-se no espaço digital.
2. **Promover a consciencialização** e compreensão da cibersegurança a fim de assegurar a proteção da informação de cada Escola e a continuidade dos serviços e infraestrutura.
3. **Proporcionar conhecimentos** sobre os possíveis riscos e a adoção de boas práticas de segurança para reduzir a probabilidade de ciberataques, bem como minimizar os impactos que podem advir de um incidente de segurança.

Como está organizado o guia?

O Guia de Boas Práticas de Cibersegurança para as Escolas está segmentado em cinco secções, que servem de orientação para os **dirigentes** das instituições de ensino e os **gestores** e pessoal técnico responsável pelas Tecnologias de Informação e Comunicação (TIC) das instituições de ensino.

De seguida, é apresentado um sumário executivo, que contém a estrutura com os elementos que são abordados ao longo do documento.

2

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

SUMÁRIO EXECUTIVO

A tecnologia é uma realidade que faz parte de diversas áreas, tanto na vida profissional como na vida pessoal de cada um de nós. É indiscutível, que o desenvolvimento destas tecnologias está em constante evolução, vão continuar a surgir novos sistemas, novas plataformas, num mundo que vive intensamente a transformação digital.

Neste contexto, as instituições de ensino não são uma exceção. A transformação digital na educação é uma realidade que nos rodeia já há algum tempo, não só pela quantidade de sistemas digitais disponíveis no meio, mas também pelo interesse de toda a comunidade escolar em utilizar a tecnologia, privilegiando a qualidade, a acessibilidade e a simplicidade do acesso à informação.

Contudo, esta transformação digital impõe alguns desafios aos utilizadores e aos responsáveis pelas Tecnologias de Informação e Comunicação (TIC) na instituição de ensino, porque está a atrair cada vez mais cibercriminosos.

Este guia tem por finalidade consciencializar os decisores e responsáveis pelas soluções TIC das instituições de ensino que é necessário passar à ação, de modo a mitigar as principais vulnerabilidades dentro deste contexto. Em termos temáticos, o guia divide-se em cinco capítulos principais:

- "Cibersegurança, ameaças e impactos", onde se apresentam as definições bem como alguns dos tipos de ataques que provocaram mais problemas às organizações portuguesas no último ano;
- "A cibersegurança na Educação", através do qual é apresentada a composição do ecossistema existente nas instituições de ensino, a situação atual sobre a cibersegurança bem como os desafios que as instituições têm de enfrentar;
- "Legislação", engloba os conceitos afetos à governança e que se aplica às entidades e organismos da Administração Pública;
- "Recomendações e Boas Práticas", através do qual são apresentados alguns aspetos que as instituições de ensino podem ter em consideração para melhorar a sua presença no ciberespaço.

Por fim, são apresentadas as principais conclusões através de uma análise global e de um conjunto de destaques com os dados mais relevantes.

3

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

1. CIBERSEGURANÇA, AMEAÇAS E IMPACTOS

O que é a cibersegurança?

A Cibersegurança é uma área de atuação bastante ampla com aplicação não só limitada às tecnologias da informação, mas também à componente dos processos e das pessoas (utilizadores), uma vez que estes são também potenciais vetores de ataque e exploração de potenciais vulnerabilidades com técnicas, como por exemplo a Engenharia Social.

A cibersegurança pode ser definida 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.

A segurança da informação assenta sobre três pilares (Figura 10), habitualmente designados por CID (Confidencialidade, Integridade e Disponibilidade) ou CIA (Confidentiality, Integrity and Availability) em inglês, acrónimo que representa as três bases Confidencialidade, Integridade e Disponibilidade.

Quais os tipos de ataques e as suas consequências?

Um ataque cibernético é uma tentativa maliciosa e deliberada de um indivíduo ou grupo de indivíduos violarem o sistema de informação de outro indivíduo ou organização. Existem vários tipos de ataques cibernéticos [1], uns mais conhecidos do que outros, que têm como objetivo causar falhas no serviço, extorquir dinheiro, obter informações com motivações políticas, ou, em casos mais extremos, danificar sistemas com o pretexto de criar o pânico.

Deste modo, seguem abaixo, alguns dos ciberataques mais comuns que acontecem no dia a dia no ciberespaço.

4

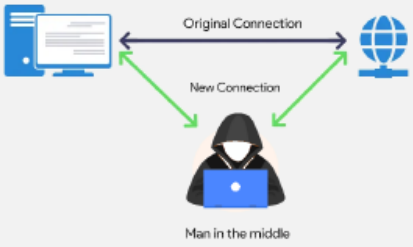
GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Malware - um malware, ou software malicioso, é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas [2]. Alguns dos exemplos são: Adware, Spyware, Vírus, Worms, Trojan, Ransomware, Rootkit, Keylogger, Criptomineração Maliciosa, Exploits, entre outros. Destes, os mais conhecidos são:

- **Trojan** (cavalo de tróia), parece que é algo útil de forma a enganar o utilizador, mas quando entra no sistema, consegue obter acesso não autorizado ao sistema em causa e roubar informações financeiras ou até instalar outras ameaças.
- **Ransomware**, bloqueia o acesso a um dispositivo e/ou cifra os ficheiros existentes no sistema e, normalmente, é exigido o pagamento de um resgate para a devolução da chave que foi utilizada para cifrar os dados. Atualmente, é a ameaça mais comum dos atacantes, uma vez que implica um pagamento em criptomoeda, cujo rasto é difícil de seguir.

Phishing - é um tipo de ataque onde são aplicadas técnicas de engenharia social para obter informação sensível de uma vítima através de um e-mail [3]. O atacante que utiliza este tipo de ataque procura ludibriar os recetores de e-mails para que estes disponibilizem informação sensível através do clique em anexos e/ou URL maliciosos ou da partilha de dados em páginas fraudulentas. Para o efeito, o atacante falseia uma marca credível ou representa alguém de confiança. Quando esta técnica é utilizada através de SMS, dá pelo nome de smishing e, por telefone (voz), de vishing.

Figura 1 - Ataque de Phishing



Man-In-The-Middle **(MITM)** - é um tipo de ataque de espionagem, em que o atacante interceta uma conversa existente ou transferência de dados. O atacante consegue infiltrar-se no meio da conversa/transferência, o atacante finge ser ambos participantes legítimos [4]. Isso permite que um atacante intercete informação e dados de qualquer uma das partes, ao mesmo tempo que envia links maliciosos ou outras informações a ambos os participantes legítimos.

5

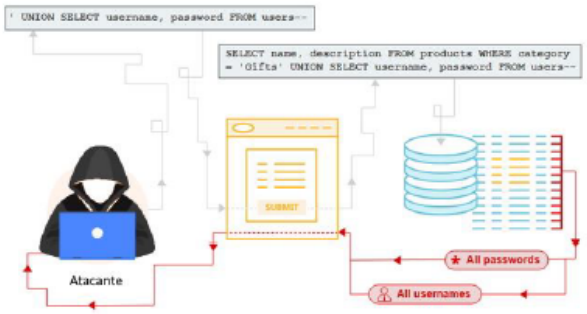
GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

***Distributed Denial-of-Service* (DDoS)** - um ataque distribuído de negação de serviço (DDoS) é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede, sobrecarregando o alvo ou a infraestrutura circundante com uma inundação de tráfego de dados [5]. Exemplos destes ataques são o Internet Control Message Protocol (ICMP) flodding (ou smurf attack ou ping of death), o atacante aproveita dispositivos de rede mal configurados e envia pacotes falsificados que executam ping aos computadores da rede de destino. Outro tipo é o SYN flodding, o atacante envia pacotes de SYN para várias portas, mas sem concluir o handshake do Transmission Control Protocol (TCP), fazendo com os que utilizadores legítimos tenham dificuldades no acesso. Um outro tipo é o ataque Denial-of-Service (DoS), em vez de serem várias fontes a realizar o ataque em simultâneo, é apenas uma fonte.

Figura 2 - Ataque de DDoS

Zero-day exploit - Uma exploração de dia zero (também designada por ameaça de dia zero) é um ataque que tira vantagem de uma vulnerabilidade de segurança, para a qual ainda não existe uma correção por parte do fabricante [6]. É chamada de ameaça de dia zero porque, uma vez descoberta a falha, o fabricante/organização tem zero dias para encontrar uma solução.

SQL injection - O SQL injection é uma falha de segurança que permite ao atacante consultar informação de uma ou várias bases de dados de uma determinada aplicação/sistema [7]. Nestes casos, o atacante pode modificar ou apagar informação da base dados, causando assim alterações persistentes no conteúdo ou comportamento da aplicação/sistema.



6

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

De seguida são apresentados os ciberataques que causaram mais problemas às organizações, em Portugal, no ano de 2023 [8].

Negação de Serviço Distribuído

O Distributed Denial-of-Service (DDoS) é uma das ciberameaças mais impactantes, causando indisponibilidade dos serviços ou diminuindo o seu desempenho. No ano de 2023, verificou-se que a utilização de Botnets fez aumentar o número de ataques de negação de serviço como também a sua volumetria. Neste mesmo ano, foi reportado o maior ataque DDoS de que há registo, tendo tido como alvo os serviços da Google.

Ransomware

No ano de 2023, verificou-se um crescimento da oferta de serviços do tipo Ransomware-as-a-Service (RaaS). Este modelo de negócio, tornou-se particularmente lucrativo e os grupos cibercriminosos têm-se dedicado cada vez mais a esta atividade tornando este tipo de serviços cada vez mais acessível a qualquer pessoa. Neste mesmo ano, assistiu-se ao uso de uma nova tática de extorsão, onde o ator malicioso ameaça reportar a vítima através das diligências legais, após a mesma ter sido comprometida e não ter reportado às autoridades competentes que tinha sido algo de ataque.

Engenharia Social

A engenharia social foi a técnica de ataque que predominou no ano de 2023. A utilização destas técnicas explora o interesse, a curiosidade, a preocupação e o medo das pessoas, principalmente através da conta de e-mail, para obter informação confidencial, como por exemplo credenciais de acesso. Esta é a técnica favorita dos atores maliciosos para o acesso inicial aos sistemas internos das organizações. Infelizmente, muitos e-mails com conteúdo malicioso, especialmente URLs, ainda passam por mecanismos básicos de segurança de filtragem de e-mails e acabam por ser entregues aos utilizadores.

Tentativa de Login

A tentativa de login continuou a ser um dos ataques mais comuns no ano de 2023. As tentativas de login/ataques de força bruta utilizam a técnica de tentativa e erro para adivinhar a palavra-passe da vítima. Os cibercriminosos utilizam todas as combinações possíveis para obter acesso à conta em questão.

7

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

2. A CIBERSEGURANÇA NA EDUCAÇÃO

As novas tecnologias estão cada vez mais presentes nas instituições de ensino. Contudo, esta transformação digital está a atrair cada vez mais cibercriminosos.

De acordo com o último relatório de segurança da CheckPoint, referente ao ano 2023, os setores da educação, governo e saúde continuam a ser os principais alvos de ataques cibernéticos, conforme é possível verificar na Figura 3. O setor da educação/investigação continua a ser o setor mais afetado a nível mundial, com uma média de 2046 tentativas de ataque semanalmente.

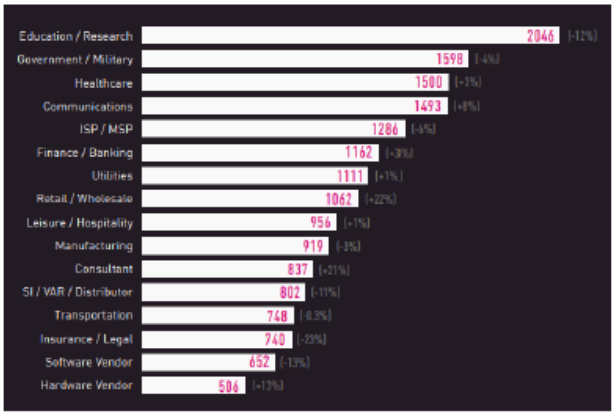


Figura 3 - Média global de ataques semanais por setor em 2023
Fonte: CheckPoint

De acordo com os últimos dados disponibilizados pela Direção-Geral da Educação, apenas 106 Agrupamentos de Escolas (AE)/Escolas Não Agrupadas (ENA) dos 486, obtiveram uma certificação europeia com o Selo de Segurança [9], ou seja, apenas 21,81% das instituições de ensino (AE e ENA) estão a adotar estratégias de sensibilização para uma utilização segura e crítica da tecnologia e dos ambientes digitais.

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Ecossistema de uma instituição de ensino cibersegura

O ecossistema de uma instituição de ensino, no âmbito da cibersegurança, é composto por:

- utentes como beneficiários dos serviços e equipamentos;
- plataformas e redes de comunicação que permitem a circulação da informação;
- infraestrutura tecnológica que sustenta toda a atividade da instituição de ensino;
- dispositivos conectados (*Internet of Things - IoT*) e toda a informação gerada e transmitida por estes;
- capacidade de cibersegurança para a proteção dos seus ativos, ou seja, uma solução que protege todos estes elementos.

Qualquer utente da instituição de ensino que tenha acesso a um equipamento (computador e/ou tablet) com sistema de email ou acesso à internet poderá, através de práticas negligentes, infetar toda ou parte da rede interna da instituição com software malicioso. Esta infeção poderá resultar em perda de dados confidenciais, interrupção dos serviços e, claro, prejuízos reputacionais para a instituição de ensino.

9

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

3. LEGISLAÇÃO, REGULAMENTOS E NORMAS

O Regime Jurídico da Segurança do Ciberespaço aplica-se aos estabelecimentos públicos de ensino?

Sim, aplica-se!

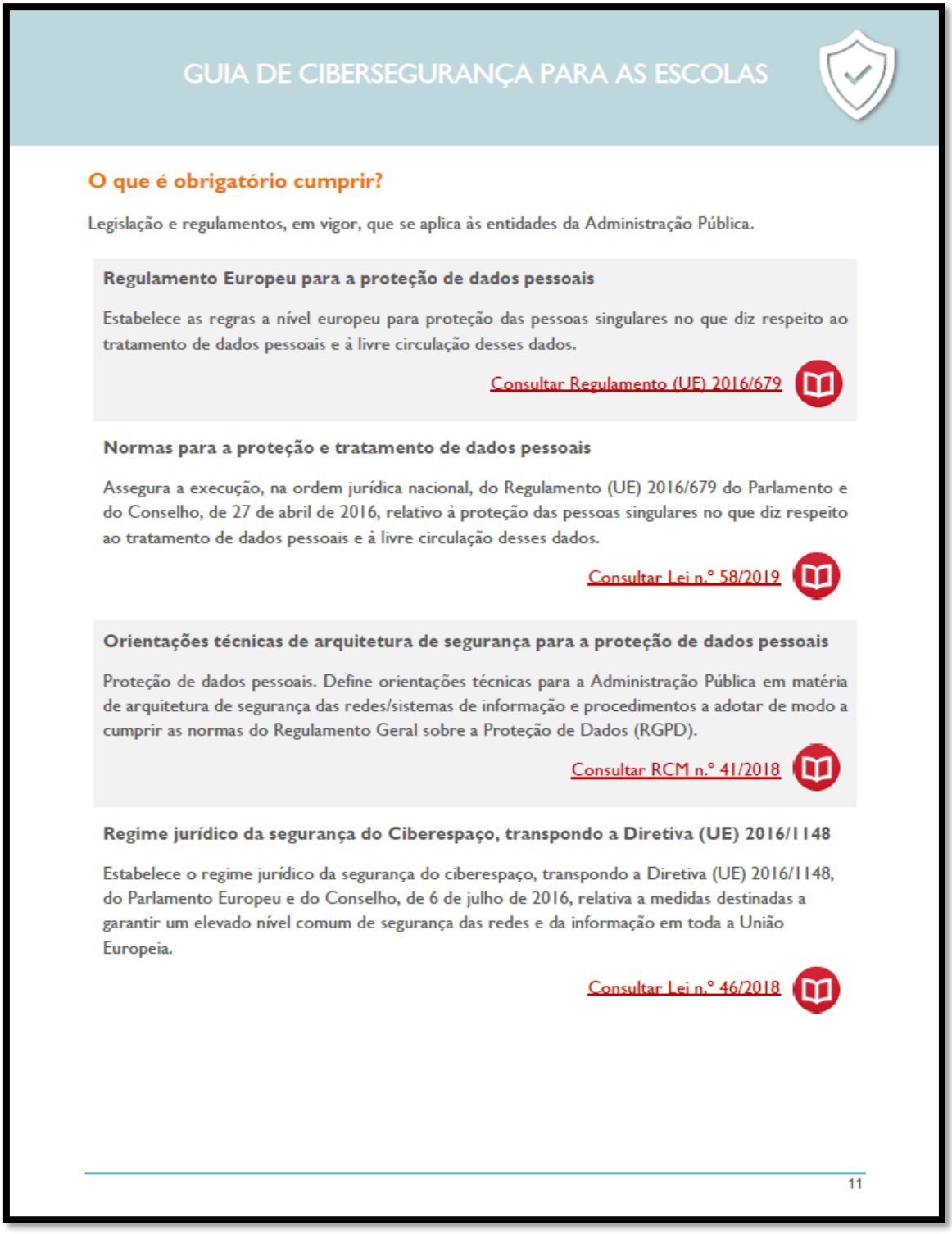
Nos termos previstos na alínea a) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto [10], que estabelece o Regime Jurídico da Segurança do Ciberespaço, encontra-se abrangida pelo âmbito de aplicação deste regime jurídico a Administração Pública.

A tipologia de entidades no âmbito de aplicação do Decreto-Lei n.º 65/2021, de 30 de julho [11], que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 [12] do Parlamento Europeu, de 17 de abril de 2019, consta do n.º 1 do artigo 2.º do referido normativo o qual remete para as alíneas a) a d) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto.

Nos termos do artigo 75.º da Constituição da República Portuguesa, o Estado cria uma rede de estabelecimentos públicos de ensino. De acordo com o enquadramento estabelecido na Lei n.º 46/86, de 14 de outubro, que estabelece a Lei de Bases do Sistema Educativo, respetivamente no artigo 40.º, e nos termos previstos no n.º 1 do artigo 6.º do Decreto-Lei n.º 75/2008, de 22 de abril [13], que aprova o regime de autonomia, administração e gestão dos estabelecimentos públicos da educação pré-escolar e dos ensinos básico e secundário, o agrupamento de escolas é uma unidade organizacional, dotada de órgãos próprios de administração e gestão, constituída por estabelecimentos de educação pré-escolar e escolas de um ou mais níveis e ciclos de ensino.

A Administração Pública integra os agrupamentos de escolas, no âmbito do Ministério da Educação e da Direção-Geral dos Estabelecimentos Escolares, como rede pública de estabelecimentos de ensino, ficando por isso no âmbito de aplicação da Lei 46/2018, de 13 de agosto, e do Decreto-Lei n.º 65/2021, de 30 de julho.

10



GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

O que é obrigatório cumprir?

Legislação e regulamentos, em vigor, que se aplica às entidades da Administração Pública.

Regulamento Europeu para a proteção de dados pessoais

Estabelece as regras a nível europeu para proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Consultar Regulamento (UE) 2016/679

Normas para a proteção e tratamento de dados pessoais

Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Consultar Lei n.º 58/2019

Orientações técnicas de arquitetura de segurança para a proteção de dados pessoais

Proteção de dados pessoais. Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes/sistemas de informação e procedimentos a adotar de modo a cumprir as normas do Regulamento Geral sobre a Proteção de Dados (RGPD).

Consultar RCM n.º 41/2018

Regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148

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.

Consultar Lei n.º 46/2018

11

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Decreto-Lei n.º 65/2021, de 30 de julho

Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019. Este normativo define de forma transversal as obrigações relativas a requisitos de segurança e notificação de incidentes. Determina também as competências do CNCS como ANCC – Autoridade Nacional de Certificação em Cibersegurança e estabelece um regime sancionatório para a matéria da certificação e acrescentou um número alargado de obrigações à Administração Pública, com destaque:

- Nomeação de um Responsável de Segurança;
- Identificação dos contactos permanentes;
- Existência de um plano de segurança formal;
- Notificação regular da lista de ativos;
- Realização de avaliações do risco dos ativos;
- Notificação de incidentes;
- Relatório anual.

Consultar Lei n.º 65/2021

Regulamento n.º 183/2022, de 21 de fevereiro

Regulamento que configura instrução técnica relativa à comunicação e informação para cumprimento das obrigações decorrentes do Regime Jurídico da Segurança do Ciberespaço referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes. Este regime jurídico 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. No Regulamento 183/2022 é possível encontrar os métodos de contacto e a estrutura da informação a ser enviada.

Consultar Lei n.º 183/2022

12

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Quais são as normas de cibersegurança mais populares?

Algumas das *frameworks* de cibersegurança que podem ser adotadas pelas instituições de ensino para melhorarem a sua presença no ciberespaço.

ISO/IEC 27001

A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados de acordo com as necessidades.

Para mais detalhes, consulte a página www.27001.pt

NIST Cybersecurity Framework 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. A versão mais recente da *framework* da NIST (CSF 2.0) apresenta 6 funções (governar, identificar, proteger, detetar, responder e recuperar) com uma subdivisão em 22 categorias. Para cada categoria existem outras subcategorias com uma variedade de controlos.

Para mais detalhes, consulte a página www.nist.gov/cyberframework

COBIT (Control Objectives for Information and Related Technologies)

Da responsabilidade do ISACA, o COBIT é um referencial de boas práticas para a governação das TIC. Ajuda as organizações a criar valor a partir das TIC e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações.

Para mais detalhes, consulte a página www.isaca.org/resources/cobit

CIS Controls Framework

Center for Internet Security Critical Security Controls (CIS Controls) disponibilizou a 18 de maio de 2021, o CIS Control V8, com um conjunto de diretrizes para as organizações melhorarem a segurança dos seus sistemas. Este conjunto de 18 controlos críticos de segurança do CIS fornecem uma estratégia abrangente para proteger os sistemas e redes contra uma variedade de ameaças cibernéticas.

Para descarregar a *framework*, aceda a learn.cisecurity.org/cis-controls-download

13

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Quadro Nacional de Referência para a Cibersegurança (QNRCS)

A segurança do ecossistema de informação depende de todos os seus componentes tecnológicos, das pessoas e dos processos/procedimentos. Neste contexto o Quadro Nacional de Referência para a Cibersegurança (QNRCS) propõe um conjunto de boas práticas/medidas de segurança, concretizadas em exemplos de implementações tecnológicas, processuais ou outras. Estão agrupadas em cinco objetivos de segurança (ver Tabela 1): Identificar, Proteger, Detetar, Responder e Recuperar, com uma ou mais categorias e subcategorias [14]. São identificadas 102 medidas de segurança que abrangem todo o ecossistema de um sistema de informação, do conjunto das quais identificámos as mais relevantes no domínio dos equipamentos/dispositivos (computadores, tablets, impressoras, multifuncionais, smartphones, etc.).

OBJETIVO	DESCRIÇÃO
IDENTIFICAR	Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes. Esta compreensão permite que a organização consiga definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco.
PROTEGER	Implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia.
DETETAR	Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação.
RESPONDER	Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos.
RECUPERAR	Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. E que, no caso de existência de um incidente, a organização consiga utilizar as medidas para suporte à recuperação em tempo útil da sua atividade.

Tabela 1 - Objetivos de Segurança

14

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

4. RECOMENDAÇÕES E BOAS PRÁTICAS

Neste capítulo são apresentadas algumas das recomendações e boas práticas que podem ser adotadas pelas instituições de ensino para melhorarem a sua presença no ciberespaço.

#1 SENSIBILIZAR TODA A COMUNIDADE ESCOLAR

Sensibilizar a comunidade escolar (incluindo pais e encarregados de educação) para a adoção das boas práticas de cibersegurança, de modo a aumentar a resiliência da instituição de ensino relativamente às ameaças no ciberespaço. As questões de segurança digital são responsabilidade de todos e, para isso, é necessário sensibilizar toda a comunidade.

Aos funcionários (docentes e não docentes) e colaboradores deve ser ministrada formação mínima no domínio de práticas básicas de segurança da informação e comportamento defensivo.

Abaixo seguem algumas das recomendações do CNCS, literacia e cursos gratuitos, que podem ser divulgados junto da comunidade escolar para promover o conhecimento sobre a cibersegurança.

Sensibilização para adoção de boas práticas
https://dyn.cncs.gov.pt/pt/boaspraticas/

Guia para campanha de sensibilização em 5 passos
https://www.cncs.gov.pt/pt/guia-para-realizar-uma-campanha-de-sensibilizacao/

C-Academy, cursos em formato de e-Learning (MOOCs)
https://www.cncs.gov.pt/pt/cursos-e-learning/

- Cidadão Cibersocial
  https://www.nau.edu.pt/pt/curso/cidadao-cibersocial/
- Cidadão Ciberseguro
  https://www.nau.edu.pt/pt/curso/cidadao-ciberseguro/
- Consumidor Ciberseguro
  https://www.nau.edu.pt/pt/curso/consumidor-ciberseguro/
- Cidadão Ciberinformado
  https://www.nau.edu.pt/pt/curso/cidadao-ciberinformado/

15

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#2 REDIGIR NORMATIVOS SOBRE A CIBERSEGURANÇA

Devem ser definidos normativos, com o objetivo de regular a cibersegurança e a segurança de informação. Estes documentos devem, no mínimo, contemplar os requisitos básicos de segurança da informação na instituição de ensino. Devem, igualmente, ser redigidos numa linguagem acessível, tendo em conta que todos os funcionários (docentes e não docentes) da instituição de ensino devem ter conhecimento dos mesmos. Alguns dos normativos que devem ser do conhecimento da comunidade escolar:

- Política de Segurança Digital: orientações para o uso da internet e dos dispositivos digitais em segurança e como recurso educativo;
- Política de Privacidade e Proteção de Dados;
- Política de Utilização Aceitável (PUA) das TIC – Alunos
- Política de Utilização Aceitável (PUA) das TIC – Docentes
- Política de Utilização Aceitável (PUA) das TIC – Não Docentes

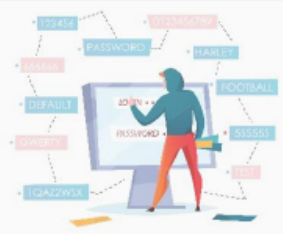
#3 CRIAR PALAVRAS-PASSE FORTES

Quanto mais robusta for a palavra-passe, mais resistente se torna a ataques de força bruta. Crie palavra-passes com, pelo menos, 14 carateres e inclua uma combinação de letras maiúsculas e minúsculas, números e símbolos, se permitido. Uma boa forma de o fazer é criar uma frase de código – utilize uma frase que inclua palavras invulgares ou palavras de diferentes línguas. Além disso, atribua sempre senhas únicas a todas as suas contas online.

O site "Have I been pwned" é um recurso gratuito para qualquer utilizador avaliar rapidamente se as suas credenciais de acesso às plataformas digitais, foram comprometidas ou "exploradas" numa violação de dados.

Verifique se o seu email consta em alguma lista negra
haveibeenpwned.com

Verifique se as suas palavras-passe constam na lista negra
haveibeenpwned.com/Passwords



16

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#4 ATIVAR A AUTENTICAÇÃO MULTIFATOR (MFA)

A autenticação multifator é uma medida de segurança que protege o utilizador e a própria instituição de ensino, exigindo que os utilizadores forneçam dois ou mais fatores de autenticação para aceder a informação confidencial que está alojada nas Tecnologias da Informação (TI), como aplicações, websites, email, entre outros. Esta autenticação adiciona camadas extra de segurança, com o objetivo de dificultar a atividade dos cibercriminosos, uma vez que as palavras-passe podem ser fracas, roubadas, expostas ou vendidas por terceiros. O utilizador apenas conseguirá aceder à informação se apresentar com sucesso duas ou mais provas (ou fatores) de autenticação.

Estes fatores são:

- Conhecimento: algo que só o utilizador sabe. (por exemplo, palavra-passe);
- Posse: algo que só o utilizador tem. (por exemplo, telemóvel);
- Inerência: algo que só o utilizador é. (por exemplo, impressão digital).

#5 UTILIZAR UM GESTOR DE PALAVRAS-PASSE

Um gestor de palavras-passe é uma forma conveniente e segura de proteger as credenciais de acesso. O gestor permite criar palavras-passe fortes e mantêm-nas em segurança. Sempre que possível a base dados do gestor de palavras-passe deve ser armazenada localmente e deve ser evitado o alojamento na *cloud*. Existem vários gestores de palavras-passe, uns Gratuitos (**G**) e outros Pagos (**P**). **Alguns dos gestores de palavras-passe:**

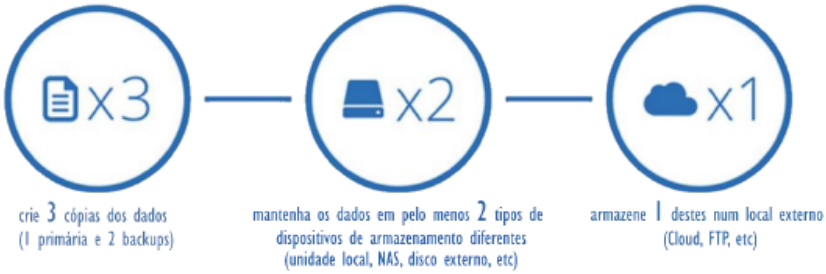
- KeePass/KeePassXC (**G**)
- LastPass (**G**, plano pessoal)
- NordPass (**G**, plano pessoal)
- Bitwarden (**G**, plano pessoal)
- Dashlane (**P**)
- 1Password (**P**)
- Enpass (**P**)
- Keeper (**P**)

17

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#6 A IMPORTÂNCIA DOS BACKUPS

Para proteger os dados de ataques de *ransomware*, é importante criar e manter uma estratégia de cópias de segurança robusta. A regra 3-2-1 aumenta consideravelmente as possibilidades de recuperação de dados perdidos ou corrompidos.



O 3 significa que devem ser realizadas três cópias de qualquer arquivo. O 2 indica que as cópias devem ser mantidas em dois tipos de armazenamentos diferentes. E o 1 significa que uma das cópias deve ser armazenada num local externo, para evitar que um ataque de *ransomware* a possa afetar.

Outras recomendações:

- Submeter as cópias de segurança periodicamente a testes de integridade e recuperação;
- Cifrar as cópias de segurança para garantir a confidencialidade, só o utilizador com acesso à chave que foi utilizada para cifrar os dados terá acesso à informação protegida;
- Realizar cópias de segurança das configurações dos sistemas críticos;
- Automatizar os sistemas de cópias de segurança e recuperação, garantindo a eficiência e solidez do seu funcionamento;
- Realizar regularmente cópias de segurança da informação crítica para suportes *offline*. De preferência, devem ser realizados backups totais para aumentar a possibilidade de recuperação total dos dados.

18

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#7 IMPLEMENTAR SISTEMA CENTRALIZADO DE MONITORIZAÇÃO DE LOGS

A monitorização de *logs* de sistema é de extrema importância na gestão da segurança de sistemas de informação. Os *logs* são registos detalhados de atividades que ocorrem em sistemas, redes, aplicações e dispositivos. Para uma visão centralizada dos *logs* é recomendado a utilização de uma plataforma de Gestão de Informações e Eventos de Segurança, em inglês Security Information and Event Management (SIEM). Estas plataformas permitem recolher e processar um grande volume de dados e detetar possíveis incidentes e iniciar uma resposta rápida a ameaças, assim como estar em conformidade com requisitos regulatórios.

Alguns dos dados que é importante recolher, pelo menos dos sistemas mais críticos:

- Tipo de evento;
- Identificação do utilizador;
- Protocolo de comunicação;
- Data, hora e fuso horário;
- URL;
- IP de origem e destino;
- Porto de origem e destino;
- Código de sucesso ou falha;

Esta informação permitirá não só identificar ataques ou tentativas de ataques, mas também diagnosticar eventuais problemas nos sistemas. Deverão ser consideradas as obrigações legais quanto ao cumprimento do Regulamento Geral de Proteção de Dados (RGPD).

Plataforma SIEM gratuitas: Elasticsearch, Wazuh, OSSIM, OSSEC, Sagan, Splunk Free, Snort, ELK Stack, entre outras.

#8 MANTER OS SISTEMAS ATUALIZADOS

Com uma boa política de atualizações é possível evitar muitos incidentes de segurança. Não é recomendado utilizar equipamentos com sistemas operativos descontinuados porque os fabricantes deixaram de disponibilizar atualizações de segurança para corrigir vulnerabilidades que, entretanto, foram identificadas. Daqui podem resultar perdas de dados confidenciais, interrupção dos serviços e, claro, prejuízos reputacionais para a instituição de ensino.

19

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

QUAL A DIFERENÇA ENTRE A ANÁLISE DE VULNERABILIDADES E O *PENTEST*?

Primeiramente uma vulnerabilidade é um ponto fraco presente num ativo ou num controlo que pode ser explorado por uma ameaça. Podem potencialmente causar um incidente indesejado, que pode originar danos a um sistema, indivíduo ou organização.

A análise de vulnerabilidade pode ser definida como o processo de avaliação e identificação de falhas e potenciais ameaças à segurança de uma infraestrutura tecnológica. Assim, o resultado da avaliação será uma lista com as principais ameaças, organizadas de acordo com a gravidade ou criticidade em relação ao negócio da organização.

Já o *Pentest* (teste de intrusão), envolve o processo de identificação da vulnerabilidade juntamente com a tentativa de explorá-la e simular um ataque real. O objetivo é testar os mecanismos de defesa dos sistemas e mapear os possíveis caminhos que um possível atacante iria seguir.

Uma das principais diferenças entre a análise de vulnerabilidade e o *pentest* está na relação entre a abrangência e a profundidade. Sendo a primeira mais ampla e procura identificar o maior número de riscos possíveis, sem necessariamente analisar a fundo cada um destes riscos.

#9 IDENTIFICAR E MITIGAR VULNERABILIDADES NOS SISTEMAS

As instituições de ensino devem assumir uma postura mais proativa no domínio da identificação, avaliação, priorização e mitigação de vulnerabilidades de software e sistema que podem ser exploradas por atacantes. O objetivo é reduzir o risco de um ciberataque bem-sucedido e manter a informação confidencial segura.

O Catálogo de Vulnerabilidades pode ser utilizado durante o processo de avaliação das vulnerabilidades, e está disponível para consulta no Anexo B do Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança do CNCS.

Algumas das soluções tecnológicas para realizar a análise de vulnerabilidades:

- OpenVAS
- Nessus Vulnerability Scanner
- Nikto
- Shodan
- Entre outros

20

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#10 REALIZAR TESTES DE INTRUSÃO (*PENTEST*)

O *Pentest* é um tipo de avaliação de segurança que envolve a simulação de um ataque cibernético a um sistema, rede ou aplicação web para identificar falhas e avaliar a segurança de um sistema, além de medir a maturidade de segurança da instituição de ensino. Os tipos mais comuns de testes de intrusão, são:

- ***Pentest* externo**: este tipo de teste concentra-se no ataque aos sistemas e infraestrutura externa da instituição. Alguns dos exemplos será o website institucional, o moodle, e as restantes soluções expostas ao público (internet);
- ***Pentest* interno**: este tipo de teste simula um ataque dentro da rede da instituição, para avaliar se os sistemas internos têm falhas nas suas configurações;
- ***Pentest* em Aplicações da Web**: este tipo de teste tem por objetivo explorar as aplicações web da instituição, como formulários online, páginas de login e outros elementos interativos.
- ***Pentest* a redes sem fios (Wi-Fi)**: este tipo de teste concentra-se em atacar as redes sem fios da instituição, como pontos de acesso Wi-Fi e dispositivos Bluetooth;
- ***Pentest* de rede**: este tipo de teste explora a infraestrutura de rede da instituição, como *routers*, *switches* e *firewalls*.

Os testes de intrusão devem ser executados apenas por profissionais de cibersegurança, pois requer conhecimento avançado, sendo também necessária uma autorização prévia da instituição.

#11 CONTROLAR ADEQUADAMENTE A SEGURANÇA DOS FORNECEDORES

É comum as instituições de ensino recorrerem à subcontratação de serviços de manutenção para os seus sistemas informáticos, pelo que é necessário tomar providências, em sede contratual, junto dos seus fornecedores de Tecnologias de Informação (TI), no sentido de assegurar:

- Cláusulas de confidencialidade;
- A transferência do risco. é necessário atribuir responsabilidades ao fornecedor e aplicar consequências;
- Que as políticas internas também são respeitadas pelos fornecedores, para não comprometer a segurança;
- O Acordo de Nível de Serviço (SLA), assegurando que os serviços contratados são prestados no período acordado.

21

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#12 CONTROLO DE ACESSOS AOS SISTEMAS INFORMÁTICOS

O reforço das medidas de controlo de acesso aos sistemas de informação é algo urgente e deve considerar os utilizadores internos (docentes e não docentes) como os externos (técnicos de informática, fornecedores, entre outros), bem como os utilizadores da instituição de ensino com privilégios máximos, nomeadamente os elementos da direção.

Algumas das recomendações a considerar são:

- Realizar uma correta gestão de palavras-passe;
- Não utilizar contas partilhadas entre utilizadores;
- Restrição de acesso a determinadas redes (VLANs) internas;
- Exigir aos utilizadores a ativação da Autenticação de Multifator (MFA);
- Atribuir privilégios de administração apenas a quem efetivamente necessita;
- Se necessário, os acessos do exterior à rede privada devem ser realizados com recurso a uma VPN (Rede Privada Virtual);
- Restringir o acesso físico a zonas onde se encontram os ativos críticos informáticos vitais para a instituição de ensino.

#13 NOMEAR OS RESPONSÁVEIS PELA SEGURANÇA DA INFORMAÇÃO

Na instituição de ensino deverá existir pelo menos um responsável pela segurança da informação e cabe a este adotar as medidas técnicas e organizacionais que garantam a:

- Salvaguarda das propriedades da informação, designadamente, a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio;
- Segurança com o tratamento de dados, de modo a prevenir-se contra acessos não autorizados, divulgação não autorizada, modificação, remoção ou eliminação dos dados pessoais.
- Comunicação de incidentes ao CNCS e às restantes entidades competentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto-Lei n.º 65/2021, de 30 de julho [11].

22

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#14 CRIAR E MANTER ATUALIZADO O INVENTÁRIO DOS ATIVOS

Nos termos do n.º 1 do artigo 4.º no Regulamento n.º 183/2022, de 21 de fevereiro [15], entende -se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços. Para cada ativo identificado de acordo com o n.º 1 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho [11], aplica-se o seguinte:

A entidade deve elaborar o inventário dos seus equipamentos de acordo com as seguintes regras:

- Os dispositivos físicos e sistemas devem ser inventariados com a seguinte informação: Número de inventário; Nome e modelo do equipamento; Número de série; e Localização.
- Os dispositivos ligados à rede devem ter a seguinte informação complementar: Endereço IP; e Endereço de hardware.
- Os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, os seguintes elementos: Nome; Contacto; e Departamento.
- Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade para a entidade.

A entidade deve efetuar o inventário de todas as suas aplicações, identificando:

- Informação necessária ao inventário de uma aplicação, nomeadamente: Nome do software; Versão; e Fabricante.
- Os responsáveis pelas aplicações com, pelo menos, os seguintes elementos: Nome; Contacto; e Departamento.
- A classificação em função da criticidade da aplicação para a entidade;
- Quando aplicável, o tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de software.

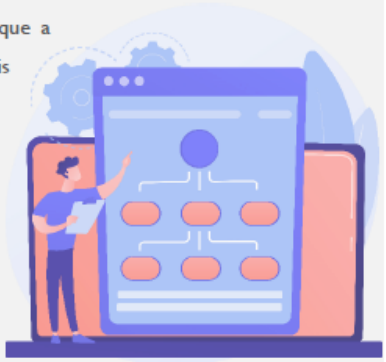
23

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#15 CRIAR E EXECUTAR UM PLANO DE RESPOSTA A CIBERINCIDENTES

Os responsáveis pela instituição de ensino precisam de saber como responder a incidentes de segurança, e como recuperar caso ocorram eventos adversos.

O Plano de Resposta a Incidentes (PRI) deve definir o que a instituição de ensino terá de realizar antes, durante e depois de um incidente de segurança. Este plano deve também incluir quais as funções e responsabilidades dos envolvidos para responder a um incidente.



O PRI deve ser aprovado pelo diretor da instituição de ensino e todos os envolvidos no processo de resposta a incidentes devem ter conhecimento do mesmo. Para uma resposta eficaz o plano deve manter-se sempre atualizado.

As lições aprendidas com os incidentes reais e simulacros permitirão que a instituição de ensino atualize e reforce o seu PRI, bem como as suas políticas, procedimentos e até tecnologias.

#16 CRIAR E EXECUTAR UM PLANO DE AUDITORIAS À SEGURANÇA

As instituições de ensino devem estabelecer um plano de auditorias à segurança dos sistemas considerados mais críticos para avaliar se os processos, princípios e políticas de cibersegurança estão a ser cumpridos. Existem diversas *frameworks* de Cibersegurança que podem auxiliar, nomeadamente:

- ISO/IEC 27001;
- *Framework* de Cibersegurança do Instituto Nacional de Padrões e Tecnologia Norte-Americano (NIST CSF);
- Controlos do Centro de Segurança para a Internet (CIS);
- Quadro Nacional de Referência para a Cibersegurança (QNRCS).

24

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

#17 PROTEGER TODA A INFRAESTRUTURA TECNOLÓGICA

Adotar medidas proativas pode ajudar a proteger adequadamente a infraestrutura tecnológica (equipamentos e sistemas). Seguem algumas das medidas que podem ser adotadas:

- Controlo do acesso à/da Internet - os sistemas internos que estão expostos aos perigos da Internet, podem ser limitados com a configuração de um proxy, permitindo assim a aplicação de medidas restritivas de acesso;
- Configurações e acessos por omissão - para aumentar a robustez das configurações dos equipamentos e sistemas os serviços desnecessários devem ser desativados e as contas de utilizadores por *default* devem ser eliminadas;
- Proteção dos equipamentos terminais - para aumentar a segurança é recomendado instalar e manter atualizado os sistemas de deteção de intrusão, como antivírus, o IDS (Intrusion Detection System), o IPS (Intrusion Prevention System) e o HIDS (Host-based Intrusion Detection System).
- Sistemas descontinuados - Desativar por completo os equipamentos que têm sistemas operativos descontinuados pelo fabricante para garantir que não comprometem a restante infraestrutura tecnológica. Se necessário estes equipamentos apenas deverão ser ligados num ambiente isolado.
- Definição de uma política BYOD (Bring Your Own Device) – nos casos em que os utilizadores utilizam os seus próprios dispositivos para acederem aos recursos tecnológicos disponibilizados pela instituição de ensino, devem ter conhecimento e aceitar a política BYOD.

25

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

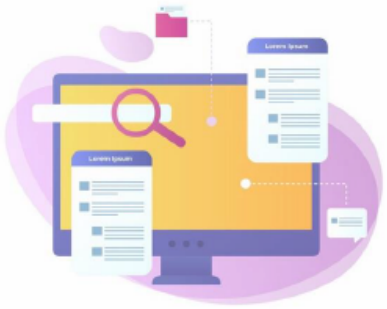
#18 PROTEGER OS DOMÍNIOS (*Registrars*)

Implementar os principais *standards* de segurança nas vertentes **web** e **email** para melhorar a presença da instituição de ensino no ciberespaço.

O serviço de email continua a ser um dos serviços internet mais utilizados nos contextos de uso pessoal, institucional e empresarial. No entanto, o mesmo foi concebido numa lógica de garantia da entrega das mensagens (disponibilidade), mas sem as preocupações de segurança quer com a integridade do conteúdo, quer com a autenticidade do remetente. De facto, o serviço de email é utilizado de forma abusiva diariamente, seja para envio massivo de mensagens não solicitadas, vulgo SPAM, seja para envio de mensagens com remetente falsificado.

Para fazer face a estes e outros problemas, a indústria, através do Internet Engineering Task Force (IETF), tem vindo a promover a adoção de um conjunto de instrumentos com vista a melhorar a segurança do popular serviço de email, de entre os quais se destacam o Sender Policy Framework (SPF), o DomaimKeys Identified Mail (DKIM) e o Domain-based Message Authentication, Reporting and Conformance (DMARC).

Recomenda-se que sejam adotados os standards **SPF**, **DKIM** e **DMARC** em todos os domínios da instituição de ensino.



Para mais detalhes sobre SPF, DKIM e DMARC, consulte a página cncs.gov.pt/pt/recomendacoes-tecnicas/

Onde verificar os domínios das plataformas digitais da Instituição de Ensino: webcheck.pt

26

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

COMO REPORTAR UM INCIDENTE?

Para reportar um incidente ou um cibercrime, utilize os seguintes contactos:

- CERT.PT (CNCS)
- Polícia Judiciária unc3t@pj.pt
- Procuradoria-Geral da República cibercrime@pgr.pt

Qualquer incidente deve ser reportado através do formulário online disponibilizado pelo CNCS

https://www.cncs.gov.pt/pt/notificacao-incidentes/

Caso a entidade não tenha a possibilidade de preencher o formulário online, ou se depare com a indisponibilidade deste, a notificação poderá ser efetuada, a título excecional, através dos seguintes contactos:

- cert@cert.pt;
- (+351) 210 497 399;
- (+351) 910 599 284 (24/7)

A notificação de incidentes ao Centro Nacional de Cibersegurança não se substitui à comunicação à autoridade judiciária ou ao órgão de polícia criminal competente quando esses incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.

27

5. CONCLUSÕES

As ameaças cibernéticas são uma realidade atual, que estão às portas de todas as instituições de ensino, à espreita de qualquer vulnerabilidade humana ou tecnológica. Não existem sistemas 100% seguros, porém são muitas as medidas que podem ser adotadas, em cada estabelecimento de ensino, para aumentarem o seu nível de proteção face aos desafios de segurança atuais. É verdade que não chega apenas implementar medidas tecnológicas, é necessário envolver as pessoas para que exista uma vontade inequívoca e um compromisso por parte de toda a comunidade escolar, bem como das empresas que fornecem e prestam serviços às instituições de ensino.

Com este guia, é possível aceder a um conjunto de recurso que visam disponibilizar as bases de conhecimento sobre o tema cibersegurança, muito direcionado ao ensino, mas também são elencadas algumas das recomendações e boas práticas que podem ajudar os responsáveis pelas Tecnologias da Informação e Comunicação (TIC) da instituição de ensino a proteger e a tornas os seus ambientes digitais mais resilientes.

6. REFERÊNCIAS

[1] H. Ahmetoglu e R. Das, «A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions», *Internet Things*, vol. 20, p. 100615, nov. 2022, doi: 10.1016/j.iot.2022.100615

[2] E. Gandotra, D. Bansal, e S. Sofat, «Malware Analysis and Classification: A Survey», *J. Inf. Secur.*, vol. 05, n.º 02, pp. 56–64, 2014, doi: 10.4236/jis.2014.52006

[3] Z. Alkhalil, C. Hewage, L. Nawaf, e I. Khan, «Phishing Attacks: A Recent Comprehensive Study and a New Anatomy», *Front. Comput. Sci.*, vol. 3, 2021, Disponível em: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060. [Acedido: 31 de janeiro de 2024]

[4] D. Javeed, U. Mohammedbadamasi, C. Ndubuisi, F. Soomro, e M. Asif, *Man in the Middle Attacks: Analysis, Motivation and Prevention*. 2020. doi: 10.13140/RG.2.2.22752.81928

[5] A. B. de Neira, B. Kantarci, e M. Nogueira, «Distributed denial of service attack prediction: Challenges, open issues and opportunities», *Comput. Netw.*, vol. 222, p. 109553, fev. 2023, doi: 10.1016/j.comnet.2022.109553

[6] R. Ahmad, I. Alsmadi, W. Alhamdani, e L. Tawalbeh, «Zero-day attack detection: a systematic literature review», *Artif. Intell. Rev.*, vol. 56, n.º 10, pp. 10733–10811, out. 2023, doi: 10.1007/s10462-023-10437-z

[7] V. Abdullayev e Dr. A. S. Chauhan, «SQL Injection Attack: Quick View», *Mesopotamian J. Cyber Secur.*, pp. 30–34, fev. 2023, doi: 10.58496/MJCS/2023/006

[8]. PT, «Relatório Anual PTSOC 2023», *PTSOC - Centro de Operações de Segurança do .PT*, 6 de fevereiro de 2024. Disponível em: https://ptsoc.pt.pt/pt/relatorio-anual-ptsoc-2023/. [Acedido: 6 de março de 2024]

[9] «Selo de Segurança Digital (eSafety Label) 2022 - Escolas Certificadas | Direção-Geral da Educação». Disponível em: https://www.dge.mec.pt/noticias/selo-de-seguranca-digital-esafety-label-2022-escolas-certificadas. [Acedido: 4 de março de 2024]

[10] «Lei n.º 46/2018 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384. [Acedido: 31 de janeiro de 2024]

[11] «Decreto-Lei n.º 65/2021 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988. [Acedido: 31 de janeiro de 2024]

[12] «Regulamento (UE) 2019/ do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança)».

[13] «Decreto-Lei n.º 75/2008 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/75-2008-249866. [Acedido: 6 de março de 2024]

[14] «cncs-qnrcs-2019.pdf». Disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf. [Acedido: 31 de janeiro de 2024]

[15] «Regulamento n.º 183/2022». Disponível em: https://files.diariodarepublica.pt/2s/2022/02/036000000/0003400039.pdf. [Acedido: 21 de fevereiro de 2024]

Outras referências:

CHECK POINT: 2024 Cyber Security Report
https://resources.checkpoint.com/cyber-security-resources/2024-cyber-security-report

.PT: Relatório Anual PTSOC 2023
https://ptsoc.pt.pt/wp-content/uploads/2024/02/Relatorio2023_PTSOC_PT.pdf

ENISA: Foresight 2030 Threats
https://www.enisa.europa.eu/publications/foresight-2030-threats

ENISA: Threat Landscape 2023
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

CNCS: Observatório de Cibersegurança, Relatório Riscos e Conflitos de 2023
https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

CNCS: Ciber(in)segurança
https://www.cncs.gov.pt/docs/1ciberin.pdf

CNCS: Ciber-higiene e boas práticas de cibersegurança
https://www.cncs.gov.pt/docs/2ciberhig.pdf

CYBER READINESS INSTITUTE: Recursos para partilhar
https://cyberreadinessinstitute.org/starter-kit/starter-kit-posters/

METARED: Gestão de Passwords
https://eventos.metared.org/file_manager/getFile/106364.html

GUIA DE CIBERSEGURANÇA PARA AS ESCOLAS

Índice Remissivo:

31


CIBERSEGURANÇA
GUIA DE BOAS PRÁTICAS PARA AS ESCOLAS
Autor:
Filipe Bagagem
maio, 2024
Créditos
As imagens utilizadas no presente guia foram obtidas em
FREEPIK.COM
(https://www.freepikcompany.com/freepik)
POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

D E C L A R AÇ Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título "Estado Atual da Cibersegurança nos Agrupamentos de Escolas e Escolas Não Agrupadas da região de Leiria", é original e foi realizado por Filipe André Pereira Bagagem (2220558) sob orientação Professora Doutora Marisa da Silva Maximiano, do Professor Doutor Mário João Gonçalves Antunes e do Professor Ricardo Jorge Pereira Gomes.

Leiria, junho de 2024

Filipe André Pereira Bagagem

Assinado por: **FILIPE ANDRÉ PEREIRA BAGAGEM**
Num. de Identificação: 12768641
Data: 2024.06.03 15:05:49+01'00'

(Assinatura digital)