INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Plano de Cibersegurança para o Agrupamento de Escolas Passos Manuel

Andreia Patrícia Semedo Motaco

Mestrado em Transformação Digital no Ensino e Aprendizagem

Orientador:
PhD Carlos José Corredoura Serrão, Professor Associado,
ISCTE – Instituto Universitário de Lisboa

Outubro, 2025

SINTRA
TECNOLOGIAS DIGITAIS
ECONOMIA E SOCIEDADE

Departamento de Ciências Sociais e Empresariais

Plano de Cibersegurança para o Agrupamento de Escolas Passos Manuel

Andreia Patrícia Semedo Motaco

Mestrado em Transformação Digital no Ensino e Aprendizagem

Orientador:
PhD Carlos José Corredoura Serrão, Professor Associado,
ISCTE – Instituto Universitário de Lisboa

Outubro, 2025

Agradecimentos

Agradeço ao ISCTE - Instituto Universitário de Lisboa, em especial ao Mestrado em Transformação Digital no Ensino e Aprendizagem, e a todos os professores envolvidos, pela oportunidade de desenvolver este trabalho.

Expresso o meu sincero reconhecimento e gratidão ao Professor Doutor Carlos José Corredoura Serrão, pela orientação, disponibilidade, paciência e apoio ao longo deste processo.

Agradeço ao Sr. º Diretor João Paulo Leonardo, do Agrupamento de Escolas Passos Manuel, pelo apoio, pela ajuda e, principalmente, por ter confiado em mim, bem como aos meus colegas da EB1/JI das Gaivotas pelo apoio que me deram e por tantas vezes ouviram os meus lamentos.

Agradeço à minha família e amigos que me acompanharam e incentivaram durante esta etapa, e, em especial, aos meus sogros, que são os melhores do mundo e verdadeiros exemplos de força e generosidade, que tornaram a gestão da família mais leve, pelo apoio incondicional que me deram. Agradeço também ao meu pai, que mesmo não percebendo muito bem o porquê de eu ter tanto trabalho, esteve sempre presente, prestando a sua ajuda com tudo o que pôde.

Aos meus filhos, Laura Gouveia e Tiago Gouveia, por serem os melhores filhos do mundo, por perceberem o tempo que abdiquei com eles sem questionarem, acreditando sempre que tudo iria correr bem. Os vossos beijinhos e abraços foram o meu amparo.

Ao André Gouveia, meu marido, meu companheiro e amor da minha vida, que me incentivou e acreditou em mim desde o primeiro segundo, nunca me deixou cair, mesmo nos dias mais difíceis. Foi pai e mãe, segurou todas as pontas quando eu não fui capaz de o fazer.

Ao André e aos meus filhos, dedico este trabalho.
A todos os que fazem parte de mim, muito obrigada!

Resumo

A crescente transformação digital no setor educativo tem impulsionado mudanças significativas nas práticas pedagógicas e na gestão escolar, levantando novos desafios ao nível da proteção de dados e da segurança digital. Em Portugal, muitos agrupamentos de escolas carecem de um plano estruturado de cibersegurança, expondo fragilidades técnicas, organizativas e pedagógicas.

Este estudo visa analisar a realidade digital do Agrupamento de Escolas Passos Manuel no ano letivo de 2025/2026, com especial enfoque na avaliação da maturidade digital, nas práticas de segurança e na proteção de dados em ambiente escolar**.** Recorrer-se-á à análise documental e à aplicação de um formulário informal à direção do agrupamento**,** com o objetivo de identificar necessidades, vulnerabilidades e oportunidades de melhoria.

Face à inexistência de uma estratégia formal, será proposto um plano de cibersegurança ajustado à realidade institucional, alinhado com o Regulamento Geral sobre a Proteção de Dados (RGPD), a Diretiva NIS 2 e os referenciais do Centro Nacional de Cibersegurança e da Comissão Europeia.

Pretende-se, com esta investigação, contribuir para o reforço da segurança digital no ensino público, promovendo uma cultura de cibersegurança colaborativa, integrada e orientada para os desafios da sociedade digital. Este trabalho contribui para a integração da cibersegurança na transformação digital do ensino e da aprendizagem em contexto educativo público, ao propor uma abordagem aplicada de diagnóstico e planeamento, passível de adaptação e replicação noutros agrupamentos de escolas.

Palavras-chave: Cibersegurança educativa, Avaliação da maturidade digital, Plano estratégico de segurança digital, Proteção de dados nas escolas, Literacia digital

Abstract

The growing digital transformation in the education sector has driven significant changes in teaching practices and school management, raising new challenges in terms of data protection and digital security. In Portugal, many school groups lack a structured cybersecurity plan, exposing technical, organizational, and pedagogical weaknesses.

This study aims to analyse the digital reality of the Passos Manuel School Group in the 2025/2026 school year, with a special focus on assessing digital maturity, security practices, and data protection in the school environment. Document analysis and an informal questionnaire will be used to identify needs, vulnerabilities, and opportunities for improvement.

In the absence of a formal strategy, a cybersecurity plan will be proposed that is tailored to the institutional reality and aligned with the General Data Protection Regulation (GDPR), the NIS 2 Directive, and the benchmarks of the National Cybersecurity Center and the European Commission.

The aim of this research is to contribute to strengthening digital security in public education by promoting a collaborative, integrated cybersecurity culture geared towards the challenges of the digital society. This study contributes to the integration of cybersecurity into the digital transformation of teaching and learning in public education contexts by proposing an applied approach to diagnosis and planning that can be adapted and replicated across other school clusters.

KeyWords: Educational cybersecurity, Digital maturity assessment, Strategic digital security plan, Data protection in schools, Digital literacy

Índice Geral

Glossário de Termos-Chave

Para facilitar a consulta, apresentam-se de seguida os principais conceitos e siglas que surgem de forma recorrente ao longo do trabalho de projeto. Esta lista não substitui o glossário integral, mas destaca os termos considerados centrais para a compreensão do ***Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel (AEPM)***.
As definições completas e referências normativas podem ser consultadas no ***Glossário de termos e conceitos.***

Backups 3-2-1: Estratégia de cópias de segurança que recomenda a manutenção de três cópias de dados, em dois suportes diferentes, sendo uma armazenada fora do local de origem (*off-site*).
Captive portal: Página de autenticação apresentada aos utilizadores de redes Wi-Fi de convidados, que regula o acesso à internet e regista ligações.
Firewall / NGFW (*Next-Generation Firewall*): Dispositivo ou serviço que controla e filtra o tráfego de rede, aplicando políticas de segurança e inspeção avançada de pacotes.
IAM (*Identity and Access Management*): Sistema de gestão de identidades e acessos que centraliza a criação, autenticação e permissões dos utilizadores.
MDM (*Mobile Device Management*): Conjunto de ferramentas e políticas para administração e proteção de dispositivos móveis, incluindo controlo remoto, encriptação e bloqueio.
MFA / 2FA (*Multi-Factor / Two-Factor Authentication*): Mecanismo de autenticação que combina dois ou mais fatores independentes (algo que o utilizador sabe, possui ou é).
NIS 2: Diretiva (UE) 2022/2555 que estabelece medidas reforçadas de cibersegurança e obrigações para entidades públicas e privadas.
Phishing: Tentativa fraudulenta de obtenção de dados pessoais ou credenciais através de mensagens enganosas, e-mails ou websites falsos.
Plano de Cibersegurança: Conjunto estruturado de medidas organizacionais, técnicas e pedagógicas que visam proteger sistemas, dados e utilizadores do Agrupamento de Escolas Passos Manuel.
RBAC (*Role-Based Access Control*): Modelo de controlo de acessos baseado em funções atribuídas aos utilizadores, permitindo aplicar políticas de forma hierárquica e centralizada.
Ransomware: Tipo de *malware* que encripta dados e exige pagamento de um resgate para permitir a sua recuperação.

RGPD (*Regulamento Geral sobre a Proteção de Dados*): Regulamento (UE) 2016/679 que define princípios, direitos e obrigações relativos ao tratamento de dados pessoais.

SIEM (*Security Information and Event Management*): Plataforma que recolhe e analisa registos de eventos de segurança para deteção (MTTD), resposta (MTTR) e auditoria.

Zero Trust: Modelo de segurança que assume "confiança zero" por defeito, exigindo autenticação, autorização e verificação contínuas de todos os utilizadores e dispositivos.

CAPÍTULO 1

Introdução

Este capítulo enquadra o trabalho, apresentando o contexto e a motivação que estiveram na sua origem. Parte-se de um problema identificado em contexto educativo, a partir do qual se formulou a questão de investigação que orienta o estudo. De forma sintética, descrevem-se ainda a metodologia adotada e as principais etapas do processo, desde a definição do problema até à elaboração e apresentação do plano de cibersegurança para o Agrupamento de Escolas Passos Manuel.

1.1. Contextualização do tema

A transformação digital tem vindo a alterar de forma profunda o modo como as escolas ensinam, aprendem e se organizam. Políticas nacionais e europeias, como o *Plano de Ação para a Transição Digital*[1] (Governo de Portugal, 2020) e o *Digital Education Action Plan 2021–2027* [2](Comissão Europeia, 2021), impulsionaram a integração das tecnologias na educação e promoveram novas formas de comunicação e de gestão escolar.

Em Portugal, os dados mais recentes do Instituto Nacional de Estatística indicam que 98,5 % das famílias com crianças têm acesso à internet e 96,7 % dispõem de ligação de banda larga (INE, 2023). A maioria das escolas possui já dispositivos digitais individuais para os alunos e cobertura de rede de alta velocidade, o que reforça as condições mínimas para o ensino digital (CNCS, 2024). A Direção-Geral da Educação destaca igualmente que as instituições escolares têm vindo a adotar mecanismos de autenticação mais seguros e a reconhecer a cibersegurança como prioridade (DGE, 2024). Apesar dos progressos, o setor educativo continua vulnerável a riscos emergentes. As escolas lidam diariamente com dados pessoais de alunos, docentes e famílias e, por isso, estão expostas a ataques de *phishing*, *ransomware* ou fugas de informação (CNCS, 2024; Veiga, 2024). O estudo Educação para a Cibersegurança no Ensino Básico e Secundário em Portugal (CNCS & FPCEUP, 2024) confirma que a maturidade em cibersegurança permanece reduzida e que faltam planos estruturados e integrados.

[1] O *Plano de Ação para a Transição Digital* (Resolução do Conselho de Ministros n.º 30/2020) define as metas da digitalização da administração pública, economia e educação em Portugal, incluindo o reforço das competências digitais e da cibersegurança.

[2] O *Digital Education Action Plan 2021–2027*, da Comissão Europeia, estabelece prioridades e ações para a educação digital nos Estados-Membros, promovendo a transformação digital e a cibercompetência.

Esta realidade é frequentemente associada à ausência de políticas institucionais estruturadas, à formação desigual dos diferentes atores educativos e à fraca consolidação de uma cultura organizacional de segurança digital. O Observatório de Cibersegurança – Sociedade 2024, assinala também fragilidades na Administração Pública, onde a adoção da autenticação multifator diminuiu de 71 % para 49 % entre 2022 e 2023 (CNCS, 2024).

A nível europeu, a *Diretiva NIS 2* [1](União Europeia, 2022) reforça as exigências de governação e gestão do risco, e o *Digital Services Act* [2](União Europeia, 2022) introduz medidas adicionais de transparência e proteção. A estratégia "*Uma Europa preparada para a era digital*[3]" (Comissão Europeia, 2024) enfatiza ainda a importância da literacia digital e da segurança online como pilares estruturais das políticas públicas.

Muitas escolas portuguesas, contudo, continuam sem planos específicos de cibersegurança (Monteiro & Gomes, 2009). A ausência de políticas claras, a desigualdade na formação digital e a falta de uma cultura institucional de segurança digital evidenciam a necessidade de uma abordagem planeada e adaptada à realidade escolar. Neste contexto, o desenvolvimento de um plano de cibersegurança institucional assume carácter prioritário, combinando dimensões técnicas, organizacionais e pedagógicas e envolvendo toda a comunidade educativa.

1.2. Questão, problema e objetivos de investigação

Partindo deste cenário, a investigação procura responder à seguinte questão orientadora:

Como conceber um plano institucional de cibersegurança adequado à maturidade digital do Agrupamento de Escolas Passos Manuel, articulando gestão, proteção técnica, capacitação e melhoria contínua?

O estudo parte da constatação de que, apesar do enquadramento legal e estratégico existente, que inclui o *Regulamento Geral sobre a Proteção de Dados* (RGPD – UE 2016/679),[4] o *Plano de*

[1] A *Diretiva (UE) 2022/2555 – NIS 2* reforça a segurança das redes e sistemas de informação na União Europeia e aplica-se a entidades públicas, incluindo instituições educativas.
[2] O *Digital Services Act* (*Regulamento (UE) 2022/2065*) regula a prestação de serviços digitais e a responsabilidade das plataformas online na União Europeia.
[3] Estratégia-quadro da Comissão Europeia (2019–2024) que orienta políticas de transição digital, inteligência artificial, literacia digital e cibersegurança nos Estados-Membros.
[4] O *Regulamento (UE) 2016/679*, conhecido como *Regulamento Geral sobre a Proteção de Dados* (RGPD), estabelece regras relativas à proteção de dados pessoais e à livre circulação desses dados no espaço europeu.

Cibersegurança na Educação[1] (CNCS, 2021) e a *Diretiva NIS 2* (União Europeia, 2022), a aplicação prática desses princípios nas escolas é ainda limitada e pouco sistematizada.

O objetivo geral deste trabalho consiste em propor um plano institucional de cibersegurança para o Agrupamento de Escolas Passos Manuel, alinhado com referenciais nacionais e internacionais e adaptado ao seu nível de maturidade digital. De forma complementar, pretende-se identificar normas e boas práticas relevantes para o contexto educativo, caracterizar as principais necessidades e vulnerabilidades do agrupamento a partir da análise documental e do contexto organizacional, estruturar fases de implementação que integrem gestão, proteção técnica, capacitação e avaliação, e propor estratégias de sensibilização e formação dirigidas a diferentes perfis da comunidade escolar.

1.3. Lacuna no conhecimento

A produção científica sobre cibersegurança tem crescido, mas a maioria dos estudos privilegia abordagens técnicas ou normativas (Xu & Li, 2025; Antunes et al., 2021), oferecendo pouca orientação prática para escolas concretas. A literatura revela também escassa participação de direções, docentes e encarregados de educação nos processos de conceção e validação (Amankwa, 2021; CNCS & FPCEUP, 2024). Essa falta de envolvimento fragiliza a aplicabilidade das recomendações existentes.

Faltam, por isso, modelos que traduzam os princípios da cibersegurança em planos operacionais realistas, capazes de articular medidas técnicas, pedagógicas e organizacionais com os recursos e limitações das escolas públicas. Este estudo pretende contribuir para colmatar essa lacuna, propondo uma abordagem prática e replicável, validada com base em referenciais como o CNCS, a ISO e o NIST.

1.4. Metodologia

A investigação assenta numa abordagem qualitativa, exploratória e propositiva, orientada para a construção de uma solução prática a um problema institucional identificado. O percurso metodológico combina a análise da literatura e dos referenciais normativos com a interpretação do contexto documental e organizacional do agrupamento, culminando na proposição de um plano de cibersegurança ajustado à sua realidade. Trata-se de um estudo aplicado, que procura transformar evidência teórica e normativa em orientações operacionais adequadas ao contexto educativo. Esta

[1] O *Plano de Cibersegurança na Educação* (CNCS, 2021) apresenta orientações nacionais para reforçar a segurança digital e a cultura de ciber-resiliência nas escolas portuguesas.

abordagem baseia-se em princípios de triangulação de fontes científicas, institucionais e experienciais, garantindo coerência e validade às conclusões. Todo o processo respeita os princípios éticos e legais em vigor, nomeadamente o *Regulamento Geral sobre a Proteção de Dados* (RGPD).

1.5. Estrutura do trabalho de projeto

A presente dissertação organiza-se em seis capítulos principais, complementados por referências bibliográficas e apêndices. A estrutura segue a sequência lógica da investigação, do enquadramento teórico à aplicação prática, orientando o leitor ao longo das etapas do estudo.

O Capítulo 1 apresenta o contexto e a relevância do tema, identifica o problema e a questão de investigação, define os objetivos gerais e específicos e introduz a metodologia adotada, estabelecendo a base conceptual e empírica do trabalho.

O Capítulo 2 sistematiza o enquadramento teórico e empírico sobre transformação digital e cibersegurança em contexto educativo, analisando conceitos, desafios e políticas internacionais e nacionais, com destaque para o papel das escolas na promoção da cultura de segurança digital.

O Capítulo 3 descreve a abordagem qualitativa e propositiva do estudo, explicitando as etapas de recolha e análise da informação, o protocolo PRISMA 2020 aplicado à revisão da literatura e os princípios éticos e legais seguidos no processo de investigação.

O Capítulo 4 caracteriza o Agrupamento de Escolas Passos Manuel, apresentando as condições digitais, recursos e práticas existentes. Este diagnóstico identifica as principais vulnerabilidades e sustenta a elaboração do plano de cibersegurança.

O Capítulo 5, núcleo central do trabalho, apresenta o Plano de Cibersegurança, estruturado por eixos de intervenção e fases de implementação, integrando dimensões técnicas, organizacionais e pedagógicas que promovem uma cultura de segurança e responsabilidade digital.

O Capítulo 6 reflete sobre os resultados alcançados, confrontando-os com a literatura e os referenciais normativos, e apresenta as conclusões, limitações e recomendações para futuras investigações e práticas escolares.

Por fim, incluem-se as referências bibliográficas, que sustentam o enquadramento teórico e empírico, e os apêndices**,** que reúnem os instrumentos e materiais complementares utilizados ao longo do estudo.

CAPÍTULO 2

Revisão da Literatura

Este capítulo enquadra teoricamente o estudo, apresentando os principais conceitos, políticas e modelos que fundamentam o Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel (AEPM). Parte-se da análise da transformação digital no sistema educativo e dos novos desafios que esta introduz em matéria de segurança, privacidade e literacia digital, exigindo abordagens integradas de gestão e capacitação institucional.

A revisão estrutura-se em seis dimensões complementares: a transformação digital e a cibersegurança em contexto educativo; princípios, ameaças e cultura de segurança digital; o enquadramento normativo e político; os modelos e ferramentas de maturidade digital e cibernética; competência digital e literacia tecnológica da comunidade educativa; e síntese crítica e implicações para o estudo. Cada uma destas dimensões contribui para identificar tendências, boas práticas e lacunas na literatura e nas políticas em vigor, constituindo a base conceptual e empírica que orienta a metodologia e sustenta o desenvolvimento do plano de intervenção apresentado nos capítulos seguintes.

2.1. Cibersegurança e transformação digital no contexto educativo

A transformação digital tem vindo a redefinir as dinâmicas de ensino, aprendizagem e gestão escolar, impulsionada por políticas nacionais e europeias como o Plano de Ação para a Transição Digital (Governo de Portugal, 2020) e o *Digital Education Action Plan 2021–2027* (Comissão Europeia, 2021). Estas iniciativas promoveram a digitalização das práticas pedagógicas, administrativas e comunicacionais, originando um ecossistema educativo mais interligado, mas também mais vulnerável a riscos tecnológicos e de segurança (CNCS & FPCEUP, 2024).

Mais do que uma digitalização de processos, esta transformação representa uma mudança cultural e pedagógica que exige novas formas de ensinar, aprender e gerir as escolas. Implica o desenvolvimento de competências digitais, a consolidação de uma cultura de segurança e a integração ética e crítica da tecnologia no quotidiano escolar (Antunes & Rodrigues, 2021; Chahid et al., 2025; Lopes, Sargento & Farto, 2023). Neste sentido, Abrantes (2020) demonstra que a tecnologia, quando

integrada em contextos reais de aprendizagem, potencia metodologias ativas e práticas pedagógicas ajustadas à era digital.

Em Portugal, 98,5 % das famílias com crianças têm acesso à internet e 96,7 % dispõem de ligação de banda larga (INE, 2023). A generalização de dispositivos digitais individuais (1:1) e a cobertura quase total de banda larga reforçam a infraestrutura tecnológica das escolas (CNCS, 2024). Contudo, estudos nacionais revelam uma maturidade ainda reduzida em matéria de cibersegurança, marcada pela ausência de planos integrados e de estratégias de proteção consistentes (CNCS & FPCEUP, 2024; Gomes, Dias & Ferreira, 2023). No plano europeu, a *Diretiva NIS 2* (União Europeia, 2022), o *Digital Services Act* (União Europeia, 2022) e a estratégia *Uma Europa preparada para a era digital* (Comissão Europeia, 2019–2024) reforçam a importância da segurança digital e da literacia tecnológica como pilares da transformação digital. Em Portugal, o Centro Nacional de Cibersegurança (CNCS) lidera esta política, disponibilizando referenciais e programas de capacitação, entre os quais o *Plano de Cibersegurança na Educação* (CNCS, 2021), o *Referencial de Competências em Cibersegurança* (CNCS, 2022) e o *Guia de Transição Digital* (CNCS, 2023). A estes somam-se recursos europeus como o DigCompEdu e o SELFIE, que apoiam escolas e docentes na autoavaliação da maturidade digital e no planeamento de estratégias de desenvolvimento (Palacios-Rodríguez et al., 2025). Assim, o sucesso da transformação digital depende não apenas da infraestrutura tecnológica, mas também da capacidade das escolas para promover uma cultura de segurança, ética e responsabilidade digital (Comissão Europeia, 2022; CNCS, 2024).

Neste contexto, a cibersegurança escolar assume-se como condição essencial da transformação digital, assegurando a proteção de dados e sistemas e reforçando a confiança da comunidade educativa no uso das tecnologias. Digitalização e cibersegurança devem, por isso, ser entendidas como dimensões complementares de uma mesma estratégia de inovação e sustentabilidade educativa (Veiga, 2024).

2.2. Princípios, ameaças e cultura de segurança digital

As escolas, pela natureza dos dados que gerem, são alvos recorrentes de ciberataques. Entre as ameaças mais comuns encontram-se o *phishing*, o *ransomware*, a engenharia social e os ataques de negação de serviço (DDoS), agravados pela ausência de políticas de segurança e de sensibilização dos utilizadores (Veiga, 2024; CNCS, 2024). O modelo da tríade Confidencialidade, Integridade e Disponibilidade (CIA) continua a ser o referencial clássico para garantir a proteção da informação (Antunes & Rodrigues, 2021).

Estudos recentes identificam ainda o roubo de identidade digital, a violação de credenciais, o *spyware*, a exposição acidental de dados pessoais e o aumento de ataques direcionados a alunos e docentes como ameaças emergentes (CNCS, 2024; Jerman Blažič & Jerman Blažič, 2025; Xu & Li, 2025). A aplicação de medidas como autenticação multifator, segmentação de rede e cópias de segurança segundo a regra 3-2-1 constitui uma boa prática essencial (NIST, 2018). De acordo com o CNCS (2024), o fator humano permanece o vetor de risco mais relevante, tornando indispensável a formação contínua e a monitorização sistemática de incidentes. A segurança digital, contudo, vai além dos controlos técnicos, requer uma cultura de responsabilidade coletiva, ética digital e participação cívica. A *Estratégia de Educação para a Cidadania na Escola* (EECE, 2023) e as orientações da Comissão Europeia (2022, 2023) sublinham a importância de integrar a cibersegurança e a literacia digital no currículo, promovendo comportamentos seguros e críticos. A educação para a cibersegurança deve ser encarada como parte da cidadania digital, preparando crianças e jovens para agir de forma consciente e segura no espaço online (CNCS & FPCEUP, 2024). Iniciativas de envolvimento parental, como a *Digital Academy for Parents* (E-REDES & DGE, 2023) e o *Digital Parenting* (EurofamNet, 2024), comprovam o impacto positivo da cooperação entre escola, alunos e famílias na consolidação da segurança digital (CNCS, 2024; ENISA, 2024). Esta abordagem evidencia que a segurança é tanto uma competência técnica como social, dependente de uma ação educativa integrada.

A sensibilização pública tem também sido reforçada através de investigações mediáticas sobre cibercrime, como os documentários *The Cyber War* (Van Zeller, 2022) e *Os segredos dos nossos dados* (Patel, 2023), que expõem vulnerabilidades e práticas ilícitas na exploração de dados. Estes exemplos sustentam a necessidade de educação em cibersegurança desde o ensino básico, fomentando a compreensão dos riscos e a adoção de comportamentos preventivos (Monteiro & Gomes, 2009; CNCS & Universidade do Porto, 2024).

O desenvolvimento de uma cultura de segurança digital deve, assim, articular-se com a promoção de valores de empatia, respeito e responsabilidade online, fortalecendo comunidades educativas mais resilientes e colaborativas (Comissão Europeia, 2022a). A mitigação de riscos depende tanto da implementação de medidas técnicas e organizacionais como da construção de uma cultura partilhada de segurança e cidadania digital (Veiga, 2024; CNCS, 2024).

2.3. Enquadramento normativo e político

O quadro legal europeu e nacional estabelece os fundamentos da proteção da informação em ambiente educativo. O Regulamento Geral sobre a Proteção de Dados (UE, 2016/679), transposto pela

Lei n.º 58/2019, define regras de tratamento de dados pessoais e obriga as escolas públicas à nomeação de um Encarregado de Proteção de Dados (DPO)[1] e à realização de Avaliações de Impacto (DPIA)[2]. A Comissão Nacional de Proteção de Dados (CNPD) tem emitido orientações específicas para o setor educativo, destacando-se a Diretriz 2018/1, relativa à publicação de dados pessoais em sítios da internet, e a Diretriz 2023/1, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais (CNPD, 2018**,** 2023). Estas orientações reforçam a importância de princípios como a minimização, a proporcionalidade e a responsabilização *(accountability)* das instituições. A nível europeu, a Diretiva NIS 2 (União Europeia, 2022) estabelece requisitos reforçados de cibersegurança e mecanismos de gestão de incidentes para entidades públicas, incluindo as do setor educativo. Complementarmente, o *Digital Services Act* (DSA) (Comissão Europeia, 2022) define normas para a prestação de serviços digitais e para a moderação de conteúdos online, impondo obrigações de transparência e segurança acrescidas. Em Portugal, a política nacional de cibersegurança é coordenada pelo Centro Nacional de Cibersegurança (CNCS), que desenvolve referenciais, guias e programas de apoio às escolas. Entre os documentos orientadores destacam-se o Plano de Cibersegurança na Educação (CNCS, 2021), o Referencial de Competências em Cibersegurança (CNCS, 2022) e o Guia de Transição Digital (CNCS, 2023). Estes instrumentos operam em articulação com o Plano de Ação para a Transição Digital (Governo de Portugal, 2020) e o Plano de Ação para a Educação Digital 2021–2027 (Comissão Europeia, 2021), assegurando alinhamento entre políticas nacionais e europeias. A ENISA *(European Union Agency for Cybersecurity)* tem igualmente contribuído para o reforço da cultura de segurança no setor público, através de modelos de maturidade e guias de boas práticas, como o *Cybersecurity Education Maturity Assessment* (ENISA, 2024**)** e o *ENISA Maturity Framework for Public Sector* (ENISA, 2023). Estes modelos propõem metodologias de autoavaliação e planeamento, úteis para a definição de estratégias institucionais de proteção digital. No contexto nacional, merecem ainda destaque iniciativas pioneiras como o Plano de Cibersegurança da Escola Profissional do Alto Ave (EPAVE, 2022), que apresenta uma abordagem integrada à segurança digital, combinando medidas técnicas, organizacionais e formativas. Este exemplo demonstra a importância de políticas internas claras e da articulação entre diferentes níveis de governação escolar.

Em síntese, o enquadramento normativo e político da cibersegurança educativa em Portugal resulta da convergência entre as políticas europeias e nacionais. A conformidade legal e o alinhamento com boas práticas internacionais constituem a base para a criação de planos institucionais robustos e

[1] O DPO **(***Data Protection Officer***)** é o responsável por monitorizar o cumprimento do RGPD, aconselhar a direção e servir de ponto de contacto com a CNPD.

[2] A Avaliação de Impacto sobre a Proteção de Dados (AIPD/DPIA) é uma análise prévia dos riscos para direitos e liberdades, exigida pelo artigo 35.º do RGPD.

sustentáveis, capazes de proteger a informação, garantir direitos digitais e promover a confiança no uso da tecnologia nas escolas (CNCS, 2024; União Europeia, 2022; ENISA, 2024).

2.4. Modelos e ferramentas de maturidade digital e cibernética

A avaliação da maturidade digital e cibernética constitui um processo essencial para compreender o grau de resiliência das instituições educativas e orientar estratégias de melhoria contínua. A utilização de modelos e ferramentas de referência permite às escolas diagnosticar vulnerabilidades, definir prioridades e planear a evolução dos seus sistemas e práticas digitais de forma sustentável.

Modelos internacionais como o *Cybersecurity Maturity Model for K-12* (*U.S. Department of Education,* 2023) e o *ENISA Maturity Framework for Public Sector* (ENISA, 2023) oferecem metodologias de autoavaliação adaptadas ao setor público e ao contexto escolar. Estes instrumentos propõem níveis de maturidade incipiente, emergente, estabelecido e otimizado e boas práticas que orientam a governação, a proteção, a deteção, a resposta e a recuperação perante incidentes de cibersegurança. O *Cybersecurity Education Maturity Assessment* (ENISA, 2024) reforça esta abordagem, ao propor uma avaliação multidimensional centrada na governação, gestão do risco, formação, infraestrutura e cultura organizacional. O modelo incentiva as instituições a evoluírem gradualmente, promovendo uma cultura de segurança integrada e uma gestão de risco baseada em evidência. No contexto europeu, o DigCompEdu (*European Framework for the Digital Competence of Educators*) e o SELFIE (*Self-reflection on Effective Learning by Fostering the use of Innovative Educational Technologies*) (Comissão Europeia, 2022) são amplamente utilizados como ferramentas de autoavaliação da maturidade digital das escolas e das competências digitais dos docentes (Palacios-Rodríguez et al., 2025). Ambos permitem medir níveis de proficiência e apoiar a definição de planos de ação digital, sendo complementares aos referenciais técnicos e de segurança definidos pelo Centro Nacional de Cibersegurança (CNCS, 2024) e pelo Plano de Ação para o Desenvolvimento Digital da Escola (PADDE)**.** A aplicação integrada destes modelos e ferramentas contribui para o fortalecimento da governação digital, da proteção técnica e da capacitação pedagógica, assegurando coerência entre políticas educativas e requisitos de segurança. O Referencial de Competências em Cibersegurança (CNCS, 2022) reforça esta ligação, ao definir perfis e níveis de proficiência alinhados com o contexto nacional e europeu, promovendo a articulação entre a literacia digital, a ética tecnológica e a proteção da informação. Em conjunto, estes modelos e *frameworks* convergem na necessidade de institucionalizar processos de autoavaliação regulares, auditáveis e transparentes, que sustentem a confiança e a sustentabilidade da transição digital. A articulação entre referenciais europeus e

nacionais, apoiada em práticas de diagnóstico e melhoria contínua, constitui a base para a construção de ecossistemas educativos mais seguros, maduros e inovadores (Antunes & Rodrigues, 2021; CNCS, 2023; ENISA, 2024).

2.5. Competência digital e literacia tecnológica da comunidade educativa

A competência digital docente é uma componente essencial da transformação digital das escolas. Estudos realizados em Portugal e Espanha demonstram níveis heterogéneos de proficiência, com lacunas particularmente evidentes na dimensão da segurança e da cidadania digital (Palacios-Rodríguez et al., 2025). Essa fragilidade reforça a importância de programas de formação contínua baseados no DigCompEdu (Comissão Europeia, 2022) e no Referencial de Competências em Cibersegurança (CNCS, 2022), bem como da estruturação de políticas, procedimentos e controlos de segurança digital adequados às necessidades das escolas.

A Estratégia de Educação para a Cidadania na Escola (EECE, 2023) reconhece a relevância de desenvolver competências transversais de literacia digital e ética online, incentivando as escolas a promover atividades de sensibilização para a cibersegurança e o uso responsável da tecnologia. Este enquadramento está em consonância com o Plano de Ação para a Educação Digital 2021–2027 (Comissão Europeia, 2021) e com o Guia de Transição Digital (CNCS, 2023), que enfatizam a necessidade de capacitar docentes e alunos para um ambiente digital seguro, ético e inclusivo. A capacitação da comunidade educativa deve abranger não apenas os docentes, mas também alunos, encarregados de educação e técnicos não docentes, promovendo uma abordagem colaborativa e sustentável. Programas nacionais como o *Portugal Digital Academy* e o *Digital Academy for Parents* (E-REDES & DGE, 2023) ilustram boas práticas de formação colaborativa (Lopes, Sargento & Farto, 2023). A nível europeu, o *Digital Parenting* (*EurofamNet*, 2024) constitui um exemplo de cooperação entre escola e famílias, contribuindo para o desenvolvimento de uma cultura partilhada de segurança digital (Comissão Europeia, 2022; CNCS, 2024). A literatura internacional evidencia que a capacitação conjunta de professores, alunos e encarregados de educação reforça a cultura de segurança e a sustentabilidade das políticas de literacia digital (Amankwa, 2021; Jerman Blažič & Jerman Blažič, 2025). De acordo com o estudo *Educação para a Cibersegurança no Ensino Básico e Secundário em Portugal* (CNCS & FPCEUP, 2024), a formação em literacia digital continua a ser pontual e pouco estruturada, exigindo maior integração curricular e articulação com as políticas de cidadania digital.

A nível internacional, Xu e Li (2025) destacam que a educação para a cibersegurança em idades precoces potencia o desenvolvimento de competências críticas e comportamentos seguros, enquanto

Monteiro e Gomes (2009) identificam a persistência de práticas de risco entre jovens portugueses, reforçando a urgência de programas educativos preventivos. O investimento em formação contínua e literacia digital não deve restringir-se à dimensão técnica, mas incluir igualmente a reflexão ética, a cidadania ativa e o pensamento crítico no uso das tecnologias (Comissão Europeia, 2022; CNCS, 2024). Segundo Lopes, Sargento e Farto (2023), a transformação digital no setor público exige estratégias de formação contínua adaptadas aos contextos locais e sustentadas por lideranças capacitadas. Esta perspetiva é corroborada por Chahid et al. (2025), que sublinham o papel das universidades e das administrações públicas na consolidação de ecossistemas de aprendizagem digital seguros. Por sua vez, Antunes e Rodrigues (2021) defendem que a segurança digital é tanto um domínio técnico como uma dimensão comportamental, devendo ser integrada nas práticas quotidianas das escolas. Assim, a consolidação da competência digital docente e institucional depende da formação, da sensibilização e do compromisso coletivo com a segurança, a ética e a cidadania digital (CNCS, 2024).

2.6. Síntese crítica e implicações para o estudo

A literatura revela que a cibersegurança escolar permanece num estádio intermédio de desenvolvimento: embora existam avanços normativos e técnicos, a aplicação prática das recomendações é limitada (CNCS & FPCEUP, 2024). Persistem falhas na articulação entre dimensões técnica, organizacional e pedagógica, bem como na definição de métricas e indicadores de maturidade digital (Rajamäki et al., 2024; Xu & Li, 2025). Identificam-se também fragilidades na formação docente, na gestão de incidentes e na integração curricular da cibersegurança, fatores críticos para o sucesso das políticas digitais (Jerman Blažič & Jerman Blažič, 2025; Amankwa, 2021). Em muitas instituições, a fragmentação de responsabilidades e a ausência de planos formais comprometem a coerência das ações (CNCS, 2024). As práticas de capacitação mantêm-se centradas em docentes e alunos, com reduzida participação de famílias e assistentes operacionais, o que limita o impacto das iniciativas (EurofamNet, 2024). A literatura defende, por isso, modelos colaborativos e inclusivos de governação (Lopes, Sargento & Farto, 2023; CNCS, 2023), sustentados em cronogramas e indicadores que permitam monitorizar a eficácia das medidas (Figueiredo, Serrão & Almeida, 2023).

Face a estas lacunas, o presente estudo propõe um plano de cibersegurança ajustado à maturidade digital do Agrupamento de Escolas Passos Manuel, articulando medidas de gestão, proteção técnica, capacitação e avaliação contínua. Baseado em referenciais europeus e nacionais, o plano visa reforçar a cultura de segurança digital e servir de modelo replicável para contextos educativos semelhantes (Veiga, 2024; CNCS, 2024).

CAPÍTULO 3

Metodologia

Este capítulo descreve a metodologia adotada no estudo, apresentando as opções epistemológicas, os procedimentos de recolha e análise de dados e os critérios que asseguram a validade, fiabilidade e ética da investigação. A abordagem é qualitativa, exploratória e propositiva, combinando revisão sistemática da literatura, análise documental e recolha empírica de dados em contexto institucional. Fundamentada na Declaração PRISMA 2020 e em referenciais normativos reconhecidos, garante transparência e reprodutibilidade em todas as fases do processo. O capítulo estrutura-se em seis secções: abordagem e desenho do estudo; estratégia de pesquisa e revisão sistemática (PRISMA 2020); análise, extração e diagnóstico de dados; síntese e caracterização dos documentos incluídos; validade, fiabilidade e ética e considerações finais que orientam a investigação.

3.1. Abordagem e desenho do estudo

O presente estudo adota uma abordagem qualitativa, exploratória e propositiva, centrada na compreensão das práticas e estratégias de cibersegurança em contexto educativo. A investigação visa identificar lacunas, mapear boas práticas e propor um plano de ação institucional adaptado à realidade do Agrupamento de Escolas Passos Manuel.

A natureza qualitativa justifica-se pela necessidade de interpretar fenómenos educativos complexos, analisando significados e contextos. O carácter exploratório decorre da escassez de estudos nacionais que articulem a cibersegurança com a transformação digital das escolas públicas. Já a vertente propositiva reflete o propósito de gerar soluções práticas, sustentadas em evidência científica e documental. O desenho metodológico organiza-se em três etapas interligadas: a revisão sistemática da literatura e a análise documental, o diagnóstico institucional e, por fim, a construção e validação do plano de cibersegurança. A revisão sistemática foi conduzida de acordo com a Declaração PRISMA 2020 (Sousa, Gonçalves-Lopes, Abreu, & Oliveira, 2024; PRISMA, 2021), garantindo transparência, rastreabilidade e replicabilidade em todas as fases do processo.

3.2. Estratégia de pesquisa documental e revisão sistemática (PRISMA 2020)

3.2.1. Fontes, estratégias e critérios de pesquisa

A pesquisa foi conduzida entre abril e setembro de 2025, em bases de dados científicas e portais institucionais, incluindo a *Scopus*, *Web of Science*, *ERIC* e *Google Scholar*. Complementarmente, integraram-se documentos oficiais provenientes de organismos nacionais e europeus, como o Centro Nacional de Cibersegurança (CNCS), a Comissão Europeia, a ENISA e a Direção-Geral da Educação (DGE). As fichas-resumo dos websites e relatórios institucionais analisados encontram-se apresentadas no (**Apêndice A**), assegurando a rastreabilidade das fontes e a transparência do processo metodológico.

Os estudos incluídos foram publicados entre 2018 e 2025, em português, inglês ou espanhol, com enfoque em educação, cibersegurança, competência digital e políticas públicas. Esta janela temporal reflete o período de intensificação das políticas digitais europeias e nacionais. A formulação das expressões de pesquisa seguiu a metodologia PRISMA 2020 (Page et al., 2021), recorrendo a operadores booleanos e à combinação de palavras-chave temáticas. As principais expressões utilizadas foram: *(“cybersecurity” OR “digital security” OR “information security”) AND (“education” OR “school” OR “students” OR “teachers”) AND (“training” OR “awareness” OR “policy”).*

A estratégia foi ajustada às particularidades de cada base de dados, por exemplo, o uso de *title-abs-key* na *Scopus* e *abstract* no *ERIC* e complementada com planos, relatórios e diretrizes oficiais disponíveis em acesso aberto. O processo de seleção seguiu as quatro fases definidas pela metodologia PRISMA 2020, identificação, triagem, elegibilidade e inclusão, representadas no diagrama de fluxo do (**Apêndice B**). A aplicação da metodologia foi verificada através da PRISMA 2020 *Abstract Checklist* (Sousa, Gonçalves-Lopes, Abreu & Oliveira, 2024), cuja versão integral em português europeu consta no (**Apêndice C**). Na fase de identificação, foram encontrados 137 registos (120 em bases de dados, 16 em websites institucionais e 1 em organização pública). Após a remoção de duplicados (n=16), resultaram 121 registos analisados com base no título e resumo. Foram excluídos 47 por falta de relevância temática, permanecendo 74 estudos elegíveis para leitura integral. Na fase de elegibilidade, 50 estudos foram lidos na íntegra e avaliados quanto à pertinência temática e metodológica; destes, 30 foram excluídos, 24 por ausência de metodologia explícita e 6 por não se enquadrarem no contexto educativo. Assim, 20 estudos foram incluídos na revisão sistemática final, constituindo o corpus de análise desta investigação.

Os critérios de inclusão abrangeram publicações científicas e documentos oficiais com foco em educação e cibersegurança, no contexto europeu ou nacional. Foram excluídos textos sem revisão por

pares, documentos corporativos sem validade científica e artigos sem ligação direta ao ambiente escolar. Todos os dados foram selecionados manualmente pela investigadora, sem recurso a software automatizado para triagem ou análise. A revisão sistemática não foi registada em bases internacionais, como PROSPERO ou OSF, atendendo ao enquadramento académico e às opções metodológicas do presente estudo.

3.3. Análise, extração e diagnóstico de dados

A análise e extração de dados foram realizadas manualmente e de forma sistemática, recorrendo a uma grelha de análise documental desenvolvida especificamente para este estudo, sem recurso a software automatizado. Para cada fonte foram registadas variáveis como o autor ou autores, o ano e o país de origem, o tipo de documento (artigo científico, relatório ou plano institucional), os objetivos e a metodologia adotados, os temas-chave abordados, formação, sensibilização, políticas, competências digitais e riscos, bem como os principais contributos e limitações identificados.

A interpretação dos dados seguiu uma lógica de triangulação entre evidência científica, normativa e institucional, assegurando validade interna e consistência teórica. Este processo permitiu identificar tendências, lacunas e boas práticas transferíveis para o contexto do Agrupamento de Escolas Passos Manuel. A síntese dos referenciais normativos e dos modelos estratégicos utilizados encontra-se sistematizada no (**Apêndice D**), complementando o enquadramento conceptual e documental da investigação. A componente empírica da recolha de dados foi operacionalizada através do Formulário de Diagnóstico de Cibersegurança (Direção AEPM, 13 de setembro de 2025), apresentado no (**Apêndice E**). O instrumento foi desenvolvido pela autora com o objetivo de identificar vulnerabilidades, práticas e níveis de maturidade digital e cibernética do Agrupamento, abrangendo dimensões técnicas, organizacionais e pedagógicas que serviram de base empírica ao plano de cibersegurança. A conceção baseou-se na análise dos referenciais normativos e metodológicos descritos anteriormente, garantindo a adequação à realidade institucional. O formulário foi estruturado em seis dimensões principais: infraestrutura de rede e proteção; equipamentos e sistemas; políticas e conformidade; práticas digitais e rotinas de segurança; formação e sensibilização; e cultura, riscos e sugestões. Estas dimensões permitem uma leitura transversal da maturidade digital e da resiliência em cibersegurança.

O instrumento fundamentou-se em referenciais nacionais e internacionais reconhecidos, nomeadamente as normas ISO/IEC 27001:2022 e 27002:2022 (ISO, 2022), o Regulamento Geral sobre a Proteção de Dados (RGPD, art.º 24.º, 25.º, 32.º e 35.º), a Diretiva NIS 2 (UE, 2022), o Referencial de

Competências em Cibersegurança (CNCS, 2022), o *Cybersecurity Education Maturity Assessment* (ENISA, 2024) e o DigCompEdu (Comissão Europeia, 2022).

A aplicação decorreu em setembro de 2025, junto da Direção do AEPM, garantindo o cumprimento das normas éticas e de proteção de dados previstas no Regulamento (UE) 2016/679 e nas Diretrizes da CNPD (2018/1; 2023/1). Sempre que necessário, foram realizadas clarificações adicionais com a Direção, assegurando a consistência e fiabilidade dos dados. O formulário foi respondido em representação institucional e os dados foram tratados de forma anónima e agregada, com utilização exclusiva para fins académicos.

Os resultados foram posteriormente analisados por triangulação com os dados documentais e técnicos apresentados no Capítulo 4, permitindo validar o diagnóstico institucional e identificar prioridades de intervenção. Esta análise sustenta o plano de cibersegurança detalhada no Capítulo 5, garantindo coerência entre a evidência empírica e a estratégia de transformação digital em curso.

3.4. Síntese e caracterização dos documentos incluídos

A aplicação do método PRISMA 2020 (Page et al., 2021) permitiu identificar e selecionar as fontes mais relevantes da revisão da literatura, assegurando transparência e rastreabilidade em todas as fases, identificação, triagem, elegibilidade e inclusão, detalhadas no ponto 3.2.1 e representadas no (**Apêndice D**). O processo resultou em 20 estudos científicos integrados na revisão sistemática. Foram igualmente analisados documentos institucionais, legais e normativos nacionais e europeus, que sustentam o enquadramento conceptual do plano, apresentados nos capítulos seguintes e listados na bibliografia final. A caracterização das fontes considerou o tipo de publicação, origem geográfica, ano e contributo temático. Identificaram-se estudos empíricos, revisões sistemáticas e relatórios técnicos, com predominância de publicações recentes (2020–2025), demonstrando a atualidade do tema. Geograficamente, observou-se uma forte representação europeia, sobretudo de Portugal, Espanha e Reino Unido, complementada por contributos internacionais que ampliaram a compreensão das tendências e desafios da integração da cibersegurança nos sistemas educativos**.** Os contributos temáticos foram agrupados em cinco eixos: (1) políticas e enquadramentos normativos; (2) formação e capacitação digital da comunidade educativa; (3) práticas pedagógicas e literacia digital; (4) medidas organizacionais e tecnológicas; e (5) sensibilização e cultura de segurança. Estes eixos estruturam a revisão do Capítulo 2 e fundamentam o diagnóstico e o Plano apresentados nos capítulos seguintes.

Por fim, relatórios da ENISA, do CNCS e da Comissão Europeia forneceram o enquadramento político e estratégico da investigação. As fichas-resumo das fontes encontram-se no Apêndice A, e a síntese dos referenciais normativos e modelos de maturidade digital e cibersegurança, no Apêndice B. Em conjunto, esta amostra documental constitui a base teórica e empírica da investigação, garantindo que o plano de cibersegurança do Capítulo 5 assenta em evidência científica atualizada e comparável a boas práticas internacionais.

3.5. Validade, fiabilidade e ética

A validade do estudo foi assegurada pela triangulação das fontes e pela aplicação rigorosa dos critérios da metodologia PRISMA 2020 (Page et al., 2021). A fiabilidade decorre da descrição pormenorizada de todas as etapas e da possibilidade de replicação por outros investigadores, garantindo consistência e transparência metodológica. A ética foi garantida pelo cumprimento do Regulamento Geral sobre a Proteção de Dados (Regulamento [UE] 2016/679) e das Diretrizes da CNPD (2018/1; 2023/1). Nenhum dado pessoal foi recolhido, e todas as fontes utilizadas são de acesso público e devidamente referenciadas. O formulário de diagnóstico, respondido pela Direção do Agrupamento em representação institucional, assegurou a validade e fiabilidade da informação recolhida. O estudo foi desenvolvido de forma independente, sem qualquer financiamento externo.

3.6. Considerações finais

A aplicação da metodologia PRISMA 2020 neste estudo garantiu transparência e rigor na seleção e análise das fontes, reforçando a coerência entre os objetivos da investigação e a proposta de intervenção. O enquadramento ético e normativo contribuiu para a credibilidade do processo e para a fiabilidade dos resultados obtidos.

Em conjunto, os procedimentos adotados asseguram a robustez científica e a reprodutibilidade da investigação, constituindo uma base sólida para o diagnóstico institucional e para a elaboração do Plano de Cibersegurança apresentado no Capítulo 5.

CAPÍTULO 4

Diagnóstico do estado atual

O presente capítulo analisa o estado atual da maturidade digital e da cibersegurança no Agrupamento de Escolas Passos Manuel, constituindo a base do plano apresentado no capítulo seguinte. O diagnóstico resulta da análise combinada de documentos institucionais, indicadores internos e externos e dos dados recolhidos através do Formulário de Diagnóstico de Cibersegurança, complementados por informações obtidas em conversas informais com a Direção do Agrupamento. A caracterização institucional e social do AEPM, a análise dos seus documentos estruturantes, a observação de indicadores locais e nacionais e a avaliação das práticas digitais existentes permitem identificar vulnerabilidades e definir áreas prioritárias de intervenção, essenciais para o reforço da resiliência cibernética da escola.

4.1. Caracterização do Agrupamento de Escolas Passos Manuel

O Agrupamento de Escolas Passos Manuel (AEPM), situado em Lisboa, integra seis estabelecimentos de ensino: a escola-sede, Escola Básica e Secundária Passos Manuel e cinco escolas do 1.º ciclo com jardim de infância (EB Gaivotas, EB Luísa Ducla Soares, EB Maria Barroso, EB Padre Abel Varzim e EB São José). A sua área de influência abrange as freguesias de Misericórdia, Santo António, Santa Maria Maior e Arroios, zonas centrais da cidade marcadas por grande diversidade socioeconómica e cultural, refletida numa comunidade escolar inclusiva e multicultural.

No ano letivo de 2025/2026, o AEPM acolhe 1 375 alunos distribuídos por 70 turmas, desde a educação pré-escolar ao ensino secundário. Destes, 40 % são estrangeiros (43 nacionalidades), 26 % beneficiam de apoios da Ação Social Escolar e 8 % apresentam necessidades educativas especiais. Estes indicadores confirmam o perfil de uma escola urbana inclusiva, com desafios acrescidos de equidade e diferenciação pedagógica. O corpo profissional, composto por mais de 200 docentes, assistentes e técnicos especializados, garante uma média de dez alunos por professor, favorecendo um acompanhamento pedagógico próximo. A missão do AEPM assenta na promoção do conhecimento, da equidade e da inclusão, valorizando o trabalho colaborativo, a inovação pedagógica e a autonomia estudantil, em consonância com o *Perfil dos Alunos à Saída da Escolaridade Obrigatória* (ME, 2017). Documentos estruturantes como o Projeto Educativo 2023–2026, o Regulamento Interno, a Estratégia

de Educação para a Cidadania na Escola (EECE 2023/24) e o Plano de Ação para o Desenvolvimento Digital da Escola (PADDE 2021–2023) expressam esta orientação, embora revelem fragilidades, nomeadamente a ausência de uma política integrada de cibersegurança e a necessidade de atualização do PADDE.

O AEPM encontra-se em processo de candidatura ao programa TEIP 4, reforçando o compromisso com a inclusão e a redução do abandono escolar. Em setembro de 2025, o Conselho Pedagógico aprovou o regimento interno de utilização de dispositivos móveis, em conformidade com o Decreto-Lei n.º 95/2025, demonstrando uma crescente preocupação com a segurança digital. Paralelamente, a implementação da plataforma Ubbu nos três ciclos do ensino básico reforça a aposta na literacia digital e na integração da cidadania digital nos currículos, exigindo políticas adequadas de autenticação e proteção de dados. Do ponto de vista pedagógico e organizacional, o AEPM conjuga tradição e inovação, promovendo a literacia digital e a sensibilização para a cibersegurança como pilares da formação de cidadãos conscientes e preparados para os desafios do século XXI. A referência ao *Referencial de Competências em Cibersegurança* (CNCS, 2022) reforça esta linha, embora subsista a necessidade de uma estratégia articulada que alinhe práticas e infraestruturas com os normativos nacionais e europeus.

Esta caracterização institucional enquadra o diagnóstico técnico e pedagógico desenvolvido nas secções seguintes. A diversidade cultural, o número de alunos e turmas, a dimensão do corpo docente e técnico e os índices de apoio social evidenciam a importância de políticas consistentes de equidade, literacia digital e gestão de infraestruturas. Este contexto justifica a análise empírica realizada através do Formulário de Diagnóstico de Cibersegurança (Direção AEPM, 13 de setembro de 2025), cujos resultados fundamentam a proposta de um plano de cibersegurança ajustado à realidade do agrupamento.

4.2. Documentos estruturantes e análise documental

A análise documental incidiu sobre os principais instrumentos de gestão e orientação pedagógica do Agrupamento de Escolas Passos Manuel, Projeto Educativo 2023–2026, Plano de Ação para o Desenvolvimento Digital da Escola (PADDE 2021–2023), Estratégia de Educação para a Cidadania na Escola (EECE 2023/2024), Regulamento Interno 2024 e Plano de Ação TEIP 2024–2027 por representarem os eixos estruturantes da política educativa e evidenciarem o grau de integração da dimensão digital e da cibersegurança na prática institucional.

O Projeto Educativo 2023–2026 organiza-se em quatro eixos, sucesso escolar, inclusão, inovação pedagógica e cidadania, valorizando a literacia digital e a integração tecnológica, em alinhamento com o *Perfil dos Alunos à Saída da Escolaridade Obrigatória* (ME, 2017). Contudo, embora reconheça a importância da tecnologia, não define políticas operacionais de segurança digital (gestão de acessos, proteção de dados, resposta a incidentes). Esta ausência é significativa, dado o alinhamento declarado com o *Plano de Cibersegurança na Educação* (CNCS, 2021), sem, porém, a correspondente tradução em medidas técnicas ou responsabilidades formais.

O PADDE 2021–2023 estrutura-se em três dimensões, infraestruturas, competências digitais e práticas pedagógicas, destacando a formação docente e o uso de plataformas digitais. Apesar da aposta na transição digital, o plano omite controlos técnicos essenciais previstos na norma ISO/IEC 27002:2022, como autenticação multifator (8.2), gestão de credenciais (8.3), proteção contra *malware* (8.7), *logging* e monitorização (8.15–8.17) ou segregação de redes (8.20 e 8.22). Acresce o facto de não ter sido atualizado após 2023, revelando uma fragilidade organizacional que limita a evolução digital sustentável do agrupamento.

A EECE 2023/2024 integra o domínio da Cidadania Digital, abordando o uso responsável da tecnologia, a privacidade e o combate à desinformação, numa perspetiva de escola inclusiva. Todavia, as metas formativas não se articulam com medidas técnicas de suporte (perfis de acesso, armazenamento de dados ou reporte de incidentes), o que compromete a operacionalização das intenções educativas.

O Regulamento Interno 2024 define normas de funcionamento e proteção de dados em conformidade com o RGPD e a Lei n.º 58/2019, mas as referências à segurança digital mantêm-se genéricas, sem políticas específicas para monitorização de acessos, eliminação segura de informação ou atribuição de responsabilidades técnicas (artigos 5.º, 24.º e 32.º do RGPD).

O Plano de Ação TEIP 2024–2027 valoriza o sucesso escolar, a inclusão e a cidadania, através de iniciativas como o Laboratório para a Aprendizagem e Inclusão (LAI), a tutoria e coadjuvação, o uso de inteligência artificial na educação e o projeto Academia Digital para Pais. Apesar da articulação com programas nacionais, o plano não contempla mecanismos de proteção da informação nem enquadramento de cibersegurança.

A superação desta fragilidade não depende exclusivamente da definição de um plano formal, mas da sua integração em processos contínuos de governação e atualização, apoiados numa implementação faseada que favoreça a adesão progressiva dos diferentes intervenientes e contribua para a consolidação da cibersegurança como uma necessidade estruturante da organização, num contexto marcado pelo dinamismo das ameaças digitais.

Em síntese, os documentos de gestão do AEPM evidenciam uma visão pedagógica que reconhece a importância da segurança digital, mas carecem de medidas técnicas, organizacionais e formativas

concretas. Confirma-se, assim, a necessidade de uma estratégia institucional integrada e alinhada com os normativos nacionais e europeus.

4.3. Indicadores e diagnóstico técnico

A Direção do Agrupamento de Escolas Passos Manuel (AEPM) definiu um conjunto de indicadores destinados a aferir o grau de maturidade digital e a resiliência em cibersegurança da instituição. Estes dados permitem caracterizar a situação atual e constituem a base empírica para a elaboração do plano de cibersegurança.

4.3.1. Indicadores locais

A recolha de indicadores locais revelou-se essencial para compreender a maturidade digital e a resiliência cibernética do AEPM, sobretudo na ausência de séries nacionais publicadas. Em setembro de 2025, verificou-se que a autenticação multifator (MFA) se encontra apenas parcialmente implementada e que o inventário centralizado de equipamentos está ainda em fase de elaboração (cf. Capítulo 4.4). Estes resultados evidenciam progressos relevantes, mas também lacunas que exigem consolidação técnica e organizacional. Apesar de preliminares, os dados recolhidos permitem articular a evidência empírica com referenciais normativos europeus e nacionais, assegurando uma leitura fiável e integrada da maturidade digital do agrupamento.

4.3.2. Indicadores nacionais complementares

A articulação entre os indicadores locais e os dados nacionais permite situar o AEPM face às políticas públicas de literacia e segurança digital. No ano letivo 2024/2025, o programa Desafios SeguraNet envolveu 455 agrupamentos, 944 docentes, 61 882 alunos e 180 pais, com 150 certificações no Mês da Cibersegurança e 170 no Dia da Internet Mais Segura. A iniciativa Líderes Digitais contou com 76 agrupamentos, 1 895 alunos e 40 apresentações em painéis nacionais e europeus.
O projeto Academia Digital para Pais, desenvolvido pela Direção-Geral da Educação e pela E-Redes, contou com 205 escolas participantes. Os Laboratórios de Educação Digital (LED) abrangeram 1 300

laboratórios em 803 agrupamentos e envolveram 6 193 professores certificados. Já o Projeto-Piloto de Manuais Digitais decorreu em 81 agrupamentos, com 674 turmas e 13 635 alunos abrangidos.
Estes dados enquadram as práticas do AEPM no esforço nacional de transformação digital das escolas, reforçando a validade do diagnóstico e sustentando a definição de metas e prioridades de ação. Importa, contudo, reconhecer que estes indicadores, maioritariamente associados a iniciativas e momentos temáticos, não traduzem por si só uma abordagem contínua e estruturada à cibersegurança, a qual exige integração permanente nas práticas organizacionais e pedagógicas.

4.3.3. Limitações e validação futura

As fragilidades documentais e técnicas identificadas foram confirmadas pelo diagnóstico empírico realizado através do *Formulário de Diagnóstico de Cibersegurança* (Direção AEPM, 13 de setembro de 2025), que evidenciou a necessidade de integrar medidas de cibersegurança nos documentos estruturantes do agrupamento.

O diagnóstico apresentado deve ser entendido como preliminar, prevendo-se a recolha complementar de dados junto da Direção e das equipas técnicas, mediante o mesmo protocolo de análise temática e triangulação. A atualização contínua destes indicadores terá em conta as orientações da Direção-Geral da Educação (DGE/ERTE) e do Centro Nacional de Cibersegurança (CNCS), tomando como referência os quadros metodológicos e os estudos desenvolvidos pela Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto (FPCEUP), de forma a garantir o alinhamento com métricas nacionais e referenciais europeus.

4.4. Infraestrutura digital e práticas pedagógicas

A infraestrutura digital do Agrupamento de Escolas Passos Manuel (AEPM) reflete a dimensão e diversidade da sua comunidade educativa, exigindo uma gestão rigorosa de recursos tecnológicos e identidades digitais. Com uma rede alargada de utilizadores e dispositivos, o agrupamento enfrenta desafios de interoperabilidade, segurança e equidade no acesso às tecnologias. Este diagnóstico analisa os principais componentes técnicos e pedagógicos que sustentam o ecossistema digital do AEPM, avaliando o nível de maturidade, as rotinas de segurança e as práticas associadas à aprendizagem digital.

4.4.1. Rede segurança perimental

A infraestrutura de rede do Agrupamento de Escolas Passos Manuel integra uma componente física cablada para suporte das operações internas e uma rede Wi-Fi institucional destinada ao acesso de docentes, alunos e convidados, protegida por firewall de próxima geração (NGFW) e mecanismos de deteção de intrusões (IDS/IPS). A rede é gerida através de ciclos regulares de atualização de *firmware* e regras de segurança.

Apesar da funcionalidade, persistem limitações relacionadas com a largura de banda contratada e a ausência de relatórios técnicos periódicos, o que reduz a visibilidade sobre o desempenho e a resiliência do sistema. Recomenda-se a migração gradual para o protocolo WPA3/802.1X com EAP**,** assegurando a separação de perfis e a integração de um *captive portal* para acessos de convidados. Para docentes e alunos, é igualmente pertinente implementar filtros de conteúdos e relatórios estatísticos sobre bloqueios e exceções, equilibrando segurança e usabilidade. A análise apresentada incide sobre a resiliência da infraestrutura de rede e da segurança perimetral, sendo a resiliência dos serviços, sistemas e dados aprofundada nas subsecções 4.4.4 a 4.4.6 do diagnóstico.

4.4.2. Gestão de identidades e acessos

A criação de contas institucionais e cartões escolares para novos alunos, atualmente assegurada pela Biblioteca Escolar/Centro de Recursos Educativos (BE/CRE), constitui uma boa prática de integração digital (*onboarding*). Contudo, a ausência de métricas sobre a cobertura da autenticação multifator (MFA), a integração de *Single Sign-On* (SSO) e os prazos de desativação de contas nos processos *joiner–mover–leaver* (JML) limita a maturidade do sistema de *Identity and Access Management* (IAM).

Como metas prioritárias, propõe-se a obrigatoriedade de MFA para docentes e administrativos até ao final do primeiro período, a desativação de contas no máximo de 24 horas após a saída do utilizador e a publicação de relatórios semestrais de conformidade. Estas medidas reforçarão a rastreabilidade e a segurança dos acessos institucionais.

4.4.3. Endpoints e dispositivos móveis

O AEPM dispõe de um parque tecnológico alargado, reforçado pela política de empréstimo de computadores a alunos, promovendo a inclusão digital. Contudo, é necessária a consolidação de um

inventário atualizado de equipamentos, conforme a norma ISO/IEC 27002:2022[1] (controlos 5.9 e 8.1), a adoção de soluções de deteção e resposta em *endpoints* (EDR)[2] e a expansão da gestão centralizada por *Mobile Device Management* (MDM)[3].

Os objetivos de referência estabelecem que pelo menos 80 % dos dispositivos estejam sob gestão MDM e que 95 % possuam encriptação ativa. O prazo máximo para correção de vulnerabilidades críticas deverá ser de 15 dias, e a percentagem de equipamentos com permissões administrativas locais não deverá exceder 10 %. Estes parâmetros garantem coerência entre segurança operacional e acessibilidade pedagógica.

4.4.4. Serviços críticos, cópias de segurança e continuidade

Os serviços digitais centrais, como as plataformas de gestão escolar, o correio eletrónico institucional e os sistemas administrativos, devem possuir metas definidas de *Recovery Point Objective* (RPO) e *Recovery Time Objective* (RTO)[4]. O objetivo é assegurar a continuidade operacional e a recuperação rápida dos dados em caso de falha.

No AEPM, propõe-se que a plataforma SIGE e o sistema Inovar PAA tenham RPO de 24 horas e RTO de 48 horas, com dois testes anuais de restauro; que o correio eletrónico institucional mantenha RPO de 12 horas e RTO de 24 horas; e que os arquivos pedagógicos possuam RPO de 48 horas e RTO de 72 horas, com pelo menos um teste anual. Estes valores seguem as recomendações da norma ISO/IEC 27031:2011 e asseguram resiliência face a incidentes ou interrupções.

4.4.5. Vulnerabilidades, monitorização e resposta a incidentes

Apesar de o AEPM dispor de *firewall* e de mecanismos de deteção de intrusões (IDS/IPS), não existem ainda rotinas sistemáticas de análise de vulnerabilidades nem métricas consolidadas sobre o tempo médio de deteção (MTTD) e o tempo médio de resposta (MTTR).

---

[1] *A ISO/IEC 27002:2022 estabelece práticas e controlos de segurança da informação; neste capítulo referem-se, entre outros, os controlos 5.9 (inventário de ativos), 8.1 (gestão de endpoints), 8.2 (autenticação), 8.3 (palavras-passe), 8.7 (proteção contra malware/EDR), 8.15–8.17 (registo e monitorização), 8.18 (sincronização temporal), 8.20 e 8.22 (segmentação e segurança de redes).*

[2] Endpoint Detection and Response (EDR) refere-se a soluções de monitorização e resposta automática a ameaças em dispositivos terminais (computadores, tablets, etc.), permitindo deteção precoce e mitigação de incidentes.

[3] Mobile Device Management (MDM) é um sistema de gestão centralizada de dispositivos móveis que permite configurar políticas de segurança, controlar atualizações e proteger dados em equipamentos institucionais.

[4] RPO (Recovery Point Objective) define a quantidade máxima de dados aceitável a perder após um incidente; RTO (Recovery Time Objective) indica o tempo máximo admissível para restabelecer um serviço crítico.

Recomenda-se a realização de análises mensais de vulnerabilidades, priorizando a resolução de falhas críticas em menos de sete dias, conforme o sistema CVSS[1]. Os registos de sistema e de rede deverão ser integrados numa ferramenta centralizada de *Security Information and Event Management* (SIEM), garantindo visibilidade sobre os eventos e alertas de segurança. Como metas operacionais, definem-se um MTTD inferior a 24 horas e um MTTR até cinco dias úteis, assegurando resposta célere e eficaz a incidentes.

4.4.6. Plataformas pedagógicas, inclusão e acessibilidade

O AEPM utiliza diversas plataformas digitais de apoio à aprendizagem, como a Ubbu (1.º–3.º ciclos) e o Inovar PAA para gestão de atividades. Estas ferramentas têm elevado potencial pedagógico, mas exigem curadoria de conteúdos, avaliações de impacto sobre a privacidade (DPIA/TIA) e monitorização contínua da conformidade com o RGPD. Em termos de maturidade digital, o *Google Workspace* apresenta DPIA concluída, com base em contrato e consentimento, registando 95 % de aceitação da política de utilização (AUP) pelos alunos. A Ubbu, sustentada em interesse público, encontra-se em fase de avaliação de impacto e com 80 % de aceitação da AUP. Já o Inovar PAA, baseado em obrigação legal, dispõe de DPIA concluída e 100 % de aceitação entre os docentes. Estes resultados demonstram avanços significativos na conformidade e na integração segura das ferramentas digitais do agrupamento.

De forma global, o AEPM dispõe de uma infraestrutura digital sólida e em crescimento, embora ainda careça de sistematização de indicadores, rotinas de segurança cibernética e mecanismos formais de inclusão digital. A concretização das medidas propostas, como a atualização do inventário de equipamentos, autenticação reforçada, gestão de vulnerabilidades, definição de RPO/RTO, formação contínua e curadoria de plataformas, permitirá alinhar a prática institucional com as normas internacionais (ISO/IEC 27002:2022), as diretrizes do CNCS e os requisitos regulamentares do RGPD e da CNPD.

4.5. Necessidades e vulnerabilidades identificadas

[1] O Common Vulnerability Scoring System (CVSS) é uma escala internacional que classifica vulnerabilidades de software e hardware segundo a sua gravidade, permitindo priorizar correções e mitigação de riscos.

A análise cruzada entre os documentos estruturantes, Regulamento Interno 2024, PADDE 2021–2023, Projeto Educativo 2023–2026 e Estratégia de Educação para a Cidadania na Escola 2023/24, os dados recolhidos através do Formulário de Diagnóstico de Cibersegurança (Direção AEPM, 13 de setembro de 2025) e o diagnóstico técnico descrito na secção 4.4, permitiu identificar sete domínios críticos que influenciam a maturidade digital e a resiliência do Agrupamento de Escolas Passos Manuel (AEPM).

4.5.1. Políticas e enquadramento organizacional

O diagnóstico confirma a existência de uma política formal de segurança informática, revista em janeiro de 2024. Contudo, o AEPM ainda não dispõe de uma política de cibersegurança integrada, aprovada pela comunidade educativa e alinhada com a norma ISO/IEC 27001:2022 (cláusulas 5.1 e 5.2) e com o Regulamento Geral sobre a Proteção de Dados (RGPD, art.º 24.º). Torna-se, assim, prioritário elaborar, aprovar e divulgar uma política institucional de cibersegurança com revisão anual e matriz de responsabilidades RACI, conforme será detalhado na Fase I – Gestão (Cap. 4.6).

4.5.2. Procedimentos e conformidade legal

Atualmente, os incidentes são reportados por canais dispersos, livro físico, sistema interno e correio eletrónico sem um fluxo formal de comunicação. Além disso, o agrupamento não realiza auditorias internas periódicas, o que evidência riscos de não conformidade com os artigos 33.º e 34.º do RGPD (notificação de violação de dados pessoais) e do artigo 19.º da Diretiva NIS 2[1] (gestão e reporte de incidentes). É fundamental instituir auditorias internas e externas regulares, criar um formulário digital normalizado para reporte de incidentes e definir métricas de deteção, notificação e correção (MTTA e MTTR). Estas medidas garantirão rastreabilidade, transparência e melhoria contínua da conformidade legal e operacional.

4.5.3. Infraestruturas e sistemas

[1] A Diretiva (UE) 2022/2555 — NIS 2 — define requisitos de gestão de risco e reporte de incidentes; no texto destacam-se os art.º 19.º (medidas técnicas/organizacionais) e 21.º–22.º (gestão, notificação e prazos).

O AEPM dispõe de cobertura Wi-Fi integral, segmentação por perfis de utilizador, *firewall* de nova geração e mecanismos IDS/IPS, com atualizações trimestrais de *firmware* e regras de segurança. Existem cópias de segurança regulares, suportadas por registos administrativos de aquisição de equipamentos; contudo, o inventário técnico centralizado e atualizado de equipamentos e software permanece em fase de consolidação. Este contexto reforça a necessidade de concluir um inventário centralizado e dinâmico, sobretudo tendo em conta o aumento de dispositivos emprestados a alunos. Para reforçar a segurança operacional, recomenda-se a implementação de *logging* centralizado com *dashboards* em tempo real (ISO/IEC 27002:2022, controlos 8.15–8.17; NIS 2, art.º 19.º), a reconciliação mensal de ativos (controlo 5.9) e a evolução do antivírus para uma solução EDR com relatórios trimestrais de conformidade (controlo 8.7).

4.5.4. Práticas digitais e rotinas de acesso

O agrupamento adota métodos diversificados de autenticação como palavra-passe, cartões RFID e autenticação de dois fatores, mas a MFA ainda não é obrigatória em todos os sistemas. As políticas de palavra-passe permanecem parciais e as *checklists* de segurança encontram-se em elaboração. Em setembro de 2025, o Conselho Pedagógico aprovou o regimento de utilização de dispositivos móveis, em conformidade com o *Decreto-Lei n.º 95/2025*, aplicável ao 1.º e 2.º ciclos do ensino básico. Esta regulamentação requer ações de sensibilização dirigidas a alunos, docentes e encarregados de educação, bem como mecanismos de fiscalização com reporte trimestral ao Conselho Pedagógico.

Recomenda-se tornar obrigatória a MFA em todas as aplicações críticas (controlo 8.2), padronizar políticas de palavra-passe com um mínimo de 12 caracteres e rotação semestral (controlo 8.3), publicar *checklists* de segurança adaptadas a cada perfil de utilizador e implementar um plano de sensibilização e fiscalização do regimento de telemóveis, assegurando coerência pedagógica e disciplinar.

4.5.5. Formação e sensibilização

A formação em segurança digital apresenta periodicidade irregular e depende, em parte, de recursos externos. O diagnóstico evidencia maior necessidade formativa nas áreas de segurança digital e gestão de aplicações. A introdução da plataforma *Ubbu* para os 1.º, 2.º e 3.º ciclos constitui uma oportunidade para desenvolver aprendizagens em cidadania digital e privacidade.

Em consonância com a *Resolução do Conselho de Ministros n.º 127/2025*, que aprova a Estratégia Nacional de Educação para a Cidadania, propõe-se estruturar um programa anual de formação composto por micro módulos destinados a alunos, docentes, não docentes e encarregados de educação. Estes módulos deverão abordar temas como uso responsável de dispositivos móveis, privacidade online e segurança nas plataformas educativas (*Ubbu* e *Google Workspace*), avaliando o impacto através de questionários pós-formação e métricas de participação (cf. Cap. 4.7 – Plano de Formação).

4.5.6. Cultura organizacional e gestão de risco

O AEPM apresenta práticas positivas de gestão personalizada de acessos a sistemas críticos, mas enfrenta riscos como a utilização de aplicações externas não autorizadas e a partilha inconsciente de dados. A escassez de orçamento e de literacia digital agrava estas limitações. A diversidade cultural e linguística da comunidade com 40 % de alunos estrangeiros e 8 % com necessidades educativas especiais, exige políticas de inclusão digital, incluindo *Acceptable Use Policies* (AUP) multilingues e garantia de acessibilidade digital segundo as diretrizes WCAG.

Recomenda-se a implementação de um processo formal de gestão de riscos (ISO/IEC 27001:2022, cláusula 6.1), o reforço das medidas de segurança no tratamento de dados (RGPD, art.º 32.º), a monitorização da cultura digital por meio de autoavaliações semestrais (SELFIE, domínio “Segurança”) e a alocação de um orçamento específico para ferramentas e programas de literacia digital, seguindo o ciclo de melhoria contínua PDCA descrito no Capítulo 4.6.

4.5.7. Síntese e transição

Em síntese, embora as infraestruturas digitais do AEPM revelem robustez e compromisso com a inovação, persistem lacunas em auditorias, políticas integradas, rotinas de segurança, formação sistemática, inclusão digital e gestão de risco. Estas necessidades sustentam o futuro Plano de Implementação (Cap. 4.6) e o Plano de Formação (Cap. 4.7), assegurando tratamento verificável, métricas de auditoria e monitorização calendarizada, em coerência com o Plano Anual de Atividades (PAA) e com os prazos definidos pelo Conselho Pedagógico.

4.6. Síntese do diagnóstico e justificação da proposta

A análise integrada realizada neste capítulo, que combinou o enquadramento institucional e metodológico (4.1), a avaliação documental (4.2), os indicadores de referência (4.3), a caracterização da infraestrutura digital e das práticas pedagógicas (4.4) e a identificação das necessidades e vulnerabilidades (4.5), permite concluir que o Agrupamento de Escolas Passos Manuel dispõe de uma base tecnológica relevante, embora careça de consolidação ao nível da gestão, da conformidade e das práticas operacionais. O reforço destas dimensões é indispensável para garantir resiliência, inclusão e segurança na aprendizagem digital.

4.6.1. Evidências-chave do diagnóstico

A análise dos resultados evidencia cinco áreas críticas: gestão e conformidade**,** infraestrutura e operação**,** identidade e acessos (IAM)**,** plataformas e privacidade e capacitação e cultura digital.
No domínio da gestão e conformidade, o agrupamento dispõe de uma política de segurança informática revista em janeiro de 2024, mas ainda carece de uma política institucional de cibersegurança integrada e validada pela comunidade. Persistem fluxos dispersos de reporte de incidentes e ausência de auditorias internas, em desconformidade com os art.º 33.º e 34.º do RGPD e os art.º 21.º e 22.º da Diretiva NIS 2 (UE, 2022).

Em infraestrutura e operação, observa-se uma rede segmentada, protegida por *firewall* de próxima geração com IDS/IPS e atualizações regulares. Contudo, faltam um sistema centralizado de *logging*, monitorização contínua, inventário atualizado de ativos e gestão de vulnerabilidades por criticidade. O aumento do empréstimo de equipamentos a alunos reforça a necessidade de soluções MDM, EDR e encriptação por defeito, bem como a definição de RPO/RTO e realização de testes de restauro regulares, em conformidade com a ISO/IEC 27002:2022 (controlos 8.15–8.17, 8.7 e 5.9) e o art.º 19.º da Diretiva NIS 2. Na área de identidade e acessos, persistem métodos de autenticação heterogéneos, cobertura insuficiente de MFA, políticas de palavras-passe não uniformes e ausência de prazos definidos nos processos *joiner–mover–leaver* (JML), fragilizando o controlo de acessos. Relativamente a plataformas e privacidade, o uso de ferramentas como a Ubbu e o Inovar PAA constitui uma oportunidade pedagógica relevante, mas exige curadoria de conteúdos, avaliações de impacto na proteção de dados (DPIA/TIA, art.º 35.º do RGPD) e divulgação eficaz das políticas de utilização aceitável (AUP). O regimento de telemóveis, aprovado ao abrigo do Decreto-Lei n.º 95/2025, reforça a importância da sensibilização e fiscalização consistentes.

Por fim, no eixo da capacitação, cultura e inclusão digital, a formação em cibersegurança mantém-se irregular. Urge implementar um programa anual adaptado a diferentes perfis, entre eles, alunos, docentes, não docentes e encarregados de educação, articulado com o currículo de Cidadania e Desenvolvimento (Resolução do Conselho de Ministros n.º 127/2025). O perfil demográfico do AEPM, com 40 % de alunos estrangeiros e 8 % com necessidades educativas especiais (NEE), reforça a importância de regulamentos e AUP multilingues, acessibilidade digital conforme as normas WCAG e apoio diferenciado que garanta equidade no acesso.

4.6.2. Priorização de riscos e impactos

A priorização qualitativa dos domínios críticos, considerando impacto e urgência, demonstra que a gestão de identidades e acessos com enfoque em MFA, políticas de palavra-passe e prazos JML, apresenta impacto muito alto e urgência muito alta, por constituir o principal vetor de compromisso e permitir redução imediata de risco.

O inventário de ativos, a gestão centralizada por MDM, a adoção de EDR e a encriptação por defeito evidenciam impacto muito alto e urgência alta, dada a dimensão do parque tecnológico e o regime de empréstimos a alunos. O *logging* centralizado com SIEM e a gestão de vulnerabilidades segundo o sistema CVSS têm impacto muito alto e urgência alta, ao garantirem deteção célere e correção dentro de prazos definidos. A definição de RPO/RTO e a realização de testes de restauro periódicos apresentam impacto alto e urgência alta, assegurando continuidade dos serviços críticos. As DPIA/TIA e a consolidação das AUP revelam impacto alto e urgência média, centrando-se na conformidade e segurança pedagógica. O regimento de telemóveis apresenta impacto médio e urgência alta, pela relevância comportamental e de segurança em contexto escolar. A formação e a cultura digital registam impacto alto e urgência média, sustentando a mudança comportamental a médio prazo.

Por fim, a inclusão e a acessibilidade digital exibem impacto médio e urgência média, garantindo equidade e eficácia pedagógica num contexto multicultural. Esta classificação decorre das secções 4.4 e 4.5 e segue critérios de probabilidade e consequência, em alinhamento com a *ISO/IEC 27001:2022* e com a *Diretiva NIS 2*.

4.6.3. Justificação da proposta

Cada eixo da proposta apresentada no Capítulo 5 decorre diretamente das lacunas diagnosticadas neste capítulo.

O eixo Gestão e Conformidade propõe a criação de uma política institucional de cibersegurança, a definição de uma matriz RACI, a implementação de auditorias internas e externas, o desenvolvimento de um formulário digital normalizado para reporte de incidentes e o alinhamento com as normas *ISO/IEC 27001* e *27002*, com o *RGPD* e com a *NIS 2*.

O eixo Infraestrutura e Operação Segura prevê a criação de um inventário vivo de equipamentos e software, a implementação de soluções MDM, EDR e de encriptação de disco, o reforço da monitorização através de SIEM e *logging* centralizado e a gestão de vulnerabilidades baseada no CVSS. Inclui ainda a definição de RPO e RTO e a calendarização de testes de restauro.

O eixo Dados e Privacidade recomenda a realização de DPIA/TIA para todas as plataformas digitais, a revisão e disseminação das AUP por perfis de utilizador e a aplicação de políticas de minimização e retenção de dados, em conformidade com o *RGPD* (*art.º* 35.º) e a *ISO/IEC 27002:2022* (controlo 5.34).

O eixo Educação e Cultura Digital Segura propõe um programa anual de formação por perfis, com conteúdos sobre utilização responsável de dispositivos móveis (*DL n.º 95/2025*), privacidade, MFA e cidadania digital (*RCM n.º 127/2025*), integrados num ciclo de melhoria contínua (PDCA) conforme descrito no Capítulo 5.

4.6.4. Objetivos operacionais e indicadores (KPIs)

A proposta será acompanhada por indicadores de desempenho que asseguram monitorização contínua e mensurável. Prevê-se alcançar cobertura de MFA igual ou superior a 90 % nos docentes e administrativos até ao final do primeiro período letivo, garantir reconciliação mensal do inventário com 95 % de cobertura dos ativos e manter sob gestão MDM pelo menos 80 % dos dispositivos com encriptação ativa em 95 % dos casos. Todas as vulnerabilidades críticas (CVSS ≥ 9) deverão ser resolvidas em sete dias ou menos; os serviços críticos terão RPO e RTO definidos e dois testes de restauro anuais com ≥ 90 % de sucesso; o *logging*/SIEM deverá produzir relatórios trimestrais para o Conselho Pedagógico e para o DPO, mantendo MTTD ≤ 24 horas e MTTR ≤ 5 dias úteis. Pretende-se ainda garantir conformidade com o RGPD através da conclusão de DPIA para 100 % das plataformas e da aceitação das AUP por ≥ 95 % dos alunos e 100 % dos docentes. Na vertente formativa, prevê-se que ≥ 80 % dos docentes frequentem, anualmente, pelo menos uma ação de formação por período, com nível médio de satisfação igual ou superior a 4/5.

Finalmente, assegura-se a publicação de regulamentos e AUP multilingues e a validação semestral dos recursos digitais em conformidade com as normas WCAG.

4.6.5. Princípios de implementação

O plano assenta nos princípios da proporcionalidade e da gestão de risco, garantindo proteção de dados desde a conceção e por defeito (*RGPD*, *art.º* 25.º). Valoriza-se a evidência e a auditabilidade, com registos e relatórios sistemáticos, uma abordagem faseada com marcos definidos no *Plano Anual de Atividades* (PAA) e nos prazos do Conselho Pedagógico, e o equilíbrio entre segurança e usabilidade, segundo o princípio pedagógico-primeiro (*security by design, learning by priority*). A inclusão e a acessibilidade digital constituem princípios estruturantes, prevendo-se recursos multilingues e conformidade com as normas WCAG.

4.6.6. Dependências e riscos de implementação

A concretização das medidas depende das capacidades da equipa TIC e da disponibilidade de tempo, mitigando-se esta limitação com a definição clara de responsabilidades RACI e a calendarização das tarefas. As restrições orçamentais poderão ser atenuadas pelo faseamento das ações e pela maximização de licenças e ferramentas já existentes. A adesão organizacional será promovida por estratégias de comunicação, formação e envolvimento do Conselho Pedagógico e da Direção. As integrações técnicas deverão ser precedidas de projetos-piloto com critérios de aceitação explícitos e documentação dos resultados.

4.6.7. Síntese final e transição

Em síntese, o diagnóstico demonstra que o AEPM possui base tecnológica consolidada, mas revela fragilidades em auditoria, políticas, formação e inclusão digital. As medidas delineadas no ***Capítulo 5. Plano de Cibersegurança para o Agrupamento Passos Manuel*** respondem diretamente a essas lacunas, estruturando uma intervenção sustentada, verificável e calendarizada. O plano propõe métricas de monitorização e auditoria contínua, em coerência com o *PAA* e com os *art.º* 37.º a 40.º do *Regulamento Interno*[1], assegurando avaliação interna e melhoria contínua.

[1] Os art.º 37.º–40.º do Regulamento Interno do AEPM estabelecem a avaliação interna, autoavaliação e mecanismos de monitorização/relato, enquadrando ciclos de melhoria e prestação de contas.

CAPÍTULO 5

Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel

O presente capítulo apresenta a proposta de Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel, construída a partir das necessidades identificadas no diagnóstico e orientada pelos referenciais nacionais e europeus em matéria de segurança digital. O plano integra medidas técnicas, organizacionais e pedagógicas, concebidas para reforçar a proteção dos sistemas, a conformidade legal e a capacitação da comunidade educativa.

A estrutura do capítulo reflete a natureza aplicada do estudo, articulando objetivos, princípios orientadores, modelo de gestão e eixos estratégicos. São detalhadas as medidas a implementar, as fases de execução e os mecanismos de monitorização e avaliação, assegurando a coerência entre a governação da cibersegurança e a missão educativa do agrupamento.

5.1. Síntese do diagnóstico e justificação da proposta

O presente plano de cibersegurança tem como finalidade responder às necessidades identificadas no diagnóstico apresentado no Capítulo 4, consolidando a infraestrutura tecnológica, reforçando a gestão organizacional e promovendo uma cultura digital segura e sustentável. A proposta foi concebida em alinhamento com os referenciais normativos nacionais e europeus e encontra-se articulada com os documentos estruturantes do Agrupamento de Escolas Passos Manuel.

Este enquadramento assume particular relevância numa instituição que acolhe 1 375 alunos distribuídos por 70 turmas, das quais 40 % são compostas por estudantes estrangeiros, 26 % beneficiam de apoios no âmbito da Ação Social Escolar e 8 % correspondem a alunos com necessidades educativas especiais. O agrupamento conta ainda com mais de 200 colaboradores, o que justifica a adoção de políticas inclusivas de literacia digital, a implementação de processos seguros de criação e gestão de contas institucionais e a consolidação de uma gestão centralizada de dispositivos.

5.1.1. Contexto institucional

O Agrupamento de Escolas Passos Manuel dispõe de uma rede segmentada, protegida por firewall de última geração, mecanismos de deteção e prevenção de intrusões (IDS/IPS) e cópias de segurança regulares. Persistem, contudo, lacunas ao nível do registo centralizado de *logs*, do inventário atualizado de ativos digitais, da gestão de vulnerabilidades e da uniformização dos processos de autenticação e acesso. A aplicação do Decreto-Lei n.º 95/2025, que regula o uso de dispositivos móveis em contexto escolar, a Resolução do Conselho de Ministros n.º 127/2025, relativa à Estratégia Nacional de Cidadania e Desenvolvimento, a adoção da plataforma Ubbu no 1.º aos 3.º ciclos, a utilização do Inovar PAA e a integração dos processos de *onboarding* digital coordenados pela BE/CRE reforçam a necessidade de operacionalizar medidas de proteção da informação e de gestão responsável da tecnologia.

5.1.2. Finalidade e metas do plano

O plano de cibersegurança tem como propósito central reforçar a resiliência tecnológica e organizacional do Agrupamento de Escolas Passos Manuel, assegurando práticas consistentes de proteção digital que promovam a continuidade pedagógica e administrativa. Pretende, ainda, garantir a salvaguarda dos dados pessoais em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e com a legislação nacional aplicável. A promoção da literacia digital e da cidadania responsável em toda a comunidade educativa constitui outro eixo essencial, articulado com a consolidação de ciclos de melhoria contínua, em coerência com os art.º 37.º a 40.º do Regulamento Interno.

Para concretizar estes objetivos gerais, o plano integra um conjunto de metas operacionais e técnicas que orientam a ação em diferentes dimensões. Do ponto de vista técnico, prevê-se a implementação da autenticação multifator (MFA) em todas as aplicações críticas, a consolidação da gestão de dispositivos através de soluções de *Mobile Device Management* (MDM) e de *Endpoint Detection and Response* (EDR), a encriptação por defeito de todos os equipamentos e a manutenção de um inventário atualizado de hardware e software, com reconciliação mensal. Complementarmente, será ativado um sistema de registo e análise centralizada de eventos (*logging* e *Security Information and Event Management – SIEM*), permitindo a medição de tempos médios de deteção (MTTD) e de resposta (MTTR). Incluem-se ainda a segmentação de rede por VLANs com protocolo 802.1X, a definição de uma política de cópias de segurança 3-2-1[1], a configuração de autenticação

[1] A regra 3-2-1 recomenda manter três cópias dos dados, em dois suportes diferentes e uma em local externo ou offline, garantindo resiliência contra perda de informação.

SPF/DKIM/DMARC no correio eletrónico institucional e o estabelecimento de um programa contínuo de gestão de vulnerabilidades com base no sistema CVSS.

No plano organizacional, o agrupamento compromete-se a criar uma matriz de responsabilidades RACI, a instituir auditorias internas e externas periódicas e a desenvolver um formulário digital para o reporte de incidentes. Prevê-se igualmente a publicação de uma política de utilização aceitável (AUP) em versão multilingue, garantindo conformidade com as diretrizes de acessibilidade digital (WCAG), e a operacionalização do regimento de telemóveis previsto no Decreto-Lei n.º 95/2025, com mecanismos de comunicação, fiscalização e monitorização adequados.

No domínio pedagógico, o plano propõe a explicitação e recolha da aceitação da política de utilização aceitável (AUP) por todos os perfis da comunidade educativa, alunos, docentes, não docentes e encarregados de educação, bem como a integração da plataforma Ubbu (1.º ao 3.º ciclo do ensino básico) em articulação com a Resolução do Conselho de Ministros n.º 127/2025. Inclui ainda a realização de sessões formativas sobre privacidade, segurança online e uso responsável de dispositivos móveis, e o desenvolvimento de trilhas de formação contínua adaptadas a cada grupo-alvo.

Por fim, na vertente de avaliação e melhoria contínua, o plano estabelece indicadores de desempenho (KPIs)[1] que permitem acompanhar a implementação das medidas e monitorizar o grau de maturidade digital alcançado. Este processo segue o modelo *Plan–Do–Check–Act* (PDCA) e garante a revisão periódica das práticas em coerência com os mecanismos de autoavaliação e de gestão da qualidade definidos no Regulamento Interno do agrupamento.

5.1.3. Indicadores de sucesso e linha de base

A definição dos indicadores de sucesso e da linha de base permite estabelecer parâmetros objetivos para a monitorização da evolução do plano. As estimativas iniciais foram obtidas a partir da análise documental e do diagnóstico empírico descrito nas secções 4.3 e 4.4, que servirão como referência (T0) para a avaliação da maturidade cibernética do Agrupamento de Escolas Passos Manuel.

Até à realização da auditoria inicial, os valores considerados têm carácter aproximado e destinam-se apenas a representar o ponto de partida. As metas projetadas refletem o nível desejável a alcançar no período de doze meses após a implementação do plano (T+12). A designação ‘ausente’ utilizada no diagnóstico refere-se à inexistência de implementação formal e sistemática, sendo representada no gráfico por um valor percentual residual, meramente indicativo, até à realização da auditoria inicial. A

[1] *Key Performance Indicators (KPIs)* são métricas que medem o progresso e a eficácia das ações definidas no plano.

Figura 5.1 apresenta, de forma comparativa, a diferença entre o estado atual estimado e as metas de desempenho estabelecidas.

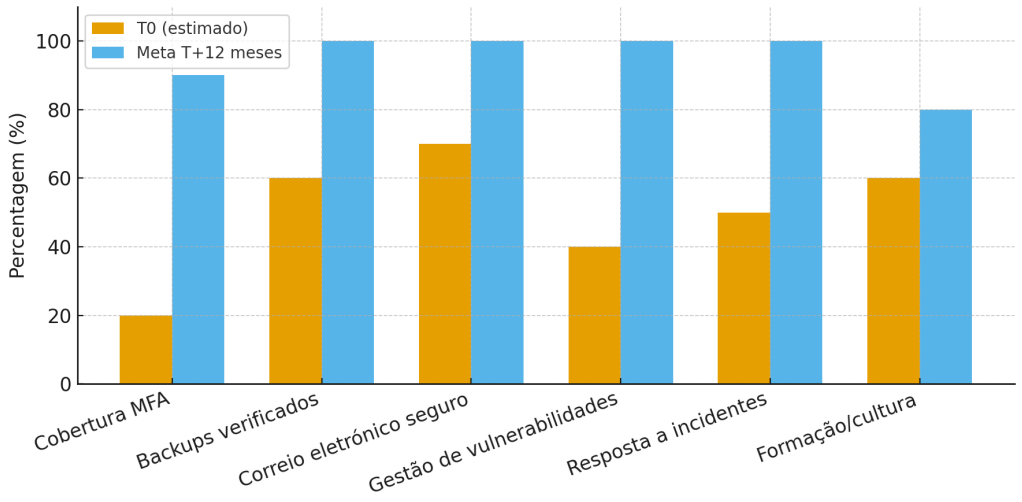


Figura 5.1 - Gap atual vs. metas de cibersegurança no AEPM

Fonte: Elaboração própria, com base no diagnóstico preliminar do Agrupamento de Escolas Passos Manuel (2025).

A análise representada na figura evidencia progressos esperados em domínios estratégicos como a autenticação multifator (MFA), os *backups* verificados, a segurança do correio eletrónico, a gestão de vulnerabilidades, a resposta a incidentes e a formação da comunidade educativa. Estes indicadores traduzem-se em metas quantitativas, expressas da seguinte forma: cobertura integral da MFA em contas privilegiadas até seis meses após o início da implementação e 90 % de cobertura em docentes e técnicos até doze meses; verificação completa de cópias de segurança e realização de testes de restauro em todos os serviços críticos até um ano; configuração de SPF e DKIM em seis meses e ativação de DMARC em modo *quarantine* ou *reject* até doze meses; resolução de vulnerabilidades críticas em menos de sete dias; redução em 30 % dos incidentes face ao ponto de partida; e tempos médios de deteção (MTTD) inferiores a vinte e quatro horas e de resposta (MTTR) inferiores a cinco dias úteis.

No domínio formativo, prevê-se que, até ao final do primeiro ano, 80 % dos docentes concluam uma ação de formação anual, que a taxa de cliques em simulações de *phishing* se reduza para menos de 10 % e que a taxa de reporte de incidentes atinja pelo menos 70 %. Estes indicadores servirão como base de acompanhamento e avaliação contínua, garantindo a coerência com o sistema de monitorização apresentado no ponto 5.6.

5.1.4. Síntese normativa

A proposta de plano está alinhada com os principais referenciais de segurança e proteção de dados: ISO/IEC 27001 e 27002:2022[1], Regulamento Geral sobre a Proteção de Dados (RGPD) e Lei n.º 58/2019, Diretiva NIS 2, *Digital Services Act*, diretrizes do Centro Nacional de Cibersegurança (CNCS), *Guidelines* da Comissão Europeia (2022) e *Cybersecurity Standards for Schools and Colleges* (Department for Education, Reino Unido, 2025). Integra ainda o Decreto-Lei n.º 95/2025, a Resolução do Conselho de Ministros n.º 127/2025 e as disposições dos artigos 37.º a 40.º do Regulamento Interno do Agrupamento, referentes à avaliação interna e autoavaliação institucional.

5.2. Síntese do diagnóstico e justificação da proposta

5.2.1. Organização geral do plano

Com base nos objetivos definidos no ponto anterior, o Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel estrutura-se em três componentes essenciais: um conjunto de princípios orientadores, um modelo de gestão com responsabilidades claramente definidas e seis eixos estratégicos que operacionalizam a proposta. Esta estrutura assegura coerência com os documentos estratégicos do agrupamento, o Projeto Educativo (PE), o Plano de Ação para o Desenvolvimento Digital da Escola (PADDE), a Estratégia de Educação para a Cidadania na Escola (EECE), o Regulamento Interno (RI), o Plano TEIP e Plano Anual de Atividades (PAA9, e garante o alinhamento com os referenciais nacionais e internacionais, nomeadamente o CNCS, o RGPD, a Diretiva NIS 2, o *Digital Services Act*, as normas ISO/IEC 27001 e 27002 e as *Cybersecurity Standards for Schools and Colleges* (DfE, 2025).

A escala e diversidade do agrupamento, que reúne 1 375 alunos distribuídos por 70 turmas, dos quais 40 % são estrangeiros de 43 nacionalidades, 26 % beneficiam de apoios da Ação Social Escolar e 8 % têm necessidades educativas especiais, apoiados por mais de 200 profissionais, exigem políticas que conciliem uma gestão técnica rigorosa com uma abordagem pedagógica inclusiva. A acessibilidade, a equidade e o suporte diferenciado são, por isso, princípios estruturantes na definição e implementação do plano.

[1] As normas ISO/IEC 27001 e 27002 definem requisitos e boas práticas para sistemas de gestão de segurança da informação, incluindo controlos técnicos e organizacionais.

5.2.2. Princípios orientadores

Os princípios que orientam o plano de cibersegurança foram agrupados em quatro categorias, gestão, técnica, operacional e inclusão, permitindo uma relação direta entre as orientações gerais e os eixos estratégicos definidos.

Na dimensão da gestão, o plano pauta-se pela proporcionalidade ao risco, pela melhoria contínua segundo o ciclo *Plan–Do–Check–Act* (PDCA), pela responsabilização institucional (*accountability*) e pela monitorização sistemática das atividades. No domínio técnico, privilegia-se a proteção de dados desde a conceção e por defeito (*privacy by design* e *by default*), a aplicação do paradigma *zero trust*, especialmente relevante para a infraestrutura de rede, e o princípio da defesa em profundidade.

A vertente operacional centra-se na gestão do ciclo de vida da informação, abrangendo a classificação, a retenção e a eliminação segura dos dados, em articulação com os eixos de gestão e privacidade.

Por fim, a dimensão da inclusão garante que todas as medidas de cibersegurança respeitam critérios de acessibilidade e usabilidade para todos os utilizadores, estabelecendo responsabilidades partilhadas com fornecedores e parceiros, conforme previsto no artigo 28.º do RGPD[1], que regula as cláusulas contratuais relativas à segurança e localização de dados.

5.2.3. Modelos de gestão

O modelo de governação proposto assegura a clarificação de responsabilidades e fluxos decisórios, promovendo a transparência e a rastreabilidade em todas as fases do plano. Este modelo baseia-se na criação do Comité de Cibersegurança do Agrupamento de Escolas Passos Manuel, entidade responsável por aprovar políticas, validar prioridades, acompanhar indicadores e reportar ao Conselho Geral. O Comité reúne-se ordinariamente de dois em dois meses e extraordinariamente sempre que ocorra um incidente classificado como de gravidade média ou superior, ou em caso de notificação da Comissão Nacional de Proteção de Dados (CNPD). Para clarificar papéis e responsabilidades, o plano adota uma matriz RACI[2] que define, para cada atividade, quem é responsável (R), quem responde pelo resultado (A), quem é consultado (C) e quem é informado (I). Esta estrutura garante a coerência entre

[1] O artigo 28.º do RGPD regula as obrigações dos subencarregados de tratamento, impondo cláusulas contratuais que garantam segurança e confidencialidade dos dados.
[2] O modelo RACI (*Responsible, Accountable, Consulted, Informed*) é uma ferramenta de gestão de responsabilidades que clarifica quem executa, supervisiona, apoia e é informado sobre cada tarefa ou decisão organizacional (PMI, 2021).

os níveis técnico, organizacional e pedagógico da governação da cibersegurança, conforme apresentado na Tabela 5.2-A.

Tabela 5.2-A — Matriz RACI das principais funções de cibersegurança do AEPM

Atividade / Tarefa	Direção	DPO	Coord. TIC	Conselho Pedagógico / Departamentos	Serviços Administrativos
Aprovar políticas de cibersegurança e disponibilizar recursos	A	C	R	I	I
Garantir conformidade com o RGPD e conduzir DPIA/TIA	I	R/A	C	I	C
Implementar controlos técnicos e gerir inventário digital (BE/CRE, JML, *logs*, backups)	I	C	R/A	I	I
Integrar a cibersegurança no currículo e promover práticas pedagógicas seguras	I	C	C	R/A	I
Formalizar contratos, gerir fornecedores e documentar a aceitação da AUP	I	C	C	I	R/A
Monitorizar indicadores, consolidar relatórios e reportar resultados	A	C	R	R	I

Nota. R – *Responsible* (executa a tarefa); A – *Accountable* (responde pelo resultado); C – *Consulted* (é consultado durante o processo); I – *Informed* (é informado do progresso ou resultado).

5.2.4. Eixos estratégicos

O plano organiza-se em seis eixos estratégicos, que articulam medidas técnicas, organizacionais e pedagógicas, garantindo coerência entre o diagnóstico e as metas definidas.

O *Eixo I Gestão, conformidade e risco* estabelece a política institucional de cibersegurança, aprovada em Conselho Pedagógico, e define a matriz RACI, sujeita a revisão anual. Prevê auditorias internas e externas calendarizadas, fluxos formais de reporte de incidentes com formulário digital integrado no PAA e no calendário do Conselho Pedagógico, a formalização e auditoria do processo de *onboarding* digital (criação e distribuição de credenciais BE/CRE e perfis JML) e a validação documental

das políticas de utilização aceitável (AUP) com registo de aceite por perfis. Inclui, ainda, a integração do regimento de telemóveis aprovado nos termos do Decreto-Lei n.º 95/2025.

O *Eixo II Infraestrutura e operação segura*, abrange o inventário atualizado de hardware e software, com reconciliação mensal e relatórios trimestrais, a gestão centralizada de dispositivos (incluindo os emprestados a alunos) através de MDM e EDR com encriptação por defeito, a centralização e análise de *logs* com métricas MTTD/MTTR, a segmentação da rede por VLANs e protocolo 802.1X e a implementação de uma política de cópias de segurança 3-2-1. Integra também o reforço da segurança do correio eletrónico institucional com autenticação SPF/DKIM/DMARC.

O *Eixo III Dados e privacidade* prevê a realização sistemática de avaliações de impacto sobre a proteção de dados (DPIA/TIA), a aplicação de políticas de minimização e retenção, o registo e a monitorização de contas privilegiadas e a adoção de políticas de palavra-passe robustas e de autenticação multifator obrigatória em serviços críticos. Inclui ainda a divulgação e aceitação das políticas de utilização aceitável por todos os perfis de utilizador.

O *Eixo IV Capacitação pedagógica e cultura digital segura* integra um programa anual de formação por perfis (alunos, docentes, não docentes e encarregados de educação), a utilização da plataforma Ubbu (1.º ao 3.º ciclo do ensino básico) com módulos de cidadania digital e segurança online e a articulação com os objetivos do programa TEIP e da Resolução do Conselho de Ministros n.º 127/2025. Inclui ainda sessões sobre o uso responsável de dispositivos móveis, em conformidade com o Decreto-Lei n.º 95/2025, e a utilização do Inovar PAA como ferramenta de gestão pedagógica e de monitorização.

O *Eixo V Resposta a incidentes e continuidade pedagógica* estabelece a definição de *playbooks* de resposta a incidentes, procedimentos de escalonamento e reporte, realização de exercícios de simulação e integração do regimento de telemóveis nos mecanismos de fiscalização e resposta disciplinar. Garante, ainda, a elaboração de planos de continuidade de serviços críticos, com objetivos de recuperação (RPO/RTO) definidos e testados regularmente.

Por fim, o *Eixo VI Avaliação, métricas e melhoria contínua* define indicadores técnicos e organizacionais de desempenho (por exemplo, MFA ≥ 90 %, vulnerabilidades críticas corrigidas em menos de sete dias e encriptação ≥ 95 %), relatórios periódicos apresentados em Conselho Pedagógico e Direção, e integração do ciclo PDCA como base de acompanhamento e revisão. Este eixo articula-se com os artigos 37.º a 40.º do Regulamento Interno, assegurando a coerência entre a autoavaliação e a avaliação interna.

5.2.5. Síntese e transição

Em síntese, o Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel assenta numa estrutura sólida composta por princípios orientadores, um modelo de gestão transparente e seis eixos estratégicos que asseguram a articulação entre as dimensões técnica, organizacional e pedagógica. Esta organização garante coerência com o diagnóstico apresentado no Capítulo 4 e com os objetivos delineados no ponto 5.1, estabelecendo as bases para a implementação faseada das medidas que serão detalhadas nas secções seguintes.

No ponto 5.3 apresenta-se o conjunto de medidas técnicas, organizacionais e pedagógicas que concretizam, de forma prática, os eixos definidos nesta secção, acompanhadas de prazos, responsáveis e indicadores de desempenho.

5.3. Medidas técnicas, organizacionais e pedagógicas

5.3.1. Enquadramento geral

As medidas apresentadas neste ponto concretizam os objetivos definidos em 5.1 e a estrutura delineada em 5.2. Foram elaboradas com base nos princípios da proporcionalidade ao risco, na melhoria contínua segundo o ciclo *Plan–Do–Check–Act* (PDCA), na proteção de dados desde a conceção e por defeito (*privacy by design* e *by default*) e na responsabilidade partilhada com os fornecedores.

A aplicação destas medidas assegura coerência com os documentos estruturantes do Agrupamento de Escolas Passos Manuel, nomeadamente entre o Projeto Educativo, PADDE, EECE, Regulamento Interno, TEIP e PAA, e está alinhada com os referenciais normativos do CNCS, com o RGPD, a Diretiva NIS 2, o *Digital Services Act* (DSA), as normas ISO/IEC 27001 e 27002 e as *Cybersecurity Standards* do *Department for Education* (Reino Unido, 2025).

A lista de serviços críticos do agrupamento, incluindo identidade e diretórios, correio eletrónico, plataformas de gestão de aprendizagem (LMS), rede/Internet e backups, será validada com base no inventário técnico e nas práticas em vigor descritas em 4.3 e 4.4. A proteção de dados será operacionalizada através da nova Política de Privacidade e Proteção de Dados do AEPM, a aprovar e integrar no Regulamento Interno. As responsabilidades partilhadas com terceiros serão asseguradas por cláusulas contratuais conformes ao art.º 28.º do RGPD e por avaliações anuais documentadas.

Cada medida inclui a identificação do responsável, o prazo de execução, as evidências esperadas e os indicadores de desempenho (KPI), em coerência com as metas definidas nos pontos 5.1.5 e 5.6.

5.3.2. Medidas técnicas

As medidas técnicas enquadram-se no *Eixo II Infraestrutura e Operações Seguras* e têm como finalidade reforçar a proteção dos sistemas críticos, a gestão de identidades, o controlo de acessos e a monitorização dos incidentes.

Relativamente à *identidade e aos acessos*, será implementada autenticação multifator (MFA) para todas as contas privilegiadas, incluindo direção, coordenação TIC e serviços administrativos, estendendo-se progressivamente aos docentes e técnicos. A gestão de identidades será suportada por mecanismos de *Single Sign-On* (SSO) e por controlos de acesso baseados em função ou atributo (RBAC/ABAC), com automatização do ciclo de vida de utilizadores (*Joiner, Mover, Leaver – JML*) e integração no processo de *onboarding* digital BE/CRE. A política de palavras-passe seguirá critérios de comprimento e rotação definidos por nível de risco, bloqueio após tentativas falhadas e utilização de cofres digitais em contas administrativas (*Privileged Access Management – PAM*).

No que diz respeito à *rede e ao perímetro*, a infraestrutura será segmentada por VLANs e sujeita a controlo 802.1X, garantindo isolamento entre utilizadores e dispositivos. As ligações sem fios utilizarão os protocolos WPA2-Enterprise e WPA3, assegurando uma rede de convidados separada. A firewall de nova geração (NGFW) funcionará com políticas restritivas *deny-by-default* e inspeção de tráfego entre segmentos, sujeita a auditoria semestral.

Quanto aos *endpoints e dispositivos*, todos os equipamentos institucionais, incluindo os emprestados a alunos, serão encriptados e protegidos por soluções EDR atualizadas, configuradas com *hardening* de acordo com *benchmarks* CIS. A gestão centralizada dos dispositivos será assegurada por MDM, aplicável também aos equipamentos *Bring Your Own Device* (BYOD) e 1:1, com políticas mínimas de PIN, encriptação e bloqueio remoto.

No que se refere ao *correio eletrónico e colaboração*, será implementada autenticação SPF/DKIM e política DMARC em modo *quarantine* ou *reject*, complementada por mecanismos de verificação dinâmica de hiperligações (*safe links*) e anexos (*sandboxing*). O reencaminhamento automático para domínios externos e as partilhas fora do ambiente institucional serão bloqueados, garantindo a integridade das comunicações.

Relativamente aos *backups e à recuperação*, será aplicada a regra 3-2-1, com pelo menos uma cópia offline e imutável (*Write Once Read Many – WORM*). Serão realizados testes de restauro trimestrais, com registo dos tempos de recuperação (RTO) e dos pontos de restauro (RPO), assegurando a fiabilidade dos processos de continuidade.

No que concerne ao *registo e à monitorização*, será criada uma infraestrutura centralizada de *Security Information and Event Management* (SIEM), que reunirá eventos de autenticação, privilégios, alterações críticas, firewall, antivírus, EDR, correio eletrónico e backups. O sistema emitirá alertas

automáticos para falhas de MFA, picos de tráfego e bloqueios de *malware*, permitindo a deteção precoce de anomalias.

Quanto à *gestão de vulnerabilidades e atualizações*, o agrupamento executará varrimentos mensais para deteção de vulnerabilidades, validará os resultados e aplicará correções críticas em menos de sete dias e as restantes em até trinta dias, reclassificando falsos positivos e mantendo registos auditáveis.

Relativamente aos *serviços em nuvem e às plataformas EdTech*, será estabelecida uma política de governação que inclua revisão de permissões, verificação de aplicações de terceiros e conformidade contratual com o art.º 28.º do RGPD. Todas as plataformas educativas, incluindo a Ubbu, estarão sujeitas a Avaliações de Impacto sobre a Proteção de Dados (DPIA), com registo e acompanhamento anual.

Por fim, no que se refere às *salvaguardas físicas e energia*, serão implementados controlos de acesso a salas e armários técnicos, manutenção de inventário de chaves e instalação de sistemas de alimentação ininterrupta (UPS) nos equipamentos críticos, garantindo a continuidade operacional e a segurança física dos recursos.

5.3.3. Medidas organizacionais

As medidas organizacionais, correspondentes aos *eixos I, III, V e VI* e têm como finalidade fortalecer a governação, a conformidade, a gestão documental e a comunicação interna.

Relativamente às *políticas e à gestão*, será aprovada uma Política Institucional de Cibersegurança acompanhada de um catálogo de políticas complementares, abrangendo acessos, palavras-passe, dispositivos pessoais (BYOD), utilização aceitável, classificação da informação e serviços em nuvem. Todas as políticas terão revisão anual e extraordinária sempre que ocorra incidente relevante.

No que diz respeito à *conformidade e proteção de dados*, o Encarregado de Proteção de Dados (DPO), em articulação com os serviços administrativos e a coordenação TIC, procederá à atualização dos registos de tratamento, à realização de DPIA e TIA e à manutenção das listas de subencarregados de tratamento. A política de utilização aceitável (AUP) será disponibilizada em versão multilingue e em formatos acessíveis, de acordo com as diretrizes WCAG.

Quanto à *gestão de terceiros*, os contratos de prestação de serviços incluirão cláusulas em conformidade com o artigo 28.º do RGPD. Será adotada uma *checklist* pré-contratual de verificação e realizada uma avaliação anual dos fornecedores, com documentação de evidências e verificação da localização dos dados tratados.

Relativamente à *resposta a incidentes e continuidade*, o agrupamento elaborará um Plano de Resposta a Incidentes[1], definindo papéis, fluxos e procedimentos de preservação de prova digital. Serão conduzidos exercícios semestrais de simulação e mantido um repositório de incidentes e de lições aprendidas, integrando os resultados nos relatórios de autoavaliação.

No que concerne à *gestão documental*, serão definidos critérios de classificação da informação, prazos de retenção e procedimentos de eliminação segura. Todos os documentos incluirão metadados obrigatórios, assegurando rastreabilidade e cumprimento do princípio da responsabilidade (*accountability*).

Relativamente à *comunicação institucional*, a Direção e o DPO desenvolverão um plano de comunicação com mensagens pré-aprovadas, canais de alerta em tempo real e divulgação pública do regimento de utilização de telemóveis, garantindo clareza e coerência entre transparência e segurança.

Por fim, no que se refere à *articulação com o programa TEIP*, as ações de cibersegurança serão integradas nos objetivos e iniciativas do plano TEIP, reforçando a inclusão digital e a segurança nos territórios educativos prioritários.

5.3.4. Medidas pedagógicas

As medidas pedagógicas, correspondentes ao Eixo IV, visam consolidar uma cultura de cibersegurança transversal à comunidade educativa, incidindo sobre a capacitação de docentes, alunos, famílias e restante pessoal escolar. Relativamente à *capacitação de docentes e não docentes*, será implementado um programa anual de formação obrigatória, complementado por micro cursos trimestrais e pela criação de uma rede de multiplicadores internos. Os conteúdos incluirão boas práticas de segurança digital, proteção de dados e uso responsável de dispositivos móveis, em conformidade com o Decreto-Lei n.º 95/2025.

No que diz respeito à *integração curricular dos alunos*, a cidadania digital será incorporada no currículo através da EECE, com atividades práticas dedicadas à privacidade, pegada digital, verificação de fontes e segurança básica. A plataforma Ubbu será utilizada no 1.º ao 3.º ciclo, articulando-se com a Resolução do Conselho de Ministros n.º 127/2025 e com projetos interdisciplinares nas disciplinas de TIC e Cidadania e Desenvolvimento.

[1] O plano define procedimentos para deteção, contenção, mitigação e comunicação de incidentes de segurança digital, garantindo continuidade de serviços.

Quanto às *simulações e exercícios*, serão realizadas simulações trimestrais de phishing e exercícios tabletop semestrais de resposta a incidentes, avaliando tempos de reação e eficácia das equipas. Cada exercício incluirá análise pós-evento e plano de melhoria, garantindo o aperfeiçoamento progressivo dos procedimentos.

Relativamente às *famílias e à comunidade*, serão promovidas ações de capacitação parental no âmbito da *Academia Digital para Pais*[1], complementadas com guias práticos e questionários de avaliação de impacto. Estas ações decorrerão em formato híbrido, presencial e online, assegurando maior flexibilidade e participação.

Por fim, no que se refere à *liderança estudantil*, será criado o programa "Líderes Digitais / Embaixadores de Cibersegurança[2]", destinado a promover o protagonismo dos alunos na disseminação de boas práticas e na sensibilização para a ética digital. O programa basear-se-á numa Carta de Responsabilidades e incluirá mecanismos de reconhecimento público e valorização de mérito.

As medidas apresentadas encontram-se mapeadas de forma detalhada aos principais referenciais normativos e legais (ISO/IEC 27002:2022, RGPD, Diretiva NIS 2, *Digital Services Act* e orientações do CNCS e da EECE), conforme se apresenta na Matriz de Correspondência constante do (**Apêndice H**).

5.4. Plano de Implementação (fases e prioridades)

5.4.1. Estrutura e enquadramento

A análise desenvolvida nas secções 4.3 e 4.4, associada à definição de medidas técnicas, organizacionais e pedagógicas apresentada em 5.3, evidenciou a necessidade de estruturar a implementação do Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel de forma progressiva, coerente e monitorizável.

O plano organiza-se em quatro fases sequenciais e interdependentes, garantindo articulação com os documentos estruturantes do agrupamento, Projeto Educativo, PADDE, EECE, RI, TEIP e PAA e alinhamento com os principais referenciais e normativos, nomeadamente as normas ISO/IEC 27001:2022 e 27002:2022, o RGPD (UE, 2016/679), a Diretiva NIS 2 (UE, 2022/2555), as recomendações do CNCS e da CNPD, o *Digital Services Act* (UE, 2022/2065) e as *Cybersecurity Standards for Schools and Colleges do Department for Education* (Reino Unido, 2025).

[1] Programa desenvolvido pela E-REDES e pela Direção-Geral da Educação que promove competências digitais parentais e segurança online familiar.

[2] Iniciativa de envolvimento estudantil inspirada em boas práticas internacionais, que incentiva o protagonismo juvenil na promoção de uma cultura de cibersegurança.

A calendarização proposta é indicativa e deverá ser validada pela Direção, pelo Encarregado de Proteção de Dados (DPO) e pelas equipas técnicas responsáveis, de acordo com os recursos disponíveis. Embora o plano tenha sido concebido com base nos seis eixos estratégicos descritos em 5.2 e 5.3, a sua execução operacional é organizada em quatro fases de implementação: Preparação e Gestão; Infraestruturas e Proteção Técnica; Capacitação e Cultura Digital Segura; Avaliação e Melhoria Contínua, o que permite concentrar esforços e acompanhar resultados de forma mais eficiente, segundo os ciclos de monitorização e avaliação apresentados em 5.6.

5.4.2. Dependências e pré-requisitos

As fases do plano apresentam uma lógica de encadeamento progressivo que garante a consolidação gradual das medidas e o controlo de riscos. A execução inicia-se com a validação das *baselines* iniciais (T0) a partir do Formulário de Diagnóstico de Cibersegurança, preenchido pela Direção do AEPM em setembro de 2025. A Fase II depende da aprovação formal da Política de Cibersegurança e da publicação da Matriz RACI. A Fase III inicia-se após a operacionalização mínima das infraestruturas fundamentais, autenticação multifator (MFA), cópias de segurança e registo centralizado de *logging*. Por fim, a Fase IV requer a conclusão de pelo menos um ciclo formativo anual da Fase III.

Estas dependências garantem coerência entre preparação, execução e avaliação, minimizando riscos e assegurando a rastreabilidade das ações. A calendarização dos principais pré-requisitos é sintetizada no Quadro 5.4-A.

Quadro 5.4 A – Pré-requisitos entre fases

Pré-requisito	Validador	Prazo
Validação das *baselines* iniciais (T0) através do Formulário de Diagnóstico	Comissão de Cibersegurança	≤ 3 meses
Publicação da Política de Cibersegurança	Direção	≤ 6 meses
Publicação da Matriz RACI	Comissão de Cibersegurança	≤ 6 meses
Operacionalização mínima de MFA, *backups* e *logging*	Coord. TIC	≤ 12 meses
Conclusão de um ciclo formativo anual	Direção / Comissão de Cibersegurança	≤ 24 meses

5.4.3. Fase I – Preparação e gestão (0 – 6 meses)

A primeira fase tem como objetivo criar as condições organizacionais e normativas necessárias ao arranque do plano. Entre as ações prioritárias incluem-se a aprovação da Política de Cibersegurança, a publicação da Matriz RACI, a revisão e formalização do regimento de utilização de telemóveis (Decreto-Lei n.º 95/2025), a criação de fluxos formais de reporte de incidentes através de formulário digital integrado no PAA e a auditoria do processo de *onboarding* digital para criação e atribuição de contas. A análise dos dados do Formulário de Diagnóstico de Cibersegurança permitirá definir as *baselines* e as metas iniciais de monitorização.

Os principais indicadores de desempenho (KPIs) desta fase incluem a aprovação da Política de Cibersegurança e da Matriz RACI em menos de seis meses e a validação de 95 % das *baselines* T0 em menos de três meses. O principal risco identificado prende-se com a eventual falta de adesão da comunidade escolar, mitigada pela realização de sessões de esclarecimento dirigidas a docentes, alunos e encarregados de educação.

5.4.4. Fase II – Infraestruturas e proteção (6 – 12 meses)

A segunda fase visa reforçar a resiliência dos sistemas críticos e assegurar a proteção dos dados em trânsito e em repouso.

Esta etapa contempla a implementação de autenticação multifator em contas privilegiadas e a sua expansão progressiva a docentes e técnicos, a gestão centralizada de *endpoints* (incluindo dispositivos emprestados a alunos), a encriptação generalizada e o uso de soluções EDR e MDM. Inclui ainda a centralização de *logs* e definição de métricas de deteção e resposta (MTTD/MTTR), a implementação da política de backups 3-2-1 com testes regulares de restauro e o desenvolvimento de um processo contínuo de gestão de vulnerabilidades, com scans mensais e correção de falhas críticas em menos de sete dias.

A articulação com o diagnóstico inicial confirmou a existência de cobertura de Wi-Fi, segmentação de utilizadores, firewall de nova geração (NGFW) e sistemas de deteção e prevenção de intrusões (IDS/IPS). Estes dados sustentam as ações propostas e reforçam a necessidade de implementação de *logging* centralizado e relatórios trimestrais de segurança.

Os indicadores definidos para a Fase II correspondem a metas intermédias do plano, coerentes com as metas globais apresentadas na Figura 5.1, que projeta os objetivos a alcançar no horizonte temporal de doze meses (T+12).

Os indicadores SMART definidos para esta fase incluem a ativação da MFA em 80 % das contas em menos de doze meses, a obtenção de 90 % de sucesso nos testes de cópias de segurança realizados trimestralmente e a análise de 100 % dos incidentes registados em relatórios de *logs* no prazo máximo de trinta dias. O risco mais relevante nesta fase relaciona-se com eventuais constrangimentos orçamentais. Como medida de mitigação, prevê-se a candidatura a programas de financiamento do PT2030 e o estabelecimento de parcerias externas.

5.4.5. Fase III – Capacitação e Cultura digital segura (12 – 24 meses)

A terceira fase tem como foco o desenvolvimento de competências digitais e de práticas seguras por toda a comunidade educativa. Esta etapa inclui a programação anual de formação diferenciada por perfis, a integração da plataforma Ubbu nos primeiros ciclos de ensino, a realização de sessões de sensibilização sobre o uso responsável de telemóveis (em conformidade com o Decreto-Lei n.º 95/2025) e a articulação com a Resolução do Conselho de Ministros n.º 127/2025, que define a Estratégia Nacional de Cidadania e Desenvolvimento. As ações incluem igualmente a integração de medidas de cibersegurança nos objetivos do programa TEIP 4 e a utilização do Inovar PAA como ferramenta de registo e monitorização das atividades.

Os principais indicadores SMART desta fase preveem que, até vinte e quatro meses após o início da implementação, pelo menos 90 % dos docentes e não docentes tenham concluído formação certificada, que 70 % dos alunos e 50 % dos encarregados de educação participem em ações de sensibilização e que sejam realizadas duas simulações anuais de *phishing*, com relatórios discutidos em Conselho Pedagógico. Prevê-se ainda que 80 % das atividades do plano TEIP relacionadas com cibersegurança estejam concluídas até ao final do segundo ano.

A principal ameaça à concretização destas metas poderá ser a resistência à participação formativa. Para mitigar este risco, o agrupamento assegurará a acreditação das formações e a integração das mesmas na progressão profissional dos docentes e técnicos.

5.4.6. Fase IV – Avaliação, melhoria contínua e sustentabilidade (12 – 24 meses)

A quarta fase encerra o ciclo de implementação e visa consolidar a maturidade digital e organizacional do agrupamento. Inclui a realização de auditorias internas anuais, a revisão periódica de indicadores técnicos, pedagógicos e organizacionais e a apresentação de relatórios de avaliação à Direção e ao Conselho Geral.

Serão monitorizados os prazos institucionais definidos no PAA e no Regulamento Interno, devendo atingir-se um nível de cumprimento igual ou superior a 95 %. As políticas e procedimentos serão atualizados com base nas lições aprendidas, assegurando a continuidade da conformidade com os artigos 37.º a 40.º do Regulamento Interno.

Os principais indicadores SMART desta fase incluem a obtenção do nível "avançado" na ferramenta SELFIE (domínio Segurança) em menos de trinta e seis meses, a revisão de 100 % das políticas de cibersegurança de forma anual e a realização de dois exercícios *tabletop* de simulação de incidentes por ano, com relatório final emitido em trinta dias. O risco mais relevante prende-se com a possível desatualização face a novas ameaças. Como resposta, será mantido um repositório interno de lições aprendidas e instituída uma revisão semestral do plano.

5.4.7. Quadro síntese do plano de implementação

O Quadro 5.4 B apresenta uma síntese das quatro fases de implementação, integrando as ações prioritárias, os indicadores SMART e os principais riscos e medidas de mitigação.

Quadro 5.4 B – Plano de Implementação do AEPM

Fase	Ações prioritárias	Indicadores SMART	Riscos e Mitigações
I – Preparação e Gestão	Aprovação da Política de Cibersegurança; publicação da Matriz RACI; revisão do regimento de telemóveis; criação de formulário de incidentes; auditoria ao *onboarding* digital; definição de *baselines* T0	Política e matriz RACI aprovadas ≤ 6 m; *baselines* T0 validadas ≥ 95 % ≤ 3 m	Falta de adesão da comunidade → sessões de esclarecimento
II – Infraestruturas e Proteção Técnica	MFA; gestão centralizada de dispositivos; encriptação e EDR/MDM; *backups* 3-2-1; *logging* centralizado; gestão de vulnerabilidades	MFA ≥ 80 % ≤ 12 m; sucesso de *backups* ≥ 90 %; incidentes analisados 100 % ≤ 30 d	Orçamento insuficiente → fundos PT2030 e parcerias
III – Capacitação e Cultura Digital Segura	Formação anual; integração da Ubbu; sessões sobre telemóveis; implementação da RCM 127/2025; integração no TEIP; uso do Inovar PAA	Formação docente ≥ 90 % ≤ 24 m; alunos ≥ 70 % e EE ≥ 50 % ≤ 18 m; atividades TEIP ≥ 80 % concluídas	Resistência à participação → certificação acreditada
IV – Avaliação e Melhoria Contínua	Auditorias internas; revisão de KPIs; relatórios CG/CP; monitorização CP/PAA ≥ 95 %; atualização de políticas	SELFIE "avançado" ≤ 36 m; políticas revistas 100 %/ano; 2 *tabletop* por ano	Desatualização → repositório de lições e revisão semestral

Nota. Prazos: curto prazo (≤ 6 meses); médio prazo (6–12 meses); longo prazo (> 12 meses).

5.4.8. Cronograma de implementação

Para complementar o quadro anterior e reforçar a rastreabilidade das ações, apresenta-se um cronograma representado sob a forma de *diagrama de Gantt*, que demonstra a duração prevista de cada fase, os marcos temporais (M1–M4) e as dependências críticas entre etapas. O cronograma evidencia a sequência temporal das atividades e permite uma leitura imediata da articulação entre os diferentes eixos do plano.

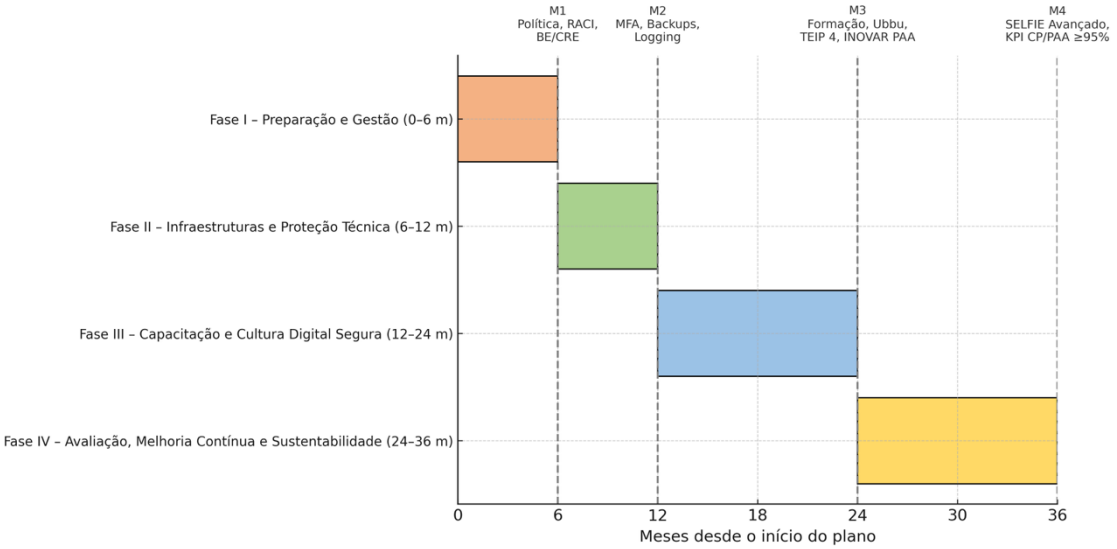


Figura 5.4 – Cronograma de Implementação do Plano de Cibersegurança (Diagrama de Gantt)

Legenda. Fase I: Preparação e Gestão; Fase II: Infraestruturas e Proteção Técnica; Fase III: Capacitação e Cultura Digital Segura; Fase IV: Avaliação, Melhoria Contínua e Sustentabilidade.
Marcos críticos: M1 (6 meses) – Política e Matriz RACI publicadas; M2 (12 meses) – MFA, backups e logging operacionais; M3 (24 meses) – conclusão do primeiro ciclo formativo, integração da Ubbu e monitorização via Inovar PAA; M4 (36 meses) – obtenção do nível "avançado" no domínio Segurança da ferramenta SELFIE, com auditorias consolidadas e KPIs institucionais ≥ 95 %.

5.4.9. Cronograma de implementação

O plano faseado garante uma progressão lógica e controlada, iniciando-se com a criação das bases organizacionais e culminando na consolidação de uma cultura de segurança sustentável. A sequência das fases assegura a integração entre gestão, tecnologia e formação, garantindo conformidade legal, resiliência operacional e capacitação da comunidade educativa.

A articulação das ações com indicadores SMART, mecanismos de mitigação de riscos e ciclos de melhoria contínua permite ao Agrupamento de Escolas Passos Manuel implementar uma estratégia

verificável e auditável, alinhada com as boas práticas europeias e nacionais em matéria de cibersegurança.

A correspondência entre as fases do plano e os principais referenciais normativos encontra-se sistematizada no (Anexo F), que complementa o Quadro 5.4 e o cronograma de implementação apresentados nesta secção.

O ponto seguinte, 5.5 Estratégias de formação e sensibilização, aprofunda a vertente pedagógica e formativa do plano, descrevendo conteúdos, metodologias e públicos-alvo que operacionalizam as fases definidas nesta secção.

5.5. Estratégias de formação e sensibilização

5.5.1. Fundamentação pedagógica e enquadramento normativo

A componente formativa e de sensibilização constitui um eixo essencial da implementação do Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel, refletindo o entendimento de que as medidas técnicas, por si só, não garantem a proteção efetiva dos sistemas e das pessoas. A literatura recente evidencia que a mitigação dos riscos digitais depende da criação de uma cultura de segurança partilhada, baseada em comportamentos conscientes, práticas informadas e aprendizagens contextualizadas (Veiga, 2024; Amankwa, 2021).

A estratégia formativa proposta articula-se diretamente com as fragilidades identificadas no diagnóstico (4.4), nomeadamente a insuficiência de competências digitais em docentes, alunos e famílias, e com as metas de literacia digital definidas nas medidas pedagógicas (5.3.4). Estas ações integram-se na terceira fase do plano (5.4.5), dedicada à capacitação e à cultura digital segura, e preparam a comunidade educativa para participar ativamente nos processos de monitorização e avaliação (5.6).

Do ponto de vista normativo, a formação e sensibilização respondem a três grandes eixos.

O primeiro é o da promoção da literacia digital e da cibersegurança em idade escolar, amplamente defendido em estudos internacionais (Xu & Li, 2025; Jerman Blažič & Jerman Blažič, 2025; Amankwa, 2021).

O segundo é o da necessidade de capacitação contínua dos profissionais de educação, em linha com o quadro DigCompEdu e com a evidência empírica que demonstra lacunas de competência digital (Palacios-Rodríguez et al., 2025; Lopes, Sargento & Farto, 2023).

O terceiro corresponde à valorização da cidadania digital e da parentalidade responsável, preconizada por documentos da Comissão Europeia e programas como o *Digital Parenting* (EurofamNet, 2023) e a *Digital Academy for Parents* (E-REDES & DGE, 2022).

A nível legal, esta estratégia está em conformidade com o Perfil dos Alunos à Saída da Escolaridade Obrigatória e com o Referencial de Competências em Cibersegurança do CNCS (2022), articulando-se ainda com a Estratégia de Educação para a Cidadania na Escola (EECE). A Diretiva NIS 2 (UE, 2022) confere-lhe especial relevância, ao estabelecer no art.º 20.º a obrigatoriedade de programas de formação regulares em cibersegurança para todos os utilizadores com acesso a sistemas críticos. A conformidade do plano inclui igualmente o RGPD, o *Digital Services* Act (Regulamento UE 2022/2065) e as orientações nacionais emanadas pela Resolução do Conselho de Ministros n.º 127/2025, que reforça a capacitação digital das escolas TEIP. Destaca-se, ainda, o art.º 32.º do DSA, que sublinha a importância de medidas educativas e de literacia digital dirigidas a menores, o que legitima a integração sistemática desta dimensão nos programas escolares.

5.5.2. Público-alvo e diferenciação de estratégias

A estratégia de formação adota uma abordagem diferenciada, ajustada aos distintos públicos da comunidade educativa, reconhecendo que os riscos, as responsabilidades e os níveis de literacia variam significativamente entre grupos.

Para os docentes e não docentes, privilegia-se o desenvolvimento de competências práticas em cibersegurança aplicadas ao contexto escolar, abrangendo a gestão de credenciais, o uso de plataformas educativas seguras, a proteção de dados e a resposta a incidentes. Estas formações são estruturadas com base nos referenciais DigCompEdu, PADDE e CNCS (2022), enfatizando a aprendizagem prática e o contexto real de trabalho.

Nos alunos, a intervenção centra-se na cidadania digital, na proteção contra riscos online como *phishing*, fraude e *ciberbullying*, e no desenvolvimento de pensamento crítico para avaliar fontes e combater a desinformação (Comissão Europeia, 2022a; 2022b). Diversos estudos evidenciam que a exposição precoce a conteúdos de segurança digital promove hábitos duradouros e reduz comportamentos de risco (Xu & Li, 2025; Monteiro & Gomes, 2009).

Os encarregados de educação e as famílias são abordados através de ações de sensibilização que visam a promoção de práticas de parentalidade digital responsável, apoiando o acompanhamento das atividades tecnológicas dos filhos e fomentando o diálogo intergeracional sobre o uso ético e seguro das tecnologias. Estas ações seguem os modelos *Digital Parenting* (EurofamNet, 2023) e *Digital Academy for Parents* (E-REDES & DGE, 2022).

Por último, o pessoal não docente, nomeadamente assistentes operacionais e técnicos de manutenção é envolvido em sessões curtas de sensibilização e em comunicações simplificadas (*light-touch*), que asseguram a adoção de comportamentos básicos de segurança digital aplicados ao quotidiano escolar.

5.5.3. Metodologias e instrumentos

A execução das ações formativas e de sensibilização baseia-se em metodologias ativas e participativas, centradas na experimentação, na reflexão e no envolvimento da comunidade educativa.

Serão promovidos workshops e sessões práticas para docentes e não docentes, com utilização de estudos de caso, simulações de *phishing* e exercícios de resposta a incidentes. Estes exercícios recorrerão a dados anónimos recolhidos através do formulário digital de reporte de incidentes, garantindo pertinência e ligação à realidade da escola (ENISA, 2024; DfE, 2025).

A cidadania digital será integrada no currículo através de projetos interdisciplinares desenvolvidos nas disciplinas de Cidadania e Desenvolvimento e de TIC, complementados com atividades práticas, *storytelling* e jogos educativos, reforçando a aprendizagem baseada em problemas e desafios (*game-based learning).* As campanhas de sensibilização periódicas incluirão cartazes, boletins digitais, pequenos questionários e desafios interativos.

A componente inovadora desta abordagem inclui o uso de micro aprendizagem (*micro-learning*) através da plataforma Ubbu, a atribuição de badges digitais (*OpenBadges*) como forma de reconhecimento de competências adquiridas, a utilização de ferramentas de interação em tempo real (*Kahoot, Mentimeter*) para aferição de perceções imediatas e o desenvolvimento de um simulador gamificado de incidentes para alunos do 3.º ciclo, permitindo exercitar a tomada de decisão em ambiente seguro.

5.5.4. Indicadores de impacto com a avaliação

A monitorização das ações de formação e sensibilização integra-se no sistema global de avaliação do plano, descrito em 5.6. Os indicadores definidos permitem medir não apenas a execução, mas também o impacto e a sustentabilidade das aprendizagens.

Entre os indicadores de maior relevância destacam-se a cobertura formativa anual, expressa pela percentagem de docentes, não docentes, alunos e encarregados de educação envolvidos; a eficácia da aprendizagem, avaliada por testes de conhecimento aplicados antes e depois das ações; e a mudança de comportamentos, medida pela redução da taxa de cliques em simulações de *phishing*, pelo aumento da utilização de palavras-passe seguras e pela maior procura dos canais institucionais de reporte de incidentes.

Adicionalmente, serão monitorizadas a perceção de segurança digital na comunidade educativa, aferida através de questionários anuais, e a evolução do score médio do agrupamento nas ferramentas SELFIE e DigCompEdu. Todos os resultados serão reportados trimestralmente no PAA e no Conselho Pedagógico e integrados no *dashboard* de monitorização institucional a desenvolver no âmbito da implementação do plano.

Este sistema de acompanhamento assegura que a formação e a sensibilização não se limitem a ações pontuais, mas constituam um processo contínuo e cíclico de desenvolvimento, alinhado com os princípios da melhoria contínua e com a consolidação de uma cultura de cibersegurança sustentável.

A calendarização anual, os responsáveis institucionais e os indicadores de impacto detalhados para cada público-alvo encontram-se apresentados no (Anexo G), que operacionaliza as estratégias formativas descritas nesta secção.

5.5.5. Síntese e transição

A estratégia de formação e sensibilização do Agrupamento de Escolas Passos Manuel assenta na integração entre capacitação técnica e pedagógica, reforçando a autonomia digital da comunidade educativa e promovendo comportamentos éticos e seguros no uso da tecnologia. A articulação com os referenciais nacionais e europeus garante a relevância e a transferibilidade das práticas propostas, enquanto o modelo de monitorização assegura a sua continuidade e evolução.

O ponto seguinte, 5.6 Monitorização e avaliação do plano de cibersegurança do AEPM, apresenta os mecanismos que permitirão verificar o grau de eficácia das medidas implementadas, assegurando a retroalimentação do processo e a sustentabilidade da estratégia a longo prazo.

5.6. Estratégias de formação e sensibilização

5.6.1. Enquadramento e princípios gerais

A eficácia do plano de cibersegurança depende de um sistema estruturado de monitorização e avaliação que permita comprovar resultados, identificar riscos e assegurar a atualização contínua face às ameaças, aos normativos e às necessidades da comunidade educativa. No Agrupamento de Escolas Passos Manuel, este sistema articula-se com os documentos estruturantes, Projeto Educativo 2023–2026, Estratégia de Educação para a Cidadania na Escola 2023/24 e Plano de Ação para o Desenvolvimento Digital (PADDE 2021–2023), bem como com a matriz RACI definida no Eixo I (Preparação e Gestão), garantindo responsabilidades claras, ciclos de melhoria contínua e reporte sistemático à Direção.

O modelo de monitorização e avaliação assenta nos princípios da proporcionalidade, transparência e melhoria contínua, em consonância com o ciclo *Plan–Do–Check–Act* (PDCA). Para tal, mobiliza referenciais amplamente reconhecidos: o *Referencial de Competências em Cibersegurança* do CNCS (2022), o *Cybersecurity Education Maturity Assessment* da ENISA (2024), os quadros DigCompEdu e SELFIE da Comissão Europeia (2022a; 2022b) e as *Cyber Security Standards for Schools and Colleges* publicadas pelo Department for Education (Reino Unido, 2025).

Do ponto de vista legal, a conformidade é assegurada pelo Regulamento Geral sobre a Proteção de Dados (RGPD), nomeadamente pelos art.º 24.º, 25.º, 32.º e 35.º, pelas diretrizes da CNPD (2018/1; 2023/1) e pela Diretiva NIS 2 (UE, 2022), que estabelece, nos art.º 21.º e 22.º, a necessidade de medidas regulares de monitorização e revisão de políticas de segurança. O enquadramento é ainda reforçado pelo *Digital Services Act* (Regulamento UE 2022/2065), cujo art.º 32.º sublinha a importância da proteção e da literacia digital dos menores. A norma ISO/IEC 27002:2022 complementa este quadro, ao oferecer controlos operacionais de referência aplicáveis ao contexto escolar.

5.6.2. Estrutura organizacional de monitorização

A monitorização e avaliação do plano são asseguradas por uma estrutura organizacional partilhada entre várias equipas e órgãos de gestão. A Equipa de Desenvolvimento Digital (EDD) coordena a monitorização operacional, o Encarregado de Proteção de Dados (DPO) supervisiona a conformidade legal, incluindo processos de pseudonimização e avaliações de impacto (DPIA) e a equipa TIC é responsável pela monitorização técnica através de sistemas SIEM, avaliando indicadores como o *Mean Time to Detect* (MTTD) e o *Mean Time to Respond* (MTTR).

As estruturas pedagógicas, nomeadamente os departamentos curriculares, os diretores de turma e a Biblioteca Escolar/Centro de Recursos Educativos (BE/CRE), são responsáveis pela recolha de evidências formativas e pela avaliação do impacto das ações de capacitação e cultura digital. A Direção

consolida os dados recolhidos, valida o Relatório Anual de Gestão de Cibersegurança e aprova as atualizações do plano.

5.6.3. Modelo de indicadores e fontes de evidência

Os indicadores definidos combinam métricas técnicas, pedagógicas e organizacionais, estabelecendo linhas de base (T0) e metas anuais, de forma a garantir alinhamento direto com o plano de implementação (5.4).

Entre os domínios de medição incluem-se a postura técnica e a resiliência, a proteção de dados, a capacitação e a literacia digital. A Tabela 5.6-A apresenta uma síntese dos principais indicadores, das respetivas frequências de recolha, das fontes de evidência e dos referenciais normativos associados.

Tabela 5.6 — Domínios de medição, métricas, frequência, fontes e referenciais normativos

Domínio	Métricas principais	Frequência	Fontes de evidência	Norma/Referencial
Postura técnica e resiliência	Cobertura MFA ≥ 95 %; tempo médio de correção ≤ 14 dias; conformidade EDR/MDM; sucesso nos restauros 3-2-1; percentagem de ativos com *logs* centralizados; MTTD/MTTR	Mensal / Trimestral	Relatórios SIEM e EDR; testes de *backup* e restauro	ISO/IEC 27002 (8.2; 8.13; 8.16; 8.18–8.19); DfE (2025)
Proteção de dados	Percentagem de processos críticos com DPIA/TIA; tempo de resposta a pedidos de titulares; percentagem de não conformidades corrigidas ≤ 30 dias	Trimestral / Semestral	Registos do DPO; auditorias internas	RGPD (24–25; 32; 35); CNPD (2018/1; 2023/1)
Capacitação	Percentagem de docentes e não docentes formados; ganho de proficiência (pré/pós-teste); índice DigCompEdu médio; *score* SELFIE	Anual	Questionários; relatórios de formação	DigCompEdu; SELFIE; ENISA (2024); Palacios-Rodríguez et al. (2025)
Comportamentos e literacia digital	Taxa de cliques em simulações de *phishing*; retenção de aprendizagens; participação parental; perceção de segurança digital	Trimestral / Anual	Simulações; inquéritos; portefólios de turma	Xu & Li (2025); Jerman Blažič & Jerman Blažič (2025); EurofamNet; E-REDES & DGE (2022)

Nota. MFA = autenticação multifator; EDR = *Endpoint Detection and Response*; MDM = *Mobile Device Management*; SIEM = *Security Information and Event Management*; DPIA = *Data Protection Impact Assessment*; TIA = *Transfer Impact Assessment*. Dados elaborados com base no plano de cibersegurança do Agrupamento de Escolas Passos Manuel (2025).

Estas métricas serão apoiadas por evidências documentais provenientes do formulário digital de reporte de incidentes, dos relatórios SIEM e EDR/MDM, das auditorias internas semestrais (com *checklists* alinhadas com a ISO/IEC 27002:2022), dos resultados SELFIE e DigCompEdu, dos questionários de perceção aplicados a alunos e docentes e dos registos de DPIA/TIA arquivados pelo DPO.

5.6.4. Processos de frequência e monitorização

O sistema de monitorização organiza-se em quatro ciclos complementares. A periodicidade mensal ou trimestral será definida na fase de implementação do plano, pela Direção e pelas equipas responsáveis, em função do nível de maturidade digital, da capacidade operacional e da criticidade dos sistemas monitorizados.

O ciclo contínuo, de carácter mensal ou trimestral, assegura a recolha e consolidação de dados técnicos, incluindo *logs*, alertas SIEM, revisões de acessos privilegiados, aplicação de *patches* e testes de *backup*. Os limites de alerta (*thresholds*) estabelecem que valores de MFA inferiores a 95 %, taxas de correção de vulnerabilidades abaixo de 90 % em catorze dias ou falhas de restauro superiores a 0 % são considerados críticos.

O ciclo semestral é dedicado às auditorias internas, que incluem a verificação das políticas institucionais, dos consentimentos, dos contratos e das avaliações de impacto, bem como a realização de testes de penetração de baixo impacto.

O ciclo anual contempla a aplicação dos instrumentos SELFIE e DigCompEdu, a realização de inquéritos de perceção, a análise curricular e a avaliação da maturidade digital com base na metodologia ENISA (2024).

Por fim, realiza-se uma revisão de gestão anual, conduzida pela Direção, que consiste na apreciação dos resultados técnicos e pedagógicos, na redefinição de prioridades e metas e na publicação do Relatório Anual de Gestão de Cibersegurança, até 31 de janeiro de cada ano.

5.6.5. Qualidade dos dados, ética e proteção da informação

O processo de monitorização respeita os princípios da minimização e da separação entre dados pessoais e operacionais, assegurando uma retenção máxima de noventa dias para *logs*, conforme o art.º 5.º do RGPD. Os dados recolhidos em simulações ou inquéritos são pseudonimizados e o acesso

aos sistemas SIEM é restrito por perfis, com registo de operações para efeitos de auditoria. Os relatórios públicos utilizam indicadores agregados e anonimizados, preservando a privacidade dos intervenientes e a integridade dos dados.

5.6.6. Revisão e atualização do plano

A revisão e atualização do plano seguem o modelo PDCA (*Plan – Do – Check – Act*)[1], integrando os resultados técnicos, pedagógicos e de conformidade recolhidos ao longo do ano. O Relatório Anual de Gestão de Cibersegurança[2] constitui o principal instrumento de retroalimentação e decisão, consolidando indicadores e recomendações. As atualizações do plano refletem as novas ameaças identificadas, as melhores práticas internacionais e as alterações normativas, incluindo as emanadas da União Europeia (UE, 2022), da ENISA (2024) e do CNCS (2022).

5.6.7. Envolvimento da comunidade educativa

O modelo de monitorização e avaliação integra mecanismos participativos, valorizando o contributo de todos os membros da comunidade educativa. Serão recolhidos feedbacks estruturados de alunos, docentes, não docentes e encarregados de educação através de questionários, fóruns e reuniões periódicas. As iniciativas *Digital Parenting* (EurofamNet, 2023) e *Digital Academy for Parents* (E-REDES & DGE, 2022) serão avaliadas quanto à taxa de participação, ao impacto percebido e à satisfação dos participantes.

Os resultados serão incorporados no *dashboard* trimestral do PAA e no relatório anual, reforçando a articulação entre as estratégias formativas (5.5) e a cultura de segurança institucional.

5.6.8. Síntese conclusiva

A monitorização e avaliação constituem a base de sustentabilidade do Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel. O sistema aqui descrito assegura não apenas a conformidade

[1] O ciclo PDCA é uma metodologia de melhoria contínua baseada em quatro fases: planear, executar, verificar e atuar, assegurando revisão constante das práticas.
[2] Documento anual que consolida resultados técnicos, pedagógicos e de conformidade, servindo de base à atualização do plano e à prestação de contas.

legal e normativa, mas também a aprendizagem organizacional, permitindo ao agrupamento evoluir continuamente e adaptar-se às exigências de um ecossistema digital em transformação.

A integração entre as dimensões técnica, pedagógica e ética garante uma abordagem holística e consolidada, sustentando a construção de uma verdadeira cultura de resiliência e segurança digital em contexto educativo[1].

[1] Elaboração própria, com base no Plano de Cibersegurança proposto para o Agrupamento de Escolas Passos Manuel (2025).

CAPÍTULO 6

Conclusão

A conclusão do presente trabalho confirma a integração plena entre rigor científico, conformidade normativa e relevância prática. O diagnóstico aprofundado da maturidade cibernética do Agrupamento de Escolas Passos Manuel (AEPM) e a subsequente construção do seu Plano de Cibersegurança institucional evidenciam uma abordagem inovadora, assente na gestão responsável, na proteção de dados e na promoção de práticas educacionais seguras, inclusivas e alinhadas com os referenciais nacionais e europeus.

O percurso metodológico seguido demonstrou elevada consistência e fiabilidade, combinando a revisão sistemática segundo a metodologia PRISMA (Sousa et al., 2024) com a análise documental e empírica, bem como com a correspondência explícita às normas ISO/IEC 27001 e 27002, ao Regulamento Geral sobre a Proteção de Dados (RGPD), à Diretiva NIS 2, ao *Digital Services Act* e às diretrizes do Centro Nacional de Cibersegurança. Todas as etapas, desde a identificação das lacunas até à construção dos instrumentos de diagnóstico e à definição das estratégias técnicas, organizacionais e pedagógicas, foram sustentadas em referências legislativas, técnicas e educativas, garantindo replicabilidade, transparência e rastreabilidade científica. Os resultados e a metodologia desenvolvidos no presente estudo reúnem condições para futura adaptação e submissão a publicação científica, nomeadamente sob a forma de artigo académico.

O plano proposto para o AEPM institui uma articulação singular entre as dimensões técnica, organizacional e pedagógica, abrangendo desde a gestão centralizada de ativos digitais e a autenticação multifatorial até à formação contínua de todos os perfis da comunidade educativa. Inclui ainda mecanismos de prevenção e resposta a incidentes, bem como medidas de inclusão e acessibilidade digital. O ciclo de melhoria contínua implementado assegura a monitorização e atualização regular das medidas, com base em indicadores SMART que permitem avaliar o impacto das ações, ajustar prioridades e garantir conformidade com os normativos mais recentes.

Do ponto de vista científico, o trabalho contribui para o aprofundamento da investigação aplicada em cibersegurança educacional, ao propor um modelo de planeamento e diagnóstico replicável noutras instituições escolares. No plano institucional, reforça a capacidade de autogoverno digital do Agrupamento Passos Manuel, oferecendo instrumentos que integram gestão, pedagogia e conformidade legal. No plano social, promove uma cultura de confiança, ética e responsabilidade digital, em consonância com as prioridades nacionais e europeias de cidadania e inclusão digital.

Reconhece-se, contudo, que o plano proposto requer acompanhamento contínuo e avaliação periódica para aferir a sua eficácia a médio prazo e a capacidade de adaptação às evoluções tecnológicas e normativas. Futuras investigações poderão centrar-se na monitorização da maturidade cibernética institucional, na análise comparada entre escolas portuguesas e europeias e na avaliação do impacto das ações de sensibilização digital na mudança de comportamentos.

Conclui-se que o presente trabalho se assume como um modelo de referência para o setor educativo nacional, ao propor práticas, instrumentos e políticas que contribuem de forma decisiva para a construção de uma comunidade escolar mais segura, resiliente e consciente dos riscos digitais contemporâneos. O compromisso ético e legal é assegurado em todos os domínios, garantindo simultaneamente a proteção efetiva dos dados pessoais, a continuidade dos serviços educativos e o reforço das competências digitais de toda a comunidade educativa.

O presente trabalho não se encerra em si mesmo, prevendo-se que o Plano de Cibersegurança desenvolvido seja apresentado à Direção do Agrupamento de Escolas Passos Manuel para apreciação interna, podendo constituir uma base estruturante para futura implementação, monitorização e ajuste progressivo das medidas propostas. A sua aplicação em contexto real poderá ainda sustentar processos de avaliação interna e estudos de acompanhamento, contribuindo para o reforço contínuo da maturidade digital e cibernética da instituição.

Por fim, reafirma-se a importância de integrar a cibersegurança na cultura organizacional das escolas, reconhecendo-a não apenas como um requisito técnico, mas como um princípio educativo e de cidadania. A consolidação desta abordagem sustentará a evolução do plano no tempo e abrirá caminho a novas práticas e investigações sobre a maturidade cibernética e a transformação digital no sistema educativo português.

Referências bibliográficas

Abrantes, P. (2020). *Aprender com robots* [Dissertação de mestrado, Universidade Aberta]. Repositório da Universidade Aberta.

Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. *Journal of Information Security, 12*(4), 233–249. https://doi.org/10.4236/jis.2021.124013

Antunes, M., & Rodrigues, A. (2021). *Introdução à cibersegurança.* FCA Editora.

Antunes, M. J., Silva, R., & Marques, J. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences, 11*(23), 11269. https://doi.org/10.3390/app112311269

Agrupamento de Escolas Passos Manuel (AEPM). (2021). *Plano de Ação para o Desenvolvimento Digital da Escola (PADDE) 2021–2023.* Agrupamento de Escolas Passos Manuel. https://aepassosmanuel.pt/quem-somos/instrumentos-de-autonomia/

Agrupamento de Escolas Passos Manuel (AEPM). (2023). *Projeto Educativo 2023–2026.* Agrupamento de Escolas Passos Manuel. https://aepassosmanuel.pt/quem-somos/instrumentos-de-autonomia/

Agrupamento de Escolas Passos Manuel (AEPM). (2023b). *Estratégia de Educação para a Cidadania na Escola (EECE) 2023/24.* Agrupamento de Escolas Passos Manuel. https://aepassosmanuel.pt/quem-somos/instrumentos-de-autonomia/

Agrupamento de Escolas Passos Manuel (AEPM). (2024). *Regulamento Interno 2024.* Agrupamento de Escolas Passos Manuel. https://aepassosmanuel.pt/quem-somos/instrumentos-de-autonomia/

Agrupamento de Escolas Passos Manuel (AEPM). (2025). *Formulário de Diagnóstico de Cibersegurança – Agrupamento de Escolas Passos Manuel.* Instrumento elaborado por Andreia Patrícia Semedo Motaco no âmbito do Mestrado em Transformação Digital no Ensino e da Aprendizagem, ISCTE-IUL. https://docs.google.com/forms/d/e/1FAIpQLSdxapiKJUbOYb5HLGcgcvk8cInTWiPuI1RMH8iR4ze-QIJF8A/viewform?usp=header

Centro Nacional de Cibersegurança (CNCS). (2021). *Plano de Cibersegurança na Educação – Linhas orientadoras para escolas e agrupamentos.* https://www.cncs.gov.pt/

Centro Nacional de Cibersegurança (CNCS). (2024a). *Guia de Transição Digital.* https://www.cncs.gov.pt/pt/guia-de-transicao-digital/

Centro Nacional de Cibersegurança (CNCS). (2024b). *Referencial de Competências em Cibersegurança.* https://www.cncs.gov.pt/pt/referencial-de-competencias/

Centro Nacional de Cibersegurança (CNCS) & Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto (FPCEUP). (2024). *Educação para a Cibersegurança no Ensino Básico e Secundário em Portugal.* https://www.cncs.gov.pt/pt/educacao-para-a-ciberseguranca/

Chahid, A., Rachid, M., Chafiq, M., & Bakkoury, Z. (2025). Digital transformation in higher education: Obstacle assessment and development of strategies against cybersecurity threats—The case of Moroccan universities. *Engineering, Technology & Applied Science Research, 15*(1), 8853–8860. https://doi.org/10.48084/etasr.8853

Comissão Europeia (2019–2024). *Uma Europa preparada para a era digital.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt

Comissão Europeia. (2022a). *Orientações para professores e educadores sobre o combate à desinformação e a promoção da literacia digital através da educação e da formação* [Versão em português]. https://data.europa.eu/doi/10.2766/283100

European Commission. (2022b). *Guidelines for teachers to foster digital literacy and tackle disinformation* [English version]. https://education.ec.europa.eu/focus-topics/digital-education/action-plan/guidelines-for-teachers-to-foster-digital-literacy-and-tackle-disinformation

Comissão Nacional de Proteção de Dados (CNPD). (2018). *Diretriz 1/2018 – Disponibilização de dados pessoais em instituições de ensino superior.* https://www.cnpd.pt/

Comissão Nacional de Proteção de Dados (CNPD). (2023). *Diretriz 1/2023 – Medidas organizativas e de segurança aplicáveis ao tratamento de dados pessoais.* https://www.cnpd.pt/

Department for Education (DfE). (2025). *Cyber security standards for schools and colleges.* UK Government. https://www.gov.uk/government/publications/cyber-security-standards-for-schools-and-colleges

Dias, I. (2022). *Literacia digital e cidadania: desigualdades no acesso e uso das plataformas digitais do Estado* [Dissertação de mestrado, ISCTE]. Repositório do ISCTE.

Direção-Geral da Educação (DGE) & E-REDES. (2024). *Digital Academy for Parents.* https://erte.dge.mec.pt/

Direção-Geral da Educação (DGE). (2023). *ERTE em Números #2.* Direção-Geral da Educação. https://erte.dge.mec.pt/

ENISA – European Union Agency for Cybersecurity. (2023). *ENISA Maturity Framework for Public Sector.* https://www.enisa.europa.eu/

ENISA – European Union Agency for Cybersecurity. (2024a). *Cybersecurity Education Maturity Framework.* https://www.enisa.europa.eu/topics/education/cybersecurity-education-maturity

ENISA – European Union Agency for Cybersecurity. (2024b). *ENISA Threat Landscape 2024.* https://www.enisa.europa.eu/topics/threat-landscape

EurofamNet. (2023). *Digital Parenting.* COST Action CA18123. https://www.eurofamnet.eu/

Figueiredo, L., Serrão, C., & Almeida, J. (2023). Deep learning model transposition for network intrusion detection systems. *Electronics, 12*(21), 4137. https://doi.org/10.3390/electronics12214137

Governo de Portugal. (2020). *Plano de Ação para a Transição Digital.* República Portuguesa. https://www.portugal.gov.pt/

Instituto Nacional de Estatística (INE). (2023). *Sociedade da Informação e do Conhecimento 2023.* https://www.ine.pt/

International Organization for Standardization (ISO). (2022a). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* ISO.

International Organization for Standardization (ISO). (2022b). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls.* ISO.

Jerman Blažič, B., & Jerman Blažič, A. (2025). Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. *Education and Information Technologies, 30*(4), 543–562. https://doi.org/10.1007/s10639-025-13155-3

Lopes, A. S., Sargento, A., & Farto, J. (2023). Training in digital skills—The perspective of workers in public sector. *Sustainability, 15*(13), 10577. https://doi.org/10.3390/su151310577

Monteiro, A., & Gomes, M. J. (2009). Comportamentos de risco na Internet por parte de jovens portugueses: Um estudo exploratório. In *Actas do X Congresso Internacional Galego-Português de Psicopedagogia* (pp. 5599–5613). Universidade do Minho. ISBN 978-972-8746-71-1

Palacios-Rodríguez, A., García-Holgado, A., Camacho, M., & García-Peñalvo, F. J. (2025). Macroassessment of teachers' digital competence: DigCompEdu study in Spain and Portugal. *Education and Information Technologies, 30*(2), 1245–1264. https://doi.org/10.1007/s10639-025-13092-1

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Patel, A. (Realizador). (2023). *Os segredos dos nossos dados* [Documentário]. BBC Studios.

Rajamäki, J., Ahonen, O., Rathod, P., Serrão, C., Ferreira, J. C., & Gomes, M. C. (2024, April). Enhancing cybersecurity education for the healthcare sector: Fostering interdisciplinary ManagiDiTH approach. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 979–989). IEEE. https://doi.org/10.1109/EDUCON60312.2024.10578769

Seara, F., & Serrão, C. (2024). Automation of system security vulnerabilities detection using open-source software. *Electronics, 13*(5), 1028. https://doi.org/10.3390/electronics13051028

Serrão, C., Neves, R., & Rodrigues, J. (2003). Open SDRM – An open and secure digital rights management solution. In *Proceedings of the 3rd International Conference on Web Engineering.*

Sousa, J. L., Gonçalves-Lopes, S., Abreu, V., & Oliveira, V. (2024). Declaração PRISMA 2020: Uma diretriz atualizada para publicação de revisões sistemáticas. *Germinare, 4*, 1–19. https://doi.org/10.5281/zenodo.13271469

Tirumala, S. S., Valluri, S., & Babu, B. R. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 334–339). IEEE. https://doi.org/10.1109/ICCIKE47802.2019.9004300

U.S. Department of Education. (2023). *Cybersecurity Maturity Model for K–12 Education.* https://www.ed.gov/

União Europeia (UE). (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção de dados pessoais (RGPD).* EUR-Lex. https://eur-lex.europa.eu/

União Europeia (UE). (2022a). *Diretiva (UE) 2022/2555 (NIS 2) relativa à segurança das redes e dos sistemas de informação.* EUR-Lex. https://eur-lex.europa.eu/

União Europeia (UE). (2022b). *Regulamento (UE) 2022/2065 – Digital Services Act (DSA).* EUR-Lex. https://eur-lex.europa.eu/

Van Zeller, M. (2022). *The Cyber War* [Documentário]. National Geographic. https://youtu.be/jtrFTHlUJ5Q

Veiga, P. (2024). *Cibersegurança.* Fundação Francisco Manuel dos Santos.

Xu, H., & Li, L. (2025). Cybersecurity matters for primary school students: A scoping review of the trends, challenges, and opportunities. *Education and Information Technologies, 30*(2), 233–260. https://doi.org/10.1007/s10639-024-13155-3

Glossário de termos e conceitos

O presente glossário reúne, de forma sistemática e organizada, os principais termos, siglas e conceitos utilizados ao longo da tese de Mestrado em *Transformação Digital no Ensino e Aprendizagem*, centrada no *Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel* (AEPM).

Para além dos conceitos estritamente ligados à cibersegurança, incluem-se também referências normativas, pedagógicas e institucionais que se revelam fundamentais para a compreensão integral do trabalho. O glossário apresenta-se em português de Portugal, com equivalentes em inglês sempre que relevante, e encontra-se estruturado alfabeticamente (A - Z) para facilitar a consulta rápida e a leitura autónoma.

ABAC (Attribute-Based Access Control): Modelo de controlo de acessos baseado em atributos do utilizador, do recurso e do contexto; permite políticas mais granulares do que o RBAC.

Accountability (Responsabilização): Princípio do RGPD/ISO que exige demonstração de conformidade e prestação de contas sobre decisões e processos.

AEPM - Agrupamento de Escolas Passos Manuel.

AIPD / DPIA (Avaliação de Impacto sobre a Proteção de Dados / Data Protection Impact Assessment): Avaliação formal de riscos para direitos e liberdades dos titulares, exigida pelo RGPD para tratamentos de alto risco.

Anonymização: Processo irreversível de remoção de identificadores pessoais; dados anonimizados deixam de ser dados pessoais.

ARP (Address Resolution Protocol): Protocolo que mapeia endereços IP para MAC em LAN; vulnerável a ARP spoofing/man-in-the-middle.

Asset management (Gestão de ativos): Processo de inventariação e controlo de todos os equipamentos, software e dados críticos da organização.

AUP (Acceptable Use Policy / Política de Utilização Aceitável): Regras de uso aceitável dos recursos TIC da escola, diferenciadas por perfil (alunos, docentes, não docentes, EE).

Backups 3-2-1: Estratégia de cópias de segurança: 3 cópias dos dados, em 2 suportes distintos, com 1 cópia off-site.

Badges digitais (Digital Badges): Credenciais digitais usadas para certificar a conclusão de formações ou aquisição de competências.

Baseline (Linha de base): Valor inicial de referência (T0) para medir evolução e eficácia de medidas.

BE/CRE (Biblioteca Escolar / Centro de Recursos Educativos): Unidade responsável, entre outros, pelo onboarding digital (criação/entrega de credenciais institucionais).

Benchmark CIS (CIS Benchmarks): Boas práticas de hardening publicadas pelo Center for Internet Security.

BYOD (Bring Your Own Device): Uso de dispositivos pessoais em contexto escolar, com salvaguardas via MDM e segmentação.

Captive portal: Mecanismo de autenticação em redes Wi-Fi de convidados que redireciona o utilizador para uma página de login.

CCTV (Closed-Circuit Television): Sistema de videovigilância em circuito fechado; sujeito ao RGPD/deliberações da CNPD.

CEB (Ciclo do Ensino Básico): Designação dos três ciclos do ensino básico (1.º, 2.º e 3.º CEB).

CERT.PT: Centro de Resposta a Incidentes de Cibersegurança em Portugal, coordenado pelo CNCS.

CG (Conselho Geral): Órgão de direção estratégica do AEPM; recebe o Relatório Anual de Cibersegurança.

Ciclo PDCA (Plan–Do–Check–Act): Metodologia de melhoria contínua aplicada à execução e avaliação do plano.

CIA (Confidencialidade, Integridade, Disponibilidade): Tríade fundamental da segurança da informação.

CIS (Center for Internet Security): Organização que publica os CIS Controls e os CIS Benchmarks.

CIS Controls v8: Conjunto de 18 controlos críticos de segurança (2021), orientador de boas práticas.

Compliance (Conformidade): Adesão a normas, leis e políticas internas aplicáveis a processos organizacionais.

Cloud / Serviços em nuvem (IaaS, PaaS, SaaS): Modelos de disponibilização de recursos geridos remotamente por terceiros (ex.: Google Workspace, Microsoft 365).

Cloud Security (Segurança na Nuvem): Conjunto de políticas e controlos aplicados a serviços cloud (IaaS, PaaS, SaaS) para garantir confidencialidade, integridade e disponibilidade.

CNCS (Centro Nacional de Cibersegurança): Autoridade nacional para cibersegurança; emite referenciais, guias e coordena o CERT.PT.

CNPD (Comissão Nacional de Proteção de Dados): Autoridade nacional de supervisão de proteção de dados; emite diretrizes e deliberações.

Contas privilegiadas: Contas com permissões elevadas (administração, direção, TIC); requerem MFA, registo/auditoria e idealmente PAM.

Cópia imutável (WORM): *Write Once Read Many*; suporte de armazenamento/backups que impede alterações após escrita.

CP (Conselho Pedagógico): Órgão que aprova políticas pedagógicas e acompanha indicadores e formação.

CVE (Common Vulnerabilities and Exposures): Base pública de vulnerabilidades conhecidas.

CVSS (Common Vulnerability Scoring System): Sistema de pontuação da gravidade de vulnerabilidades.

CWE (Common Weakness Enumeration): Catálogo de fraquezas comuns em software.

DA (Digital Academy for Parents): Programa nacional de literacia parental em competências digitais e cibersegurança.

Dashboard de monitorização: Painel visual que apresenta indicadores e métricas de cibersegurança e desempenho institucional.

Data governance (Governação de dados): Estrutura de políticas e responsabilidades que assegura a gestão ética e segura da informação.

Defesa em profundidade (Defense in Depth): Estratégia de camadas redundantes de segurança em pessoas, processos e tecnologia.

DGE (Direção-Geral da Educação): Órgão do ME que coordena políticas para a transição digital e a cibersegurança nas escolas.

DfE (Department for Education): Ministério da Educação do Reino Unido; autor dos *Cyber Security Standards for Schools and Colleges* (2025).

DigComp 2.2: Quadro europeu de competências digitais para cidadãos (5 domínios, 21 competências).

DigCompEdu: Quadro europeu de competências digitais dos educadores.

Digital footprint (Pegada digital): Conjunto de informações que um utilizador deixa online, voluntária ou involuntariamente.

DKIM (DomainKeys Identified Mail): Mecanismo de autenticação de e-mail baseado em assinaturas digitais (chaves públicas).

DL n.º 95/2025: Diploma que regula o uso de telemóveis no 1.º e 2.º ciclo do ensino básico.

DLP (Data Loss Prevention): Políticas e ferramentas que impedem exfiltração não autorizada de dados.

DMARC (Domain-based Message Authentication, Reporting and Conformance): Política de autenticação de e-mail baseada em SPF e DKIM; define ações como *quarantine/reject*.

DPO / EPD (Data Protection Officer / Encarregado de Proteção de Dados): Responsável pela conformidade RGPD, registos, DPIA e notificações de violação.

DRM (Digital Rights Management): Tecnologias de controlo de acesso/uso de conteúdos; ex.: Open SDRM.

DSA (Digital Services Act): Regulamento (UE) 2022/2065 sobre serviços digitais; inclui proteção de menores e literacia (art.º 32).

DT (Transição Digital): Termo usado no PADDE e em políticas nacionais.

EAP (Extensible Authentication Protocol): Protocolo de autenticação usado em WPA3/802.1X para Wi-Fi *Enterprise*.

E-safety (Segurança online): Conjunto de práticas, políticas e comportamentos que visam proteger os utilizadores, especialmente alunos, de riscos digitais como fraude, ciberbullying e exposição indevida de dados pessoais em ambientes virtuais.

EB / EB1 / JI: Escolas Básicas; Escolas Básicas de 1.º ciclo com Jardim de Infância.

ECSF (European Cybersecurity Skills Framework): Quadro europeu de competências profissionais em cibersegurança.

Email security (Segurança de e-mail): Conjunto de mecanismos técnicos e organizativos que protegem as comunicações eletrónicas contra ameaças como *phishing, spoofing* e *malware,* incluindo o uso de protocolos SPF, DKIM e DMARC.

EDD (Equipa de Desenvolvimento Digital) - Estrutura interna que coordena a monitorização e avaliação (M&A) operacional do plano.

EDR (Endpoint Detection and Response): Tecnologia de proteção/monitorização contínua de *endpoints*; suporta deteção e resposta a ameaças.

Encryption (Encriptação): Processo de codificação de informação que a torna ilegível para utilizadores não autorizados, garantindo confidencialidade e integridade dos dados durante o armazenamento ou transmissão (ex.: TLS, cifra de disco).

EdTech (Educational Technology): Plataformas e ferramentas digitais para educação (LMS, apps, etc.).

EE (Encarregados de Educação): Pais ou tutores legais dos alunos.

EECE (Estratégia de Educação para a Cidadania na Escola): Documento orientador para cidadania e literacia digital.

ENISA (EU Agency for Cybersecurity): Agência da UE para cibersegurança; publica cenários de ameaça e boas práticas.

Endpoint: Dispositivo final (PC, portátil, tablet, smartphone) com acesso a serviços institucionais.

Endpoint management (Gestão de dispositivos): Administração centralizada de computadores, tablets e outros dispositivos conectados à rede institucional, assegurando atualizações, controlo de acessos, encriptação e políticas de segurança consistentes.

EPAVE: Escola Profissional do Alto Ave; exemplo nacional de plano de cibersegurança.

Engenharia social (Social engineering): Técnica de manipulação psicológica usada por cibercriminosos para induzir utilizadores a revelar informações confidenciais ou realizar ações que comprometam a segurança digital.

ERTE (Equipa de Recursos e Tecnologias Educativas): Unidade da DGE responsável por políticas digitais e formação TIC.

FPCEUP: Faculdade de Psicologia e Ciências da Educação da Universidade do Porto.

Firewall / NGFW (Next-Generation Firewall): Dispositivo/serviço de filtragem de tráfego com inspeção de aplicação, IPS e controlo granular.

Framework de maturidade: Estrutura que permite avaliar o nível de evolução de uma organização em cibersegurança ou competências digitais.

Formulário digital de incidentes: Canal padronizado para reporte e triagem de incidentes pela comunidade escolar.

Fuga de dados / Data breach: Divulgação ou acesso não autorizado a dados pessoais ou sensíveis.

Fake news (Notícias falsas): Informação intencionalmente incorreta ou enganosa, disseminada para manipular a perceção pública.

GAAF (Gabinete de Apoio ao Aluno e à Família): Estrutura de apoio socioeducativo envolvida em ações de literacia digital com famílias.

Gamificação (Gamification): Uso de dinâmicas de jogo em contextos educativos ou de formação para aumentar o envolvimento.

Gestão de identidades (IAM): Gestão de ciclo de vida de contas, perfis e acessos (inclui SSO, RBAC/ABAC, JML).

Governança de TI: Políticas, RACI e comités que asseguram direção e controlo das TIC.

Hardening: Endurecimento de sistemas por remoção de serviços desnecessários e aplicação de benchmarks de configuração segura.

Hash (Função de dispersão): Algoritmo que converte dados em valores únicos e irreversíveis, usado em autenticação e integridade de ficheiros.

IA (Inteligência Artificial): Técnicas (incl. ML) aplicadas à deteção de intrusões e análise de anomalias.

IDS / IPS (Intrusion Detection/Prevention System): Sistemas que detetam (IDS) e previnem (IPS) atividades maliciosas.

Identidade digital (Digital identity): Conjunto de informações e credenciais eletrónicas que permitem identificar e autenticar um utilizador ou entidade num sistema digital, garantindo o acesso seguro a serviços e dados.

IEC (International Electrotechnical Commission): Organização que, com a ISO, desenvolve normas internacionais.

INE (Instituto Nacional de Estatística): Entidade estatística oficial de Portugal.

Indicadores de desempenho (KPIs): Métricas quantitativas ou qualitativas utilizadas para avaliar a eficácia das ações do plano de cibersegurança, como taxas de incidentes, cumprimento de prazos e níveis de conformidade.

INOVAR PAA: Módulo do sistema INOVAR usado para gestão/monitorização do PAA.

IoT (Internet of Things): Rede de dispositivos conectados à internet (ex.: sensores, câmaras, tablets) que requerem medidas de segurança específicas.

ISO/IEC 27001: Norma para Sistemas de Gestão de Segurança da Informação (SGSI); certificável.

ISO/IEC 27002:2022: Norma de controlos de segurança; referência para implementação/ mapeamento.

JML (Joiners–Movers–Leavers): Processo de criação, alteração e remoção de acessos ao longo do ciclo de vida do utilizador.

Kahoot / Mentimeter: Ferramentas de quizzes e feedback em tempo real usadas em capacitação/sensibilização.

KPI (Key Performance Indicator): Indicador-chave de desempenho para medir objetivos do plano.

Literacia digital: Conjunto de competências cognitivas, técnicas e críticas que permitem utilizar, compreender e avaliar de forma segura e responsável as tecnologias digitais, promovendo a cidadania informada e a inclusão.

LED (Laboratórios de Educação Digital): Rede nacional de laboratórios para inovação pedagógica com tecnologia.

Liderança digital (Digital leadership): Capacidade de orientar equipas e processos educativos no uso estratégico e ético das tecnologias, fomentando a inovação, a segurança digital e a transformação organizacional.

LMS (Learning Management System): Plataforma de gestão de aprendizagem (Moodle, Google Classroom).

Logging / Registo centralizado: Consolidação de registos (autenticações, privilégios, alterações, firewall, EDR/AV, e-mail, backups) em SIEM para deteção/auditoria (retenção ≥ 90 dias).

Maturidade digital (Digital maturity): Nível de desenvolvimento e integração das tecnologias digitais numa organização, avaliado em dimensões como liderança, competências, infraestrutura e segurança, e usado para orientar processos de melhoria contínua.

M&A (Monitorização e Avaliação): Sistema de acompanhamento contínuo e avaliação periódica do plano, com reporte a CP/Direção/CG.

Malware: Software malicioso (vírus, *worms, trojans* e *ransomware*).

MDM (Mobile Device Management): Gestão de dispositivos móveis (políticas de PIN, encriptação, bloqueio remoto).

MFA / 2FA: Autenticação multifator/dois fatores (algo que sabe/tem/é).

Mitigação de risco (Risk mitigation): Conjunto de medidas preventivas e corretivas destinadas a reduzir a probabilidade e o impacto de ameaças, assegurando resiliência operacional e continuidade das atividades.

ML (Machine Learning): Aprendizagem automática, usada em modelos de deteção de intrusões e UEBA.

MTTD / MTTR: Tempos médios de deteção e de resposta a incidentes.

MTTA (Mean Time to Acknowledge): Tempo médio para reconhecer/registar um incidente após a sua deteção.

M1, M2, M3, M4: Marcos de implementação (6, 12, 24, 36 meses) do plano.

NEE (Necessidades Educativas Especiais): Alunos com apoio diferenciado; inclui acessibilidade digital.

NGFW (Next-Generation Firewall): Firewall de próxima geração com inspeção de aplicação, IPS e controlo granular.

NIDS (Network Intrusion Detection System): IDS dedicado à monitorização de tráfego de rede.

NIS 2: Diretiva (UE) 2022/2555 que reforça requisitos de cibersegurança para entidades públicas/privadas.

NIST CSF (Cybersecurity Framework): Quadro do NIST com funções Identificar, Proteger, Detetar, Responder, Recuperar.

NIST SP 800-63: Recomendações sobre identidade digital e MFA.

NIST SP 800-115: Norma de metodologias de testes de intrusão/*pentesting*.

Norma ISO 27036 (Gestão de fornecedores): Norma internacional que define requisitos e boas práticas para garantir a segurança da informação na relação com terceiros e fornecedores, reforçando a avaliação de riscos e a proteção de dados partilhados.

Newsletter de segurança: Comunicação periódica de sensibilização e boas práticas para a comunidade escolar.

Notificação de incidentes (Incident notification): Processo formal de comunicação de incidentes de segurança às autoridades competentes e aos titulares de dados, em conformidade com o RGPD (art.º 33.º–34.º) e a Diretiva NIS 2.

Open SDRM: Arquitetura *open-source* de DRM baseada em *Web Services* e XML *Security*.

Open source (Código aberto): Modelo de desenvolvimento e distribuição de software cujo código-fonte é público e pode ser livremente utilizado, modificado e partilhado, favorecendo a transparência e a inovação colaborativa.

OpenBadges: Credenciais digitais abertas para reconhecimento de competências (ex.: badges de cibersegurança).

Onboarding digital: Criação/entrega formal de credenciais institucionais (no AEPM, via BE/CRE).

Operacionalização (Operationalization): Processo de implementação prática de um plano, estratégia ou política, através da definição clara de ações, responsabilidades, cronogramas e indicadores de desempenho.

OpenVAS: Ferramenta *open-source* para scans e avaliação de vulnerabilidades em redes e sistemas.

OWASP Top 10 / CWE Top 25: Taxonomias de vulnerabilidades/fraquezas mais críticas para auditoria e *pentesting*.

PADDE (Plano de Ação para o Desenvolvimento Digital da Escola): Documento estratégico de transição digital das escolas.

Perfil dos Alunos à Saída da Escolaridade Obrigatória: Documento orientador do sistema educativo português que define as competências, valores e atitudes essenciais a desenvolver pelos alunos ao longo da escolaridade obrigatória.

PAA (Plano Anual de Atividades): Instrumento de planeamento/monitorização pedagógica; integra ações de cibersegurança.

PAM (Privileged Access Management): Soluções para cofre/controlo/auditoria de contas privilegiadas.

Política de segurança: Conjunto de princípios, normas e procedimentos que orientam a utilização segura dos recursos digitais, a proteção da informação e o cumprimento das obrigações legais.

Patching: Aplicação de atualizações de segurança a sistemas e aplicações.

Plano de Cibersegurança: Conjunto estruturado de medidas organizacionais, técnicas e pedagógicas destinadas a proteger sistemas, dados e utilizadores, assegurando a resiliência digital de uma instituição.

Pentest (Teste de intrusão): Avaliação prática de segurança através de simulações controladas de ataque.

Phishing: Técnica fraudulenta de engenharia social que utiliza mensagens enganosas (geralmente e-mails) para induzir o utilizador a revelar informações confidenciais ou aceder a sites falsos.

PII (Personally Identifiable Information): Informação pessoal identificável.

PIN (Personal Identification Number): Código numérico para autenticação em dispositivos/contas.

Plataformas digitais: Ambientes online utilizados para comunicação, ensino ou gestão de informação, que exigem práticas de segurança, autenticação e privacidade adequadas.

Playbook: Procedimento detalhado para resposta a incidentes específicos.

Privacy by design/by default: Princípios que exigem proteção de dados desde a conceção e por defeito.

Privacidade digital: Direito e prática de proteger a vida privada e os dados pessoais em ambientes digitais, garantindo a utilização ética e segura da informação.

Projeto Educativo (PE): Documento estruturante com visão e objetivos do AEPM.

Proteção de dados (RGPD): Princípios e regras do Regulamento (UE) 2016/679.

PRISMA 2020: Diretriz metodológica para revisões sistemáticas (*checklist* de 27 itens).

Quadro europeu de competências digitais (DigComp): Referencial europeu que define as competências necessárias para a cidadania digital ativa e segura, incluindo literacia informacional, comunicação, criação de conteúdo, segurança e resolução de problemas.

Quarantine / Reject (DMARC): Ações definidas por políticas DMARC para mensagens que falham autenticação (quarentena/recusa).

RACI (Responsible-Accountable-Consulted-Informed): Matriz que clarifica papéis e responsabilidades nas equipas, identificando quem executa, supervisiona, consulta e é informado em cada processo.

RBAC (Role-Based Access Control): Modelo de controlo de acesso baseado em funções atribuídas aos utilizadores, permitindo aplicar permissões de forma hierárquica e centralizada.

RCM n.º 127/2025: Resolução do Conselho de Ministros que aprova a Estratégia Nacional de Educação para a Cidadania e a Cibersegurança, definindo orientações para o setor educativo.

Referencial de Competências em Cibersegurança (CNCS): Documento publicado pelo Centro Nacional de Cibersegurança que define perfis e níveis de competência digital e cibersegurança aplicáveis a cidadãos, docentes e profissionais do setor público.

Regimento de utilização de telemóveis: Normas internas (DL n.º 95/2025) que regulam o uso de dispositivos móveis em contexto escolar, promovendo um ambiente digital seguro e pedagógico.

Resiliência digital (Digital resilience): Capacidade de uma organização ou sistema educativo para resistir, adaptar-se e recuperar rapidamente de incidentes de cibersegurança, garantindo a continuidade pedagógica e operacional.

RI (Regulamento Interno): Conjunto de regras de funcionamento, conduta e autoavaliação interna do Agrupamento de Escolas Passos Manuel (art.º 37.º–40.º).

Risco cibernético (Cyber risk): Probabilidade de ocorrência de ameaças digitais que comprometam a confidencialidade, integridade ou disponibilidade dos sistemas e dados do agrupamento.

RPO/RTO (Recovery Point Objective / Recovery Time Objective): Objetivos de ponto e tempo de recuperação definidos para restaurar dados e sistemas após um incidente, minimizando a perda de informação e o tempo de inatividade.

RGPD (Regulamento Geral sobre a Proteção de Dados): Regulamento (UE) 2016/679, que estabelece as regras para o tratamento de dados pessoais, incluindo os art.º 28.º (subencarregados) e 33.º–34.º (notificação de violações).

Ransomware: Tipo de *malware* que encripta dados e exige o pagamento de um resgate para permitir a sua recuperação, sendo uma das ameaças mais comuns em contextos educativos.

Root cause analysis (Análise de causa raiz): Processo de investigação que identifica as causas fundamentais de um incidente, permitindo propor medidas corretivas e prevenir recorrências.

SAFE (Segurança, Autonomia, Fiabilidade e Ética): Acrónimo que sintetiza os princípios orientadores do plano de cibersegurança do AEPM, promovendo um uso responsável, autónomo, fiável e ético da tecnologia.

Sandboxing: Execução de ficheiros ou links em ambiente isolado para observar o seu comportamento e identificar eventuais ações maliciosas, sem comprometer o sistema principal.

SELFIE (Self-reflection on Effective Learning by Fostering the use of Innovative Educational Technologies): Ferramenta europeia de autoavaliação da maturidade digital das escolas, que inclui o domínio "Segurança".

SeguraNet: Programa nacional de cidadania digital e segurança online, desenvolvido pela Direção-Geral da Educação em parceria com o Centro Nacional de Cibersegurança.

Security awareness (Sensibilização em segurança): Processo contínuo de formação e comunicação que visa promover comportamentos seguros, reduzir riscos humanos e criar uma cultura de cibersegurança na comunidade educativa.

Service account (Conta de serviço): Conta técnica utilizada por aplicações ou serviços automatizados; deve ter permissões mínimas e estar sujeita a controlo e auditoria reforçados.

Shadow IT: Utilização de aplicações, serviços ou dispositivos não autorizados pela instituição, que representam riscos de segurança, conformidade e privacidade.

SIEM (Security Information and Event Management): Plataforma que agrega e analisa registos de eventos de segurança para deteção (MTTD), resposta (MTTR) e auditoria.

SIGE (Sistema Integrado de Gestão Escolar): Plataforma de gestão administrativa e pedagógica utilizada pelo AEPM para centralizar dados escolares e operacionais.

Simulação de phishing: Ação formativa e de teste prático que avalia a capacidade dos utilizadores para reconhecer e evitar mensagens fraudulentas ou enganosas.

SLA (Service Level Agreement): Acordo de nível de serviço que define tempos máximos e responsabilidades (ex.: correção de vulnerabilidade crítica ≤ 7 dias).

Social engineering (Engenharia social): Técnica de manipulação psicológica usada por atacantes para induzir pessoas a divulgar informações confidenciais ou realizar ações que comprometam a segurança.

SPF (Sender Policy Framework): Registo DNS que identifica os servidores autorizados a enviar e-mails em nome de um domínio, prevenindo tentativas de *spoofing*.

SSO (Single Sign-On): Mecanismo de autenticação única que permite ao utilizador aceder a múltiplos serviços ou aplicações com uma única credencial.

Supply chain (Cadeia de fornecimento): Conjunto de entidades e processos envolvidos na criação, manutenção e distribuição de produtos ou serviços digitais, cuja segurança deve ser supervisionada.

Sustentabilidade digital: Utilização responsável, ética e eficiente das tecnologias digitais, garantindo equilíbrio entre inovação, segurança, inclusão e proteção ambiental.

Tabletop (Exercício de mesa): Simulação colaborativa que reproduz cenários de incidentes de segurança, permitindo testar e melhorar a resposta das equipas sem comprometer sistemas reais.

Tenant (Nuvem): Instância lógica dedicada dentro de uma plataforma *cloud* (ex.: Google Workspace, Microsoft 365), que isola os dados e configurações de cada organização.

TEIP (Territórios Educativos de Intervenção Prioritária): Programa de apoio a escolas situadas em contextos socioeconómicos vulneráveis; no plano do AEPM, enquadra-se no TEIP 4.

Threat intelligence (Inteligência de ameaças): Processo de recolha, análise e partilha de informação sobre ameaças, vulnerabilidades e atacantes, permitindo antecipar riscos e reforçar as defesas da organização.

Threat Landscape: Panorama de ameaças que descreve tendências, vetores e estatísticas de ciberataques a nível nacional e internacional.

TIA (Transfer Impact Assessment): Avaliação de impacto das transferências internacionais de dados pessoais, exigida pelo RGPD para garantir níveis adequados de proteção fora da UE.

TIC (Tecnologias de Informação e Comunicação): Conjunto de tecnologias utilizadas para aceder, criar, armazenar, gerir e partilhar informação em contexto educativo, administrativo e de segurança digital.

T0 / T+n: T0 representa o momento inicial de referência (baseline); T+n indica as metas temporais definidas para o acompanhamento (ex.: T+6, T+12).

TLS (Transport Layer Security): Protocolo criptográfico que assegura comunicações seguras pela internet, protegendo a confidencialidade e integridade dos dados transmitidos.

Token MFA (Authentication Token): Dispositivo físico ou aplicação que gera códigos temporários usados na autenticação multifator, reforçando a segurança dos acessos.

Tokenização: Processo de substituição de dados sensíveis por identificadores únicos (tokens), reduzindo o risco de exposição e facilitando a proteção de dados pessoais.

Transição digital: Processo de modernização tecnológica das organizações educativas, que visa integrar tecnologias digitais de forma estratégica, segura e inclusiva.

Transformação digital: Mudança profunda nos processos, cultura e práticas pedagógicas e organizacionais, impulsionada pela adoção de tecnologias digitais e pela inovação educativa.

Two-person rule (Regra das duas pessoas): Princípio de controlo que exige a validação ou autorização de duas pessoas para executar ações críticas, prevenindo erros, fraudes ou abusos.

Ubbu: Plataforma educativa de programação e pensamento computacional que promove a cidadania digital e o desenvolvimento de competências digitais nos alunos do 1.º ao 3.º ciclo do ensino básico.

UEBA (User and Entity Behavior Analytics): Sistema de análise comportamental que monitoriza padrões de atividade de utilizadores e entidades para detetar anomalias e comportamentos potencialmente maliciosos.

UPS (Uninterruptible Power Supply): Sistema de alimentação elétrica ininterrupta que assegura o funcionamento de equipamentos críticos durante falhas de energia, prevenindo perda de dados e danos de hardware.

URL Filtering (Filtragem de URLs): Mecanismo de segurança que controla o acesso a endereços ou websites específicos, bloqueando conteúdos maliciosos ou inadequados e protegendo os utilizadores contra ameaças online.

Utilizador privilegiado (Privileged user): Conta com permissões elevadas sobre sistemas ou dados sensíveis; deve ter autenticação multifator, registo de atividades e auditoria reforçada para evitar abusos ou falhas de segurança.

Vishing: Forma de *phishing* realizada através de chamadas telefónicas ou mensagens de voz fraudulentas, com o objetivo de obter informações pessoais ou credenciais de acesso.

VLAN (Virtual LAN): Segmentação lógica de rede que separa grupos de dispositivos e serviços, isolando tráfego e melhorando a segurança e a gestão da infraestrutura.

VPN (Virtual Private Network): Rede virtual encriptada que protege comunicações realizadas através da internet, garantindo confidencialidade e acesso seguro a sistemas internos.

Vulnerability scanning (Varredura de vulnerabilidades): Processo automatizado que identifica fraquezas de segurança em sistemas, aplicações e redes, permitindo a sua correção antes de serem exploradas.

Vulnerabilidade: Fraqueza explorável num ativo, sistema ou aplicação; deve ser gerida através de identificação (*scans*), avaliação (CVSS), correção (*patching*) e verificação periódica.

WCAG (Web Content Accessibility Guidelines): Diretrizes internacionais de acessibilidade digital que garantem que websites e conteúdos online possam ser utilizados por todos os utilizadores, incluindo pessoas com deficiência.

Wi-Fi: Tecnologia de rede local sem fios sujeita a padrões de segurança; utiliza protocolos como WPA2-Enterprise e WPA3 para autenticação segura.

Whitelisting / Blacklisting: Políticas de segurança que controlam o acesso a aplicações, endereços ou utilizadores, permitindo apenas os elementos incluídos em listas de confiança (*whitelist*) e bloqueando os restantes (*blacklist*).

Workflow: Sequência estruturada de tarefas e validações que define o fluxo de execução de um processo digital, permitindo automatizar procedimentos e melhorar a eficiência organizacional.

WORM (Write Once Read Many): Tecnologia que permite gravar dados apenas uma vez, impedindo alterações ou eliminações posteriores; usada em cópias de segurança imutáveis.

WPA2-Enterprise / WPA3: Padrões de segurança para redes Wi-Fi; o modo *Enterprise* utiliza autenticação 802.1X/EAP para proteger acessos e credenciais.

XML Security (XML Signature/Encryption): Conjunto de especificações que assegura a assinatura e encriptação de documentos XML, utilizadas em mecanismos de gestão de direitos digitais (DRM).

Zero Trust: Modelo de segurança que assume confiança zero por defeito; exige verificação contínua e menor privilégio.

Apêndice A – Fichas-resumo de website e relatórios institucionais

Documentos e recursos oficiais incluídos na fase de revisão da literatura (PRISMA 2020) como fontes de literatura cinzenta. Cada ficha apresenta a informação essencial de rastreabilidade e justificativa de inclusão.

1. CNCS — Centro Nacional de Cibersegurança

Título: Guia de Transição Digital

Entidade responsável: CNCS

Ano: 2024

URL: https://www.cncs.gov.pt/pt/guia-de-transicao-digital/

Data de acesso: 15/09/2025

Motivo de inclusão: Documento orientador nacional para a transição digital segura em instituições públicas e educativas.

Nível de evidência: Elevado

1. CNCS — Centro Nacional de Cibersegurança

Título: Referencial de Competências em Cibersegurança

Entidade responsável: CNCS

Ano: 2024

URL: https://www.cncs.gov.pt/pt/referencial-de-competencias/

Data de acesso: 15/09/2025

Motivo de inclusão: Recurso oficial para identificação de perfis e competências digitais aplicáveis a contextos escolares.

Nível de evidência: Elevado

2. CNCS & FPCEUP

Título: Educação para a Cibersegurança no Ensino Básico e Secundário em Portugal

Entidade responsável: CNCS e FPCEUP

Ano: 2024

URL: https://www.cncs.gov.pt/pt/educacao-para-a-ciberseguranca/

Data de acesso: 15/09/2025

Motivo de inclusão: Estudo nacional de referência sobre o estado da educação para a cibersegurança em escolas portuguesas.

Nível de evidência: Elevado

3. DGE/ERTE

Título: *ERTE em Números #2*

Entidade responsável: Direção-Geral da Educação (DGE)

Ano: 2023

URL: https://erte.dge.mec.pt/erte-em-numeros-2

Data de acesso: 15/09/2025

Motivo de inclusão: Fonte estatística nacional sobre maturidade digital e práticas tecnológicas nas escolas.

Nível de evidência: Elevado

4. DGE

Título: *PADDE 2021–2023 – Plano de Ação para o Desenvolvimento Digital das Escolas*

Entidade responsável: Direção-Geral da Educação (DGE)

Ano: 2023

URL: https://erte.dge.mec.pt/padde

Data de acesso: 15/09/2025

Motivo de inclusão: Documento estratégico interno de referência no diagnóstico digital do AE Passos Manuel.

Nível de evidência: Elevado

5. AEPM

Título: Projeto Educativo 2023–2026

Entidade responsável: Agrupamento de Escolas Passos Manuel

Ano: 2023

URL: [documento interno]

Data de acesso: 15/09/2025

Motivo de inclusão: Documento estruturante do agrupamento que enquadra a proposta do plano de cibersegurança.

Nível de evidência: Elevado

6. AEPM

Título: Regulamento Interno 2024

Entidade responsável: AEPM

Ano: 2024

URL: [documento interno]

Data de acesso: 15/09/2025

Motivo de inclusão: Define práticas institucionais relacionadas com segurança e proteção de dados.

Nível de evidência: Elevado

7. AEPM

Título: Estratégia de Educação para a Cidadania na Escola (EECE)

Entidade responsável: AEPM

Ano: 2023

URL: [documento interno]

Data de acesso: 15/09/2025

Motivo de inclusão: Documento articulador entre literacia digital, cidadania e ética online.

Nível de evidência: Elevado

8. ENISA

Título: *Cybersecurity Education Maturity Framework*

Entidade responsável: European Union Agency for Cybersecurity (ENISA)

Ano: 2024

URL: https://www.enisa.europa.eu/topics/education/cybersecurity-education-maturity

Data de acesso: 15/09/2025

Motivo de inclusão: Quadro europeu de referência para avaliação da maturidade cibernética na educação.

Nível de evidência: Elevado

9. ENISA

Título: *ENISA Threat Landscape 2024*

Entidade responsável: ENISA

Ano: 2024

URL: https://www.enisa.europa.eu/topics/threat-landscape

Data de acesso: 15/09/2025

Motivo de inclusão: Relatório técnico europeu sobre tendências e vetores de ataque, utilizado para contextualizar riscos educativos.

Nível de evidência: Elevado

10. European Commission

Título: *Orientações para professores e educadores sobre o combate à desinformação e a promoção da literacia digital*

Entidade responsável: Comissão Europeia

Ano: 2022

URL: https://data.europa.eu/doi/10.2766/283100

Data de acesso: 15/09/2025

Motivo de inclusão: Diretriz oficial europeia sobre educação mediática e literacia digital crítica.

Nível de evidência: Elevado

11. DfE – Department for Education (UK)

Título: *Cybersecurity Standards for Schools and Colleges*

Entidade responsável: Department for Education (Reino Unido)

Ano: 2025

URL: https://www.gov.uk/government/publications/cyber-security-standards-for-schools-and-colleges

Data de acesso: 15/09/2025

Motivo de inclusão: Exemplo internacional de boas práticas normativas para cibersegurança em escolas.

Nível de evidência: Elevado

12. EurofamNet

Título: *Digital Parenting*

Entidade responsável: EurofamNet – COST Action CA18123

Ano: 2023

URL: https://eurofamnet.eu/outputs/digital-parenting

Data de acesso: 15/09/2025

Motivo de inclusão: Documento de referência sobre parentalidade digital e envolvimento familiar na literacia digital.

Nível de evidência: Médio

13. Portugal Digital

Título: *Portugal Digital Academy*

Entidade responsável: Estrutura de Missão Portugal Digital

Ano: 2024

URL: https://portugaldigital.gov.pt/academia-digital

Data de acesso: 15/09/2025

Motivo de inclusão: Programa nacional de capacitação digital de adultos, com aplicabilidade em contextos escolares.

Nível de evidência: Médio

14. E-REDES / DGE

Título: *Digital Academy for Parents*

Entidade responsável: E-REDES e Direção-Geral da Educação (DGE)

Ano: 2024

URL: https://www.dge.mec.pt/digital-academy-parents

Data de acesso: 15/09/2025

Motivo de inclusão: Programa português de literacia parental em cibersegurança e competências digitais.

Nível de evidência: Médio

15. European Commission

Título: *Uma Europa preparada para a era digital*

Entidade responsável: Comissão Europeia

Ano: 2024

URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt

Data de acesso: 15/09/2025

Motivo de inclusão: Documento político europeu que enquadra a transição digital e a importância estratégica da cibersegurança e literacia digital.

Nível de evidência: Contextual (nível descritivo)

Fonte: elaboração própria a partir da revisão documental (2025).

Apêndice B – Diagrama de fluxo PRISMA 2020

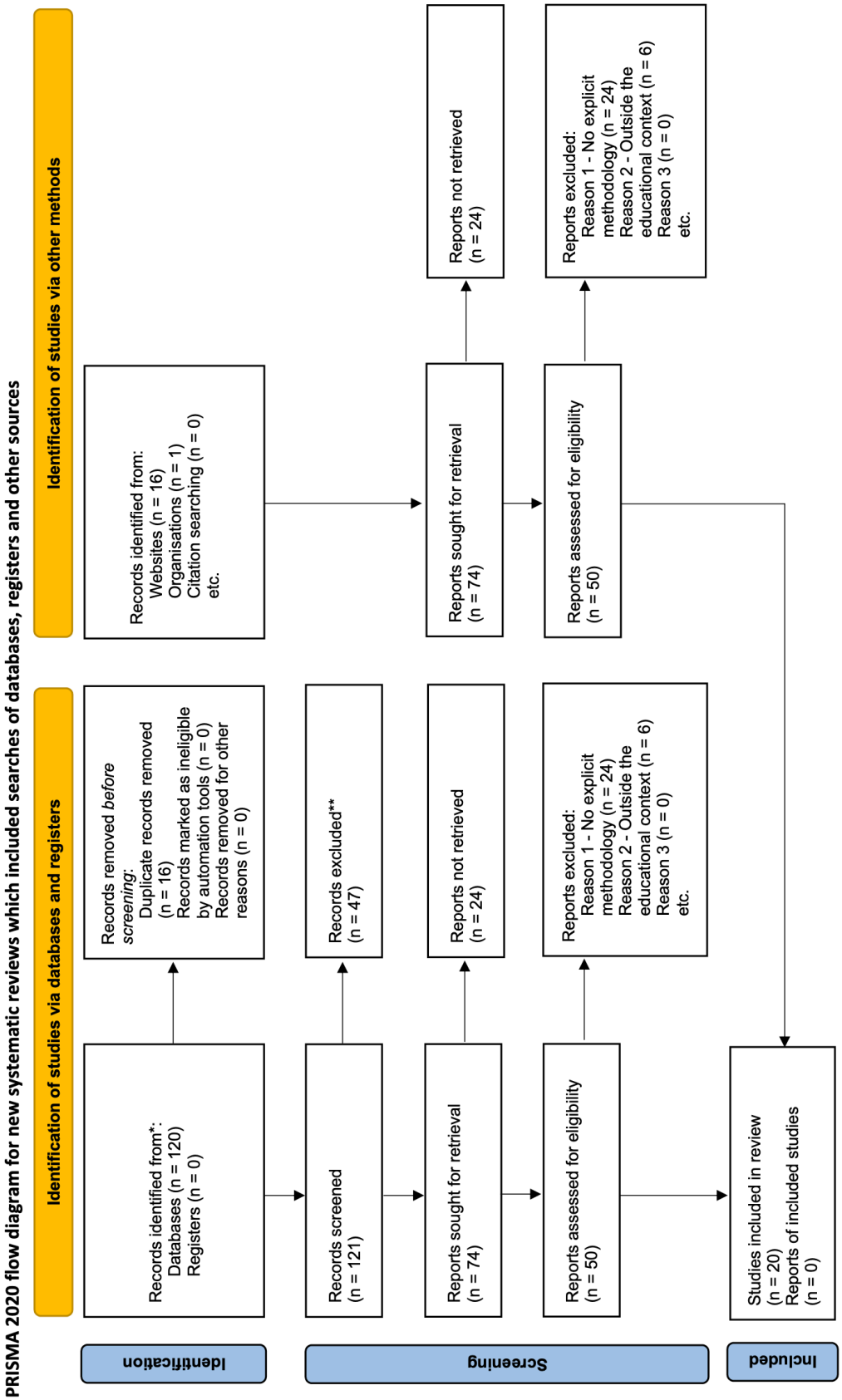
(PRISMA 2020 Flow Diagram)

O diagrama apresentado neste anexo corresponde à versão oficial do modelo PRISMA 2020, traduzida e publicada por Page et al. (2021). Este modelo representa graficamente o processo de identificação, triagem, elegibilidade e inclusão dos estudos considerados na revisão sistemática realizada no presente trabalho.

O diagrama foi integrado sem quaisquer alterações, servindo exclusivamente para reforçar a transparência metodológica e a rastreabilidade do processo de revisão.

Fonte: PRISMA (2021). *PRISMA 2020 flow diagram*. Disponível em: https://www.prisma-statement.org/prisma-2020-flow-diagram

(Segue imagem do documento original na página seguinte.)



Source: Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71.

Apêndice C – PRISMA 2020 – Lista de verificação para o resumo

(PRISMA 2020 Abstract Checklist – Versão Portuguesa)

O documento apresentado neste anexo corresponde à versão portuguesa oficial da *PRISMA 2020 Abstract Checklist*, traduzida e adaptada por Sousa, Gonçalves-Lopes, Abreu e Oliveira (2024). É incluído integralmente e sem modificações, com o objetivo de assegurar transparência e conformidade metodológica na aplicação da metodologia PRISMA neste estudo.

Fonte: Sousa, J. L., Gonçalves-Lopes, S., Abreu, V., & Oliveira, V. (2024). *Declaração PRISMA 2020: uma diretriz atualizada para publicação de revisões sistemáticas*. *Germinare, 4*, 1–19. https://doi.org/10.5281/zenodo.13271469

(Segue a imagem do documento original na página seguinte.)

PRISMA 2020 Lista de verificação para o Resumo

Secção ou Tópico	Item #	Item da lista de verificação	Mencionado (Sim/Não)
TÍTULO			
Título	1	Revisão sistemática da literatura sobre cibersegurança em contexto educativo no AE Passos Manuel – PRISMA 2020	Sim
BACKGROUND			
Objetivos	2	Avaliar práticas, lacunas e normativos de cibersegurança em instituições de ensino básicas e secundárias, com enfoque no contexto português e aplicação ao AEPM.	Sim
MÉTODOS			
Critérios de elegibilidade	3	Estudos entre 2015–2025 sobre cibersegurança em contexto educativo, publicados em português, inglês ou espanhol; incluídos estudos empíricos, revisões sistemáticas e relatórios institucionais; excluídos artigos sem metodologia explícita, fora do contexto educativo ou duplicados.	Sim
Fontes de informação	4	Estudos publicados 2015–2025 sobre cibersegurança em contexto educativo; exclusão de artigos sem metodologia explícita e fora do contexto educativo. Bases de dados: Scopus, IEEE Xplore, ERIC, MDPI, SpringerLink, Google Scholar e ResearchGate. Websites institucionais: CNCS, ENISA, DGE, OWASP, SANS, Comissão Europeia.	Sim
Risco de viés	5	A qualidade metodológica foi avaliada segundo os princípios CASP e do *Joanna Briggs Institute* (rigor, relevância e transferibilidade), assegurando a fiabilidade dos estudos incluídos e a mitigação do risco de viés através da triangulação de fontes e da aplicação consistente dos critérios de inclusão e exclusão definidos na metodologia PRISMA 2020.	Sim
Síntese dos resultados	6	A síntese foi qualitativa e temática, com triangulação entre evidência científica, normativa e institucional.	Sim
RESULTADOS			
Estudos incluídos	7	20 estudos incluídos: principais temas — gestão de identidades, formação docente, segurança de redes, *endpoint management*, políticas de *backup* e resposta a incidentes.	Sim
Síntese dos resultados	8	Registos identificados**:** 137 (120 bases de dados + 16 websites + 1 organização); duplicados: 16; triagem: 121; excluídos: 47; elegíveis: 74; artigos lidos integralmente: 50; excluídos por não conformidade: 30 (24 sem metodologia, 6 fora do contexto); incluídos: 20 (estudos que cumpriram todos os critérios de inclusão e integraram a revisão sistemática).	Sim
DISCUSSÃO			
Limitações da evidência	9	A revisão evidencia fragilidades na formação em cibersegurança nas escolas e na consolidação de práticas normativas, justificando a proposta de um plano institucional integrado, em conformidade com o RGPD, a Diretiva NIS 2 e a norma ISO/IEC 27001.	Sim
Interpretação	10	Os resultados sustentam a necessidade de estratégias formativas e técnicas integradas, orientadas por referenciais europeus (CNCS, ENISA, DigCompEdu, SELFIE), para reforçar a cultura de segurança digital nas escolas públicas.	Sim
OUTROS			
Financiamento	11	Sem financiamento externo.	Sim
Registo	12	Não aplicável (revisão sistemática académica não registada)	Sim

Traduzido por: Verónica Abreu, Sónia Gonçalves-Lopes*, José Luís Sousa* e Verónica Oliveira / *ESS Jean Piaget - Vila Nova de Gaia - Portugal*
A partir de: Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

Apêndice D – Tabela-resumo de normas, modelos e documentos de referência

Os documentos e normas apresentados nesta tabela constituem a base normativa, metodológica e estratégica que fundamenta o Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel (AEPM). Incluem referenciais europeus, normas técnicas internacionais, modelos de competências e documentos institucionais.

Apêndice D – Tabela-resumo de normas, modelos e documentos de referência

Categoria	Documento / Norma / Modelo	Entidade / Ano	Finalidade no estudo	Observações
Normas e legislação europeia	Regulamento Geral sobre a Proteção de Dados (RGPD – UE 2016/679)	União Europeia, 2016	Define princípios e obrigações para o tratamento e proteção de dados pessoais no contexto escolar.	Norma jurídica obrigatória.
Normas e legislação europeia	Diretiva NIS 2 (UE 2022/2555)	União Europeia, 2022	Estabelece requisitos mínimos de cibersegurança para entidades públicas e privadas, incluindo escolas.	Diretiva europeia em vigor.
Normas e legislação europeia	*Digital Services Act* (UE 2022/2065)	União Europeia, 2022	Reforça a segurança e responsabilidade digital das plataformas e serviços online.	Complementar ao RGPD.
Normas técnicas internacionais	ISO/IEC 27001:2022 – Sistemas de Gestão da Segurança da Informação	ISO/IEC, 2022	Define requisitos para estabelecer, implementar e melhorar sistemas de gestão da segurança da informação.	Norma certificável.
Normas técnicas internacionais	ISO/IEC 27002:2022 – Controlo e Gestão de Medidas de Segurança	ISO/IEC, 2022	Apresenta boas práticas para implementação de controlos técnicos e organizacionais.	Complementa a ISO/IEC 27001.
Modelos e referenciais de competências	*DigCompEdu* – Quadro Europeu de Competências Digitais dos Educadores	Comissão Europeia, 2017–2022	Fornece estrutura de desenvolvimento das competências digitais dos docentes.	Usado como base de capacitação no plano.
Modelos e referenciais de competências	*SELFIE* – Ferramenta de Autoavaliação Digital das Escolas	Comissão Europeia, 2020	Apoia escolas na avaliação da maturidade digital e planeamento estratégico.	Aplicável ao diagnóstico institucional.

Modelos e referenciais de competências	*ENISA Maturity Framework*	ENISA, 2024	Estabelece níveis de maturidade em cibersegurança no setor público e educativo.	Referência europeia de diagnóstico.
Modelos e referenciais de competências	CNCS – Referencial de Competências em Cibersegurança	CNCS, 2024	Define perfis de competência e áreas de formação em cibersegurança aplicáveis a diferentes contextos educativos.	Referencial nacional.
Modelos e referenciais de competências	*Cybersecurity Education Maturity Assessment*	ENISA, 2024	Instrumento de avaliação de maturidade da educação em cibersegurança.	Complementar ao ENISA Maturity Framework.
Guias, estratégias e programas institucionais	CNCS – Guia de Transição Digital	CNCS, 2024	Apresenta recomendações para uma transição digital segura e sustentável em instituições públicas.	Base estratégica nacional.
Guias, estratégias e programas institucionais	DGE – Plano de Ação para o Desenvolvimento Digital das Escolas (PADDE)	DGE, 2023	Orienta a transformação digital das escolas portuguesas, incluindo medidas de segurança e capacitação.	Documento de referência nacional.
Guias, estratégias e programas institucionais	AEPM – Projeto Educativo 2023–2026	AE Passos Manuel, 2023	Define a missão, valores e objetivos pedagógicos do agrupamento, integrando a dimensão digital e cidadania.	Documento estruturante interno.
Guias, estratégias e programas institucionais	AEPM – Regulamento Interno 2024	AE Passos Manuel, 2024	Estabelece normas de funcionamento e regras de proteção de dados e segurança digital.	Base normativa interna.
Guias, estratégias e programas institucionais	AEPM – Estratégia de Educação para a Cidadania na Escola (EECE)	AE Passos Manuel, 2023	Promove a cidadania digital, ética e responsabilidade no uso das tecnologias.	Documento de articulação curricular.
Guias, estratégias e programas institucionais	ENISA – *Threat Landscape* 2024	ENISA, 2024	Analisa as principais ameaças e tendências de ciberataques a nível europeu.	Fonte de contextualização técnica.
Guias, estratégias e programas institucionais	DfE (UK) – *Cybersecurity Standards for Schools and Colleges*	*Department for Education* (UK), 2025	Apresenta boas práticas internacionais para gestão e proteção de dados em escolas.	Exemplo internacional de referência.
Guias, estratégias e programas institucionais	*Cyber Security Strategy* 2025–2028	Universidade Internacional, 2025	Exemplo de planeamento estratégico institucional em cibersegurança.	Documento comparativo para o plano AEPM.

Guias, estratégias e programas institucionais	*Digital Academy for Parents* – E-REDES/DGE	E-REDES/DGE, 2024	Promove a literacia parental em segurança e competências digitais.	Programa de envolvimento comunitário.
Guias, estratégias e programas institucionais	Declaração PRISMA 2020	Sousa et al., 2024	Diretriz metodológica utilizada para a revisão sistemática da literatura.	Base metodológica.
Guias, estratégias e programas institucionais	CASP / *Joanna Briggs* (adaptado)	*Joanna Briggs Institute*, 2024	Conjunto de critérios para avaliação da qualidade metodológica dos estudos incluídos.	Aplicado na fase de triagem.

Apêndice E – Formulário de Diagnóstico de Cibersegurança

(Agrupamento de Escolas Passos Manuel)

O documento apresentado neste anexo corresponde ao Formulário de Diagnóstico de Cibersegurança, desenvolvido pela autora no âmbito da presente investigação. O instrumento teve como finalidade recolher informação sobre a infraestrutura tecnológica, as práticas pedagógicas digitais e as medidas de segurança implementadas no Agrupamento de Escolas Passos Manuel, no ano letivo de 2024/2025.

O formulário foi disponibilizado em formato eletrónico através da plataforma *Google Forms* e foi respondido pela Direção do Agrupamento, representando a perspetiva institucional sobre a maturidade digital e a gestão da cibersegurança. O processo de recolha de dados manteve carácter anónimo e confidencial, cumprindo as disposições do Regulamento (UE) 2016/679 (RGPD) e da Lei n.º 58/2019. As respostas obtidas serviram exclusivamente para fins académicos e de diagnóstico, constituindo a base empírica para a elaboração do Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel.

Fonte: Formulário elaborado por Andreia Patrícia Semedo Motaco (2025), no âmbito do *Mestrado em Transformação Digital no Ensino e da Aprendizagem* — ISCTE-IUL.

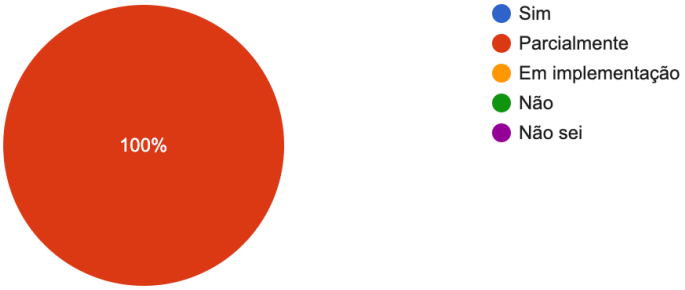
(Seguem as imagens do documento original nas páginas seguintes.)

1. Infraestrutura de Rede e Proteção

1.1. O Agrupamento de Escolas Passos Manuel dispõe de rede Wi-Fi em todos os espaços letivos?

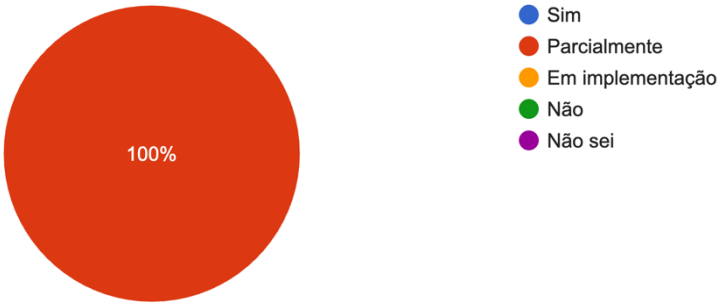
Copiar gráfico

1 resposta



1.2. A rede está segmentada por perfis de utilizador (ex.: docentes, alunos, visitantes)?

1 resposta



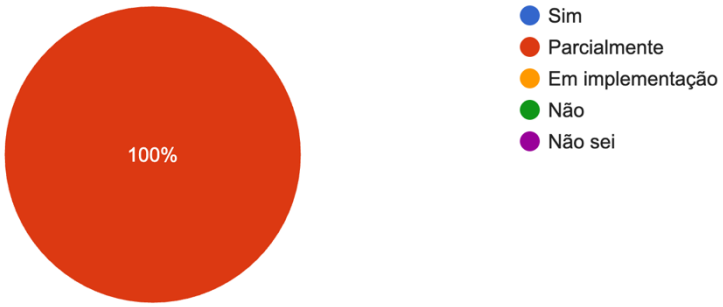
1.3.Utilizam firewall ou outra barreira de proteção na ligação à internet?

1 resposta

N

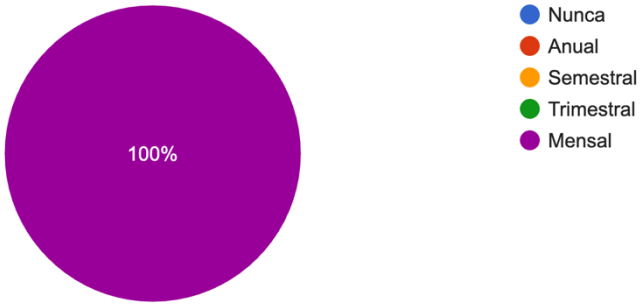
1.4. Há sistemas de deteção de acessos suspeitos (ex.: IDS/IPS, sistemas de monitorização de tráfego)?

1 resposta



1.5. Com que frequência fazem atualização de firmware e regras de segurança nos equipamentos de rede?

1 resposta



2. **Equipamentos e Sistemas**

2.1. Quantos equipamentos digitais (computadores, portáteis e tablets) estão atualmente em uso no Agrupamento de Escolas Passos Manuel (ano letivo 2024/2025)?

Por favor, indique o número aproximado por categoria de utilizador:

Docentes:

Alunos:

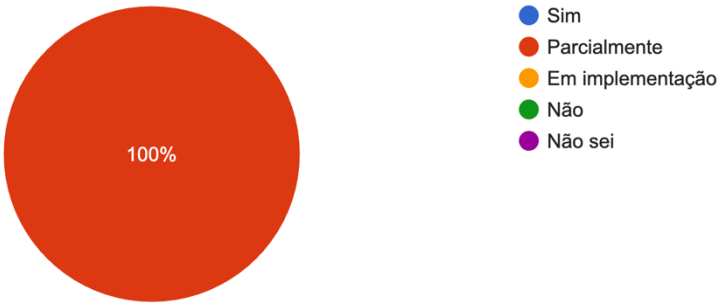
Serviços administrativos:

1 resposta

Docentes: 200; Alunos: 300; SAE: 20

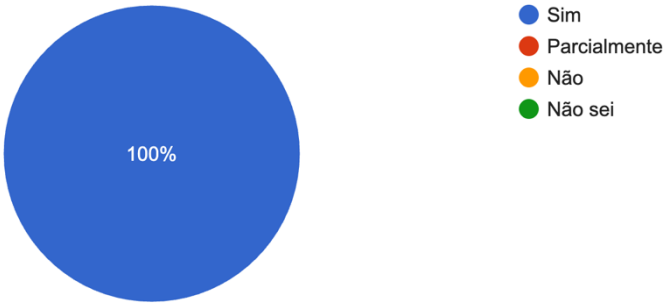
2.2. Todos os computadores têm antivírus/anti-malware instalado e atualizado?

1 resposta



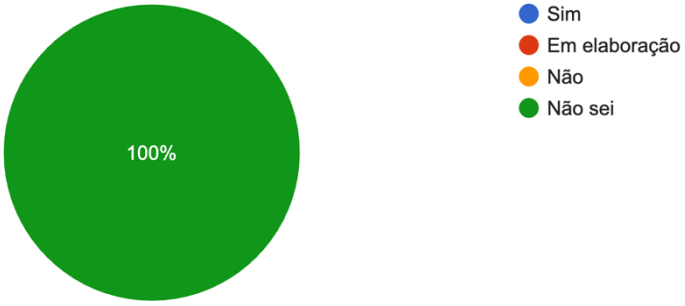
2.3. Realizam backups regulares dos dados críticos (em servidor local, NAS ou cloud)?

1 resposta



2.4. Existe inventário centralizado dos equipamentos ligados à rede (hardware e software)?

1 resposta

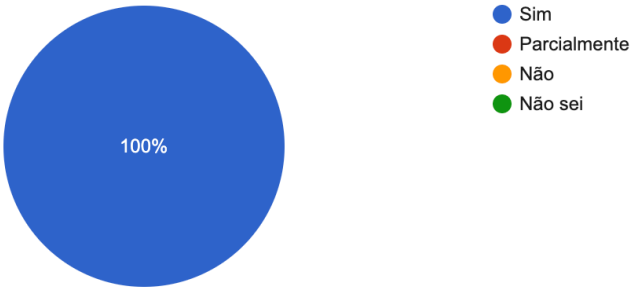


3. Políticas, Procedimentos e Conformidade

3.1. O Agrupamento possui política formal de segurança informática ou proteção de dados (por exemplo, documento próprio ou integrando-se no PADDE)?

Copiar gráfico

1 resposta



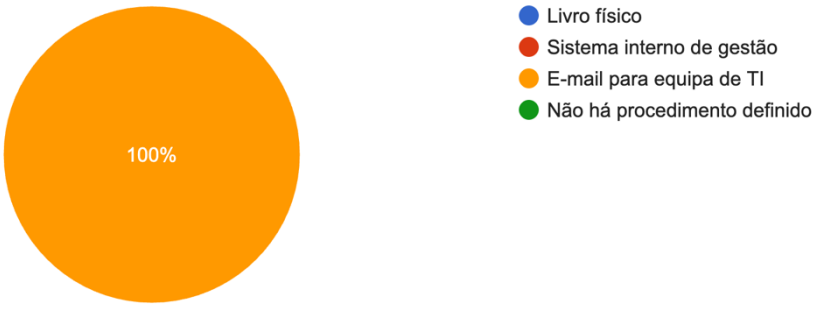
3.2. Se sim, indique nome e data da última revisão.

1 resposta

Janeiro 2024

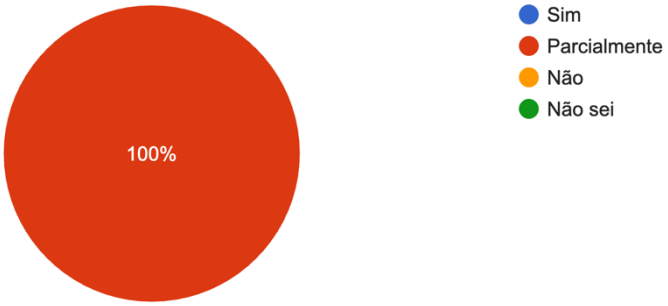
3.3. Como são reportados e registados os incidentes de segurança (ex.: phishing, ransomware, falha de serviço)?

1 resposta



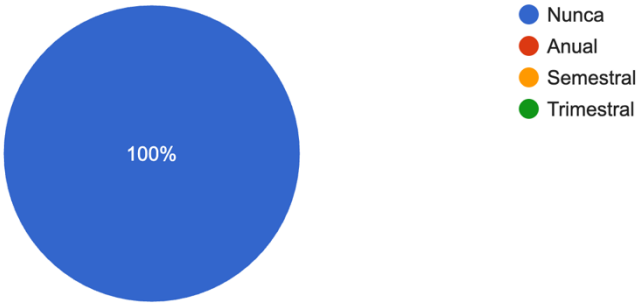
3.4. O Agrupamento cumpre requisitos do RGPD e da Diretiva NIS 2 no tratamento de dados pessoais e infraestruturas críticas?

1 resposta



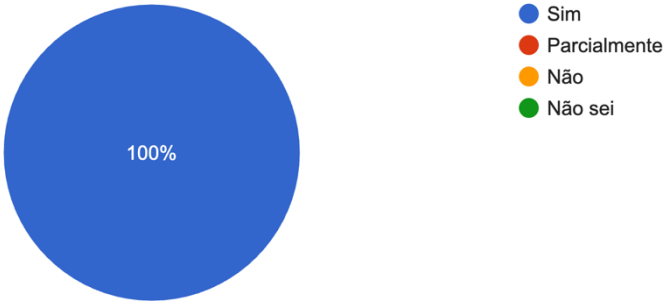
3.5. Com que frequência realizam auditorias ou revisões de conformidade (internas ou por entidade externa)?

1 resposta



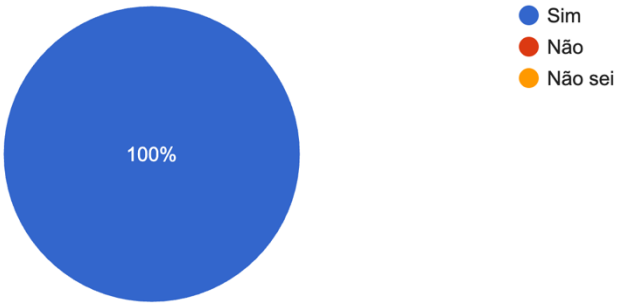
3.6. Existem perfis diferenciados de acesso para administrativos, docentes e alunos?

1 resposta



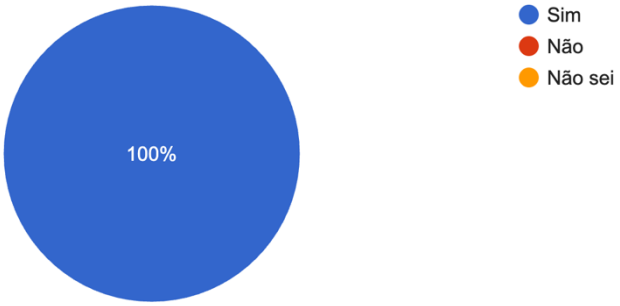
3.7. Já foi reportado algum incidente de segurança digital nos últimos 2 anos?

1 resposta



3.8. Há regras internas sobre a criação e manutenção de passwords?

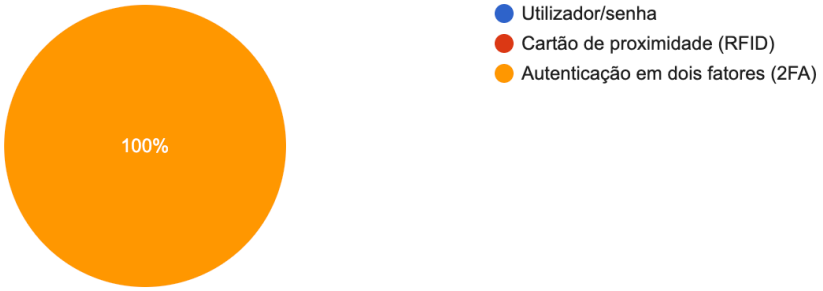
1 resposta



4. Práticas Digitais e Rotinas de Segurança

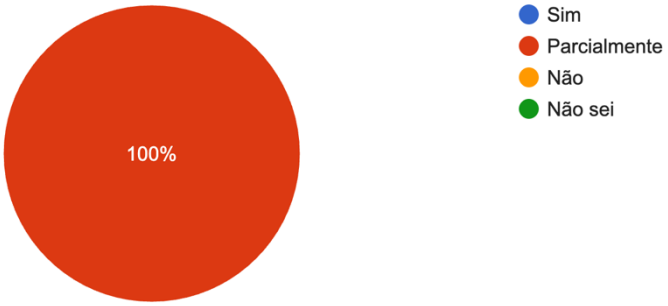
4.1. Que métodos de autenticação estão em uso nos sistemas centrais? Copiar gráfico

1 resposta



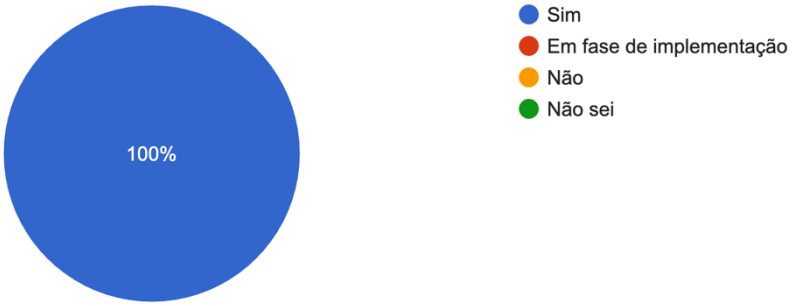
4.2. Há regras internas para criação e renovação de passwords (ex.: comprimento mínimo, complexidade, troca periódica)?

1 resposta



4.3. As salas de aula e laboratórios têm perfis de acesso diferenciados (ex.: desbloqueio de aplicações, restrições de sites)?

1 resposta



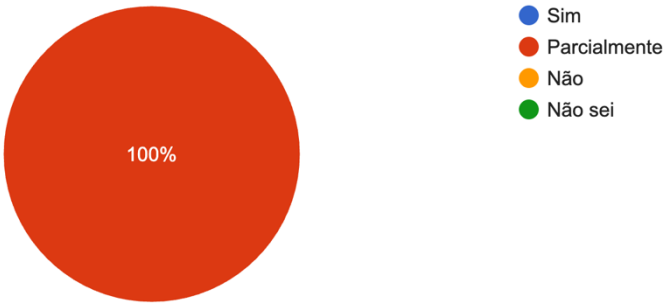
4.4. São disponibilizadas listas de verificação de segurança (checklists) a professores e funcionários?

1 resposta

T

4.5. O PADDE do Agrupamento contempla medidas específicas de segurança digital?

1 resposta



4.6. Existem orientações escritas sobre o uso das plataformas digitais (Classroom, email institucional...)?

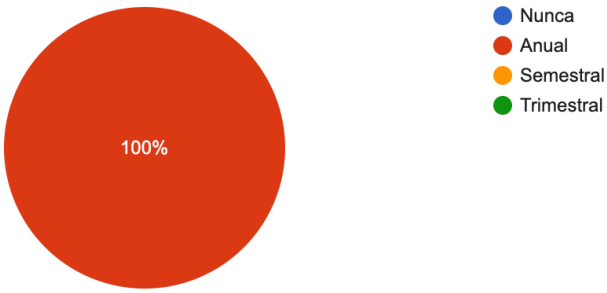
1 resposta

5. Formação e Sensibilização

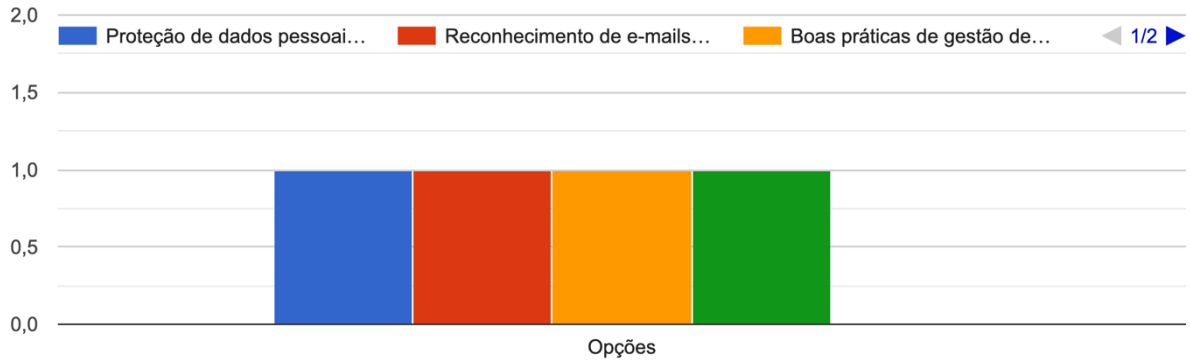
5.1. Com que frequência o pessoal docente e não docente recebe formação ou workshops sobre cibersegurança?

Copiar gráfico

1 resposta

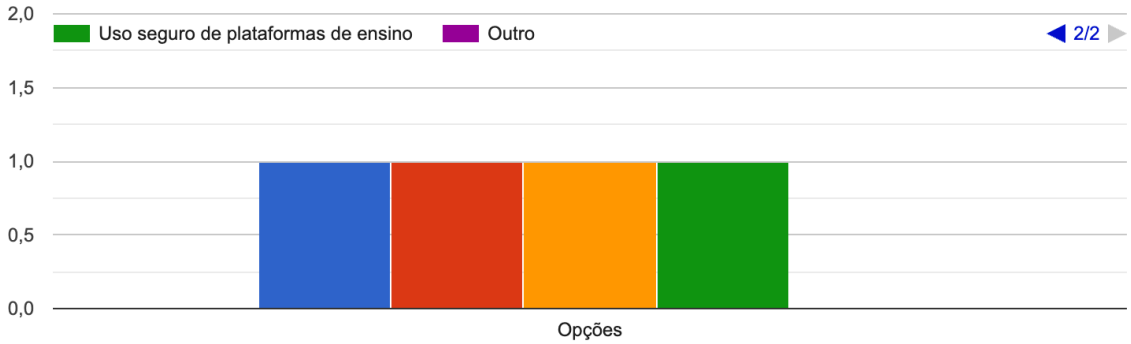


5.2. Que tópicos já foram abordados em formação ou workshops sobre cibersegurança (assinale os que aplicam):



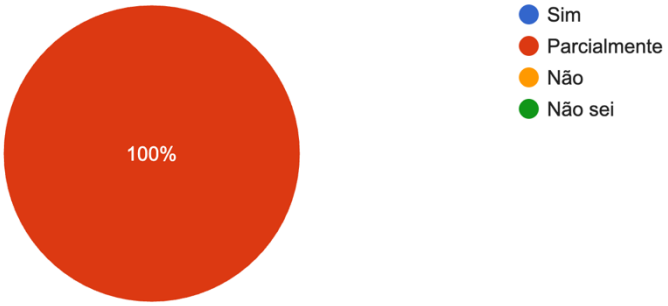
5.2. Que tópicos já foram abordados em formação ou workshops sobre cibersegurança (assinale os que aplicam):

Copiar gráfico



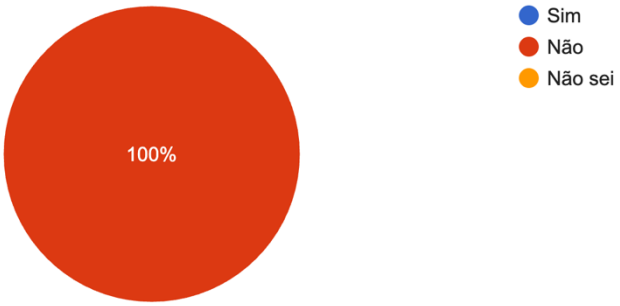
5.3. Utilizam recursos externos (por exemplo, CNCS, DGE, Portugal Digital) em ações de sensibilização?

1 resposta



5.4. Existem campanhas internas ou ações de sensibilização sobre cibersegurança?

1 resposta



5.5. Em que área sente maior necessidade de formação futura?

1 resposta

Segurança Digital e Gestão de Aplicações

6. Cultura, Riscos e Sugestões

6.1. Que boas práticas de segurança digital já existem na escola/agrupamento?

1 resposta

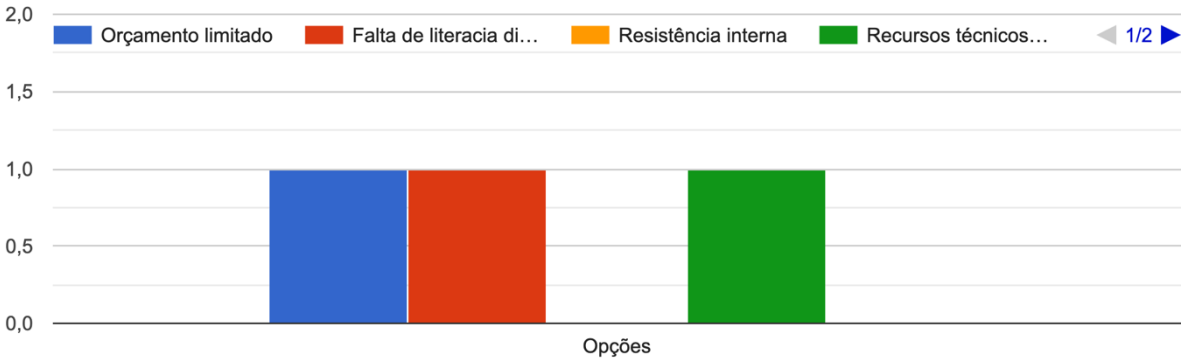
Gestão personalizada no acesso a sistemas criticos

6.2. Quais, na sua opinião, são as três principais ameaças atuais ao Agrupamento?

1 resposta

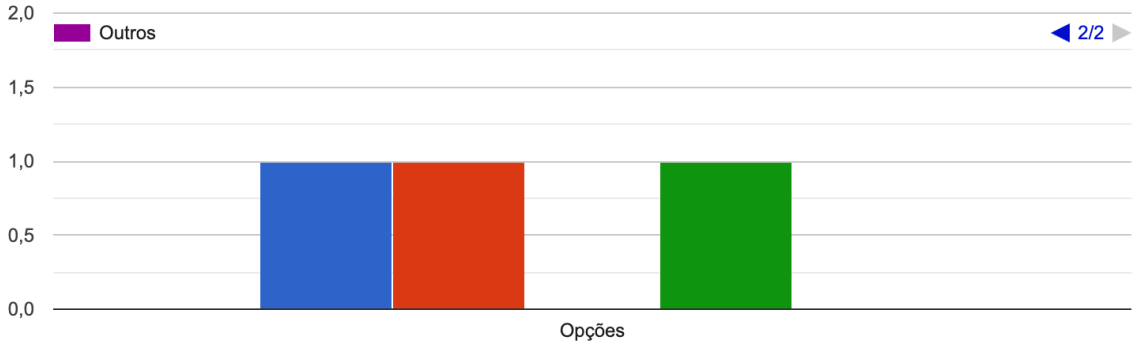
Proliferação de aplicações, gestão de informação pessoal cedida de forma inconsequente pelos utilizadores e confidencialidade na gestão da informação

6.3. Que obstáculos dificultam hoje a implementação de medidas de segurança?

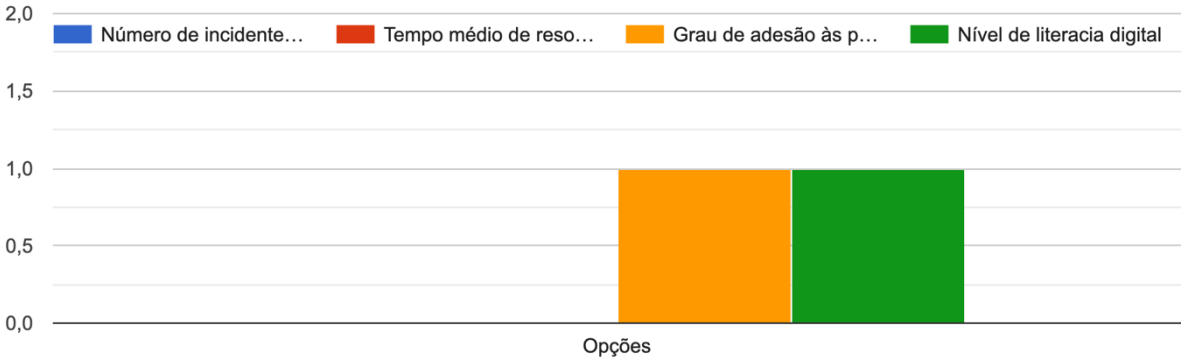


6.3. Que obstáculos dificultam hoje a implementação de medidas de segurança?

Copiar gráfico



6.4. Que indicadores gostava de usar para avaliar o sucesso do plano de cibersegurança?



X

6.5. Que riscos, fragilidades ou necessidades urgentes identifica nesta área?

1 resposta

Proliferação de aplicações de educação com fins pouco claros;
Gestão, partilha de informação e sua disponibilização;
Assegurar uma boa utilização da informação disponibilizada e garantir a confidencialidade da informação

6.6. Deseja acrescentar alguma informação ou comentário relevante sobre a realidade digital do agrupamento?

1 resposta

A enorme proliferação de aplicação e a gestão de recursos digitais (software e hardware) que possuem uma complexidade técnica elevada, tendo em conta os custos financeiros e de horas que a manutenção, gestão e atualização constantes requerem.

Muito obrigada pela sua colaboração!

Apêndice F – Plano de implementação com normas/controles

Associação das quatro fases do plano de cibersegurança do AEPM aos principais referenciais normativos e orientadores, incluindo a ISO/IEC 27002:2022, o Regulamento Geral sobre a Proteção de Dados (RGPD), a Diretiva NIS 2, a Resolução do Conselho de Ministros n.º 127/2025, o Referencial de Competências em Cibersegurança do CNCS, a Estratégia de Educação para a Cidadania na Escola (EECE) e o Regulamento Interno (RI).

Apêndice F – Plano de implementação com normas/Controles (versão expandida)

Fase	Normas e referenciais aplicáveis	Artigos / Controlos	Âmbito de aplicação no plano (Quadro 4.4-B)
Fase I - Preparação e Gestão	ISO/IEC 27002:2022Regulamento Geral sobre a Proteção de Dados (RGPD)Diretiva NIS 2 (UE, 2022)	ISO 27002: sec. 5.1, 5.2RGPD: art.º 24.º, 25.ºNIS 2: art.º 21.º	Definição de políticas, papéis e responsabilidades; constituição do Comité de Cibersegurança; gestão de risco e de ativos críticos.
Fase II - Infraestruturas e Proteção Técnica	ISO/IEC 27002:2022RGPDNIS 2 (UE, 2022)	ISO 27002: sec. 8.2, 8.7, 8.13, 8.16RGPD: art.º 32.ºNIS 2: art.º 15.º–19.º	Medidas técnicas de segurança — *MFA*, gestão de *endpoints*, encriptação, *backups 3-2-1*, *logging* centralizado, gestão de vulnerabilidades.
Fase III - Capacitação e Cultura Digital Segura	Resolução do Conselho de Ministros n.º 127/2025Centro Nacional de Cibersegurança (CNCS, 2022) Estratégia de Educação para a Cidadania na Escola (EECE, 2023/24) *Digital Services Act* (DSA, UE, 2022)	CNCS: Referencial de Competências, eixos 2 e 3EECE: domínios "Literacia Digital" e "Cidadania" DSA: art.º 32.º	Formação contínua de docentes e não docentes; integração da cibersegurança no currículo; promoção de cultura digital segura e participação cidadã.
Fase IV - Avaliação, Melhoria Contínua e Sustentabilidade	ISO/IEC 27002:2022NIS 2 (UE, 2022) Regulamento Interno (AEPM, 2024)	ISO 27002: sec. 10.1NIS 2: art.º 22.ºRegulamento Interno: art.º 37.º–40.º	Monitorização e auditoria interna; avaliação de indicadores (KPIs); processos de melhoria contínua e autoavaliação institucional.

Nota. Os controlos e artigos foram selecionados com base na correspondência direta entre as medidas operacionais do Quadro 5.4 – Plano de Implementação do AEPM e as obrigações normativas dos referenciais indicados.

Apêndice G – Estratégias de formação e sensibilização no AEPM (versão expandida), com calendarização anual, responsáveis institucionais e indicadores de impacto

Para efeitos de operacionalização prática e acompanhamento sistemático, apresenta-se no Quadro G, uma versão expandida das estratégias de formação e sensibilização previstas no Plano de Cibersegurança do Agrupamento de Escolas Passos Manuel (AEPM). Este quadro detalha, para cada público-alvo, as estratégias e metodologias a adotar, a calendarização anual, os responsáveis institucionais e os indicadores de impacto, permitindo enquadrar cada ação num plano operativo plenamente alinhado com os referenciais normativos e pedagógicos em vigor.

Apêndice G - Estratégias de formação e sensibilização no AEPM (versão expandida), com calendarização anual, responsáveis institucionais e indicadores de impacto.

Público-alvo	Estratégias	Instrumentos e metodologias	Calendarização	Responsáveis institucionais	Indicadores de impacto
Docentes	Capacitação em boas práticas de cibersegurança, proteção de dados e uso pedagógico seguro das TIC.	*Workshops* práticos; simulações de *phishing*; estudos de caso; alinhamento com *DigCompEdu* e PADDE; integração de dados do formulário digital de reporte de incidentes.	2 sessões anuais (setembro e março), revistas anualmente.	Equipa TIC; Equipa de Desenvolvimento Digital (EDD).	% docentes abrangidos; ganho de proficiência (pré-/pós-teste); índice *DigCompEdu* médio; taxa de cliques reduzida.
Não docentes	Formação em segurança digital aplicada a funções administrativas e técnicas.	Sessões presenciais e *online*; exercícios de resposta a incidentes; *checklists* de boas práticas.	1 sessão anual (novembro), revista anualmente.	Direção; EDD; Serviços Administrativos.	% não docentes formados; conformidade no uso de credenciais e dispositivos; perceção de segurança digital.
Alunos (1.º e 2.º ciclos)	Educação para a cidadania digital e proteção contra riscos *online* (*ciberbullying*,	Projetos interdisciplinares; jogos educativos; *storytelling*; integração em Cidadania e	Atividades semestrais (outubro e abril), revistas anualmente.	Docentes titulares; BE/CRE; Depart. Cidadania e TIC.	% alunos abrangidos; retenção de aprendizagens (questionários); mudança de

	phishing, privacidade).	Desenvolvimento/TIC.			comportamentos digitais.
Alunos (3.º ciclo e secundário)	Desenvolvimento de competências críticas de análise de informação e combate à desinformação.	Debates; análise crítica de notícias; projetos colaborativos digitais; recursos da Comissão Europeia (CE) e do CNCS; simulador *gamificado* de incidentes.	1 projeto anual (2.º período), revisto anualmente.	Depart. Cidadania; Depart. TIC; DT; BE/CRE.	% turmas integradas; índice *SELFIE* médio; aumento do reporte de incidentes.
Encarregados de educação	Parentalidade digital e acompanhamento das práticas tecnológicas dos filhos.	Sessões híbridas; *Digital Parenting* (EurofamNet); *Digital Academy for Parents* (E-REDES/DGE); divulgação e aceitação da *AUP (Acceptable Use Policy)* multilingue.	2 sessões anuais (outubro e fevereiro), revistas anualmente.	Direção; Assoc. de Pais; EDD; EECE.	% participação parental; perceção de utilidade (inquéritos); adoção de práticas seguras em casa.
Pessoal não académico	Sensibilização em práticas básicas de segurança digital aplicadas ao trabalho escolar.	Sessões *light-touch*; *newsletters* digitais específicas; distribuição de guias práticos curtos; *badges* digitais de participação (*OpenBadges*).	Trimestral (setembro, janeiro, abril, junho), revistas anualmente.	EDD; Equipa TIC; BE/CRE.	% participação em sessões; taxa de leitura das *newsletters*; perceção geral de segurança digital.

Nota. Todas as ações foram mapeadas segundo referenciais normativos aplicáveis (ISO/IEC 27002; RGPD; Diretiva NIS 2, art.º 20.º; *Digital Services Act*, Regulamento (UE) 2022/2065, art.º 32.º), assegurando conformidade regulatória e pedagógica.

Apêndice H – Matriz de correspondência entre as medidas do Plano de Cibersegurança do AEPM e os referenciais normativos

Correspondência detalhada entre as medidas apresentadas no Capítulo 5 e os principais referenciais legais e normativos aplicáveis: ISO/IEC 27002:2022, RGPD, Diretiva NIS 2 (UE 2022/2555) e orientações nacionais e europeias (CNCS, ENISA, DfE, CNPD, DSA).

Apêndice H - Matriz de correspondência entre medidas do Plano de Cibersegurança do AEPM e referenciais normativos

Área / Medida (5.3.x)	Descrição resumida	ISO/IEC 27002:2022	RGPD	NIS 2	Outros (CNCS / DSA / DfE / EECE)
5.3.2	MFA em contas privilegiadas e serviços críticos; *SSO* com *RBAC/ABAC*	8.2 Gestão de identidades; 8.3 Autenticação; 8.4 Gestão de credenciais	art.º 32.º (segurança do tratamento)	art.º 15.º e 21.º (medidas técnicas e gestão de risco)	CNCS AP4; *DfE Minimum Cyber Security Standards*
5.3.2	Política de palavras-passe e *PAM* básico (cofres; rotação)	8.3 Autenticação; 8.4 Gestão de Credenciais; 8.5 Gestão de acesso privilegiado	art.º 32.º	art.º 15.º e 20.º	CNCS – Boas Práticas Senhas
5.3.2	Segmentação de rede (*VLANs*), *802.1X*, rede de convidados isolada	8.20 Segurança de redes	art.º 32.º	art.º 21.º e 23.º	CNCS – Guias de Segmentação
5.3.2	*NGFW* e política *deny-by-default* entre segmentos	8.20 Segurança de redes; 8.23 Proteção contra *malware*	art.º 32.º	art.º 15.º e 21.º	*ENISA Good Practices for Schools*
5.3.2	Cifra de disco em *endpoints*; *EDR*; *Hardening* CIS	8.7 Segurança de ativos; 8.12 Defesa contra *malware*; 8.28 *End-user devices*	art.º 32.º	art.º 15.º e 21.º	*CIS Benchmarks*; CNCS
5.3.2	*SPF/DKIM/DMARC*; *sandboxing*; *banners*; bloqueio de *forward* externo	8.23 Proteção de *e-mail*; 8.24 Gestão de *phishing*	art.º 32.º	art.º 15.º e 21.º	*DfE Email Security Guidance*; CNCS

5.3.2	*Backups 3-2-1*; *WORM*; testes de restauro com *RTO/RPO*	8.13 *Backup*	art.º 32.º	art.º 21.º e 23.º	*ENISA – Backup & Recovery*
5.3.2	Centralização de *logs*; alertas; retenção ≥ 90 dias	8.16 *Logging* e monitorização	art.º 32.º; art.º 5.º, n.º 2 (responsabilização)	art.º 21.º e 23.º	CNCS – *Logging*; *ENISA*
5.3.2	Inventário de ativos; varrimento mensal; correções críticas ≤ 7 dias; altas ≤ 30 dias; reclassificação de falsos positivos	8.9 Gestão de vulnerabilidades; 8.8 Gestão de mudanças	art.º 32.º	art.º 21.º e 23.º	*CVE/CVSS*; CNCS
5.3.2	*Baseline* de segurança *cloud*; revisão de *apps* de terceiros; art.º 28.º	5.19/5.20 Gestão de fornecedores; 8.30 *Cloud services*	art.º 28.º, 32.º, 44.º-49.º	art.º 21.º	*DSA* (deveres de plataformas); CNCS *TIA*
5.3.2	Controlo de acesso físico; *UPS*; inventário de acessos	7.8 Segurança física e ambiental	art.º 32.º	art.º 21.º	CNCS – Segurança Física
5.3.3	Catálogo de políticas; revisão anual e pós-incidente; matriz *RACI*	5.1 Políticas; 5.2 Responsabilidades	art.º 24.º (responsabilização); art.º 5.º, n.º 2	art.º 20.º (governação)	CNCS *Governance Toolkit*
5.3.3	Registos art.º 30.º; *DPIA*; *TIA*; consentimento de menores (13 anos)	5.7 Conformidade; 8.10 Requisitos legais	art.º 5.º, 6.º, 8.º, 30.º, 35.º, 44.º-49.º	art.º 21.º	CNPD Guias Escolas; CNCS AP6
5.3.3	Gestão de terceiros: cláusulas art.º 28.º e auditorias	5.19/5.20 Gestão de fornecedores	art.º 28.º	art.º 21.º	*ISO/IEC 27036*; CNCS
5.3.3	Plano de resposta; *playbooks*; lições aprendidas	8.18 Gestão de incidentes	art.º 33.º-34.º (notificação/comunicação)	art.º 23.º (notificação); art.º 20.º	*CERT.PT Boas Práticas*
5.3.3	Plano de continuidade/*DRP*; exercícios	8.19 Continuidade do negócio	art.º 32.º	art.º 21.º	*ENISA Business Continuity*
5.3.3	Classificação documental; retenção; eliminação segura; metadados	5.32 Gestão de informação; 8.12 (*media handling*)	art.º 5.º, n.º 1(c)(e) minimização/limitação; art.º 32.º	art.º 21.º	CNCS – Gestão Documental
5.3.3	Plano de comunicação e canais de alerta em tempo real	5.35 Gestão de comunicação de segurança	art.º 33.º-34.º	art.º 23.º	*CERT.PT*; CNCS
5.3.4	Formação anual; micro-módulos;	6.3 Consciencialização e formação	art.º 24.º (responsabilização)	art.º 20.º	CNCS Referencial; *DigCompEdu*

	multiplicadores internos				
5.3.4	Integração curricular de cidadania digital (EECE)	6.3 (*awareness*) – suporte organizacional	art.º 5.º, n.º 2	—	EECE; *Perfil dos Alunos*
5.3.4	Simulações de *phishing* e exercícios *tabletop*	8.18; 6.3 (*awareness*)	art.º 32.º	art.º 21.º	*DfE Simulated Phishing Guidance*
5.3.4	Academia Digital para Pais; guias; *survey*	6.3	art.º 5.º, n.º 2	—	*DGE/ERTE Programas*
5.3.4	*Líderes Digitais / Embaixadores*; Carta de Responsabilidades	6.3	—	—	*DGE SeguraNet*; CNCS

Nota.
MFA = *Autenticação Multifator*;
SSO = *Logon Único*;
RBAC/ABAC = *Controlo de Acesso Baseado em Função/Atributo*;
PAM = *Gestão de Acessos Privilegiados*;
EDR = *Endpoint Detection and Response*;
MDM = *Mobile Device Management*;
NGFW = *Next-Generation Firewall*;
CIS = *Center for Internet Security*;
WORM = *Write Once Read Many*;
RTO = *Recovery Time Objective*;
RPO = *Recovery Point Objective*;
DPIA = *Data Protection Impact Assessment*;
TIA = *Transfer Impact Assessment*;
DPO = *Encarregado de Proteção de Dados*;
DRP = *Disaster Recovery Plan*;
EECE = *Estratégia de Educação para a Cidadania na Escola*;
ENISA = *European Union Agency for Cybersecurity*;
CNCS = *Centro Nacional de Cibersegurança*;
CNPD = *Comissão Nacional de Proteção de Dados*;
DfE = *Department for Education* (Reino Unido);
DSA = *Digital Services Act*;
TEIP = *Territórios Educativos de Intervenção Prioritária*;
DigCompEdu = *Digital Competence Framework for Educators*;
DGE = *Direção-Geral da Educação*;
ERTE = *Equipa de Recursos e Tecnologias Educativas*;
CERT.PT = *Equipa de Resposta a Incidentes de Segurança Informática em Portugal*.
Fonte: Elaboração própria (2025), com base nas secções 5.3.2 a 5.3.4 do Capítulo 5.

Última página intencionalmente deixada em branco