POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE EDUCAÇÃO E CIÊNCIAS SOCIAIS

NAVEGAÇÃO SEGURA: CAPACITANDO ALUNOS DO 1.º CEB PARA A CIDADANIA DIGITAL

Relatório de Projeto

Maria Elisa Ribeiro Borges

Trabalho realizado sob a orientação de

Carla Sofia Costa Freire

Leiria, setembro 2024

Mestrado em Utilização Pedagógica das TIC

ESCOLA SUPERIOR DE EDUCAÇÃO E CIÊNCIAS SOCIAIS

INSTITUTO POLITÉCNICO DE LEIRIA

AGRADECIMENTOS

Gostaria de manifestar a minha mais sincera gratidão à minha orientadora, professora Carla Freire, cuja sabedoria, apoio incondicional e confiança foram fundamentais ao longo de toda esta trajetória. Sua dedicação e expertise foram indispensáveis para a conclusão deste trabalho, e sua paciência e incentivo foram a base sólida em cada etapa do projeto.

Aos meus colegas de mestrado, quero expressar um profundo agradecimento pela colaboração e pelo apoio constante. Compartilhar desafios e conquistas com vocês foi um verdadeiro privilégio. Um agradecimento especial aos colegas que cederam gentilmente as suas turmas para a realização deste estudo, bem como aos professores da AEC de TIC, cujo apoio foi crucial para o sucesso deste projeto.

Minha gratidão eterna à minha família, cujo amor, compreensão e apoio inabalável foram as chaves para superar cada obstáculo, especialmente nos momentos mais difíceis. Por fim, aos amigos e a todos que acreditaram em mim, que ofereceram encorajamento nos momentos mais desafiantes e nunca deixaram de me motivar, expresso o meu mais sincero agradecimento. Esta conquista também é vossa!

RESUMO

A finalidade deste projeto consiste em desenvolver competências que permitam uma navegação segura na *internet*, aos alunos do 4.º ano do 1.º CEB, como um modo de os capacitar para uma maior responsabilidade e segurança digital. Para alcançar os objetivos principais do projeto foram desenvolvidas atividades, utilizando os mais diversos suportes, como por exemplo jogos digitais, filmes educativos e plataformas de apresentação e programação como *Canva* e *Nearpod* numa pedagogia interativa e centrada no aluno.

Os alunos tiveram, desse modo, a possibilidade de trabalhar, prática e dinamicamente, conteúdos como *phishing*, *cyberbullying*, privacidade e proteção de dados. Assim, de forma a aumentar os conhecimentos teóricos e a incutir, nos alunos, a real necessidade de ações de segurança digital, foram realizadas atividades específicas, que permitem o desenvolvimento do pensamento crítico e a autonomia, através de uma metodologia lúdica e divertida. Existiram ainda momentos de discussão e reflexão em grupo, que promoveram a construção do significado sobre o conceito de cidadania digital, bem como para fins de comportamentos mais responsáveis na navegação e interação *online*.

Os resultados obtidos indicam que a metodologia desenvolvida exerceu um efeito positivo e significativo no sucesso e na evolução do presente projeto, na medida em que foi possível ampliar conhecimentos e ações práticas ao nível do tema abordado. O envolvimento e a participação dos alunos, assim como o *feedback* atempado das plataformas digitais podem ter representado uma mais-valia para o seu empenhamento e para a interiorização de todos os novos conceitos e conhecimentos.

Palavras chave

Cidadania Digital, Competências Digitais, Literacia Digital Segura, Navegação Consciente, Proteção Cibernética, Segurança Digital

ABSTRACT

The purpose of this project is to develop skills that enable safe internet browsing for 4th-grade students in Primary Education, to equip them with greater responsibility and digital safety. To achieve the main objectives of the project, activities were developed using various resources, such as digital games, educational films, presentation and programming platforms like Canva and Nearpod, all within an interactive, student-centered pedagogy.

This way, students had the opportunity to work practically and dynamically on topics such as phishing, cyberbullying, privacy, and data protection. Thus, to enhance their theoretical knowledge and teach them the real need for digital safety measures, specific activities were carried out that fostered the development of critical thinking and autonomy using fun and playful methodology. There were also moments of group discussion and reflection, which promoted the understanding of the concept of digital citizenship and encouraged more responsible behavior in online navigation and interaction.

The results obtained indicate that the developed methodology had a positive and significant impact on the success and progress of this project as it allowed for the expansion of knowledge and practical actions on the addressed topic. The involvement and participation of the students, as well as the timely feedback from the digital platforms, may have represented added value to their engagement and to the internalization of all the new concepts and knowledge.

Keywords

Digital Citizenship, Digital Skills, Safe Digital Literacy, Conscious Browsing, Cyber Protection, Digital Safety

ÍNDICE GERAL

Índice de Figuras

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

ABREVIATURAS (FACULTATIVO)

TIC - Tecnologias de Informação e Comunicação
1.º CEB – 1.º Ciclo do Ensino Básico
PIEC - Política de Inovação Educação Conectada
CNCS - Centro Nacional de Cibersegurança
CSSN - Centro de SeguraNet
AE - Aprendizagens Essenciais
ENEC - Estratégia Nacional de Educação para a Cidadania

INTRODUÇÃO

As inovações tecnológicas proporcionaram benefícios consideráveis, sobretudo para o campo educativo. Desde que os computadores foram introduzidos nas instituições de ensino, passando pela chegada da *Internet*, e até a utilização da Inteligência Artificial, estas tecnologias aperfeiçoaram a gestão da informação, o acesso aos materiais e recursos educativos, proporcionando a diferenciação pedagógica, bem como a expansão dos ambientes de ensino aprendizagem.

Conforme Freire et al. (2023), a tecnologia contribui, significativamente de forma colaborativa, para o avanço educativo ao promover ambientes de aprendizagem mais ativos e inclusivos, facilitando o desenvolvimento de competências adaptadas às necessidades dos alunos. Por seu lado, Costa e Badaró (2021) tratam das implicações sociais das tecnologias digitais nas crianças, destacando os desafios relacionados com as interações sociais e riscos associados à privacidade e ao bem-estar no uso das ferramentas.

Esses avanços refletem-se no campo educativo, onde a interação e o contacto com ferramentas digitais proporcionam vantagens no envolvimento e empenho dos alunos, tornando o ensino mais interativo e centrado nos alunos (Souza, 2000). No entanto, esses avanços também apresentam desafios de adaptação, afetando e interferindo nas alterações sociais. Também é importante ponderar e avaliar os possíveis riscos associados ao uso das tecnologias, em particular, em termos de segurança e bem-estar dos alunos (Pontes, 2023).

Aureliano e Queiroz (2023) apontam a crescente autonomia dos alunos no acesso à informação como potencial fonte de desafios de segurança. Nascimento e Feitosa (2020) especificam perigos, como roubo de identidade e invasão de privacidade. Praxedes et al. (2023) expande o debate, incluindo temas como privacidade, participação cívica e discurso de ódio, destacando a importância de uma abordagem e observação ética e crítica. Os autores concordam que a interação entre educação, tecnologia e cidadania é complexa e dinâmica, tornando necessária uma dedicação contínua à ética e à responsabilidade.

Para que se efetive a construção de cidadãos conscientes e comprometidos, é necessário cuidar da educação de qualidade e da cidadania ativa. Vivemos a era da tecnologia digital, que promove transformações significativas nas práticas de ensino. De acordo com Cruz

e Costa (2022), as instituições educativas deverão tornar-se cada vez mais flexíveis, adaptativas e abertas às mudanças, bem como realçar a questão de educar para o uso seguro e consciente das ferramentas e tecnologias digitais.

Neste sentido, a pesquisa nesta área torna-se fundamental para lidar com os desafios e dificuldades com que se deparam os alunos do 1.º CEB, na medida em que não têm oportunidades para usar a tecnologia de forma adequada e intencional.

Consoante Souza et al. (2022), a mudança requer, inegavelmente, apoio institucional e pesquisa na promoção da segurança cibernética e formação de cidadãos digitais conscientes. Pelo que Cruz e Costa (2022) e Souza et al. (2022) reforçam que ensinar os alunos a abordar proativamente as dificuldades digitais permitirá desenvolver cidadãos ativos e bem-sucedidos, contribuindo para o atual e futuro da sociedade. Consequentemente, a integração de habilidades e aptidões digitais deve ser necessária desde as fases iniciais da formação académica para promover qualidade do ensino e uma cidadania ativa, participativa, informada e consciente. Pretende-se fomentar a formação de pessoas bem informadas e participativas, capazes de lidar com desafios enfrentados pela tecnologia por uma educação híbrida, integrada e coordenada entre vários agentes educativos.

A sociedade está afetada pela mundialização da digitalização e pela evolução tecnológica que determina especialmente, a educação. Um espaço seguro para a aprendizagem e para a proteção dos alunos frente a ameaças cibernéticas pode-se apresentar como um aspeto supérfluo para uma educação de qualidade do século XXI, sendo um elemento indispensável para o sucesso escolar e o bem-estar digital

Contexto e Relevância

Conforme o Conselho Nacional de Educação (2023), a inovação pedagógica é vital para ajustar métodos e abordagens pedagógicas, para que as futuras gerações consigam desenvolver as habilidades e competências essenciais para uma participação segura e consciente no ambiente digital. As habilidades digitais são cruciais para alunos e professores, porque viabilizam o acesso a recursos educativos *online*, a eficácia da informação e o trabalho em ambientes de aprendizagem virtual. Preparar alunos desde tenra idade é vital para a sua preparação em relação a futuros desafios.

O uso de tecnologias e a incorporação de aprendizagens interativas e personalizadas promovem a melhoria da experiência educativa (Farias et al., 2019).

O julgamento da eficácia da ação educativa, construído a partir da utilização dos dados e do *feedback* do ambiente digital, torna-se mais divulgado e ajustado às exigências de aprendizagem de cada aluno, transformando as aprendizagens na referência da ação educativa. Também é necessário garantir que os professores sejam formados para operar as tecnologias de acordo com a necessidade do trabalho educativo, para que este alcance o seu valor máximo.

Múltiplas iniciativas mundiais (globais) promovem a inovação pedagógica no âmbito digital a partir da preparação dos alunos para um mundo em mudança. Fomentar a inovação no ensino digital é fundamental, através de boas práticas e da cooperação internacional. Ajustar a educação às necessidades e aos desafios do século XXI é fundamental para formar cidadãos, competentes e preparados para o futuro digital.

Neste sentido, este estudo está ligado aos desafios contemporâneos ligados à cibernética, contribuindo para a consolidação da base da educação digital. É fundamental que a educação esteja preparada para o século XXI, em termos de que, alunos e professores estejam cuidadosamente preparados para prosperar na realidade digital.

Motivação pessoal

A crescente dependência da sociedade em tecnologias digitais e a exposição dos cidadãos a ameaças digitais motivaram este estudo. Com o presente trabalho espero aperfeiçoar a minha compreensão das táticas e tentar consciencializar nos mais jovens a criação de uma cultura mais forte de segurança. Ao longo dos anos verifiquei uma carência cada vez maior entre a utilização frequente da *internet* e a falta de aptidões digitais. Sendo esta carência aliada à insuficiência na preparação dos recursos que tinham ao seu alcance para a proteção da *internet* levaram-me a entender que devia fornecer solução a este problema. Reconhecendo o papel crucial das escolas na preparação dos jovens, para o mundo das tecnologias, entendo que é necessário fornecer soluções para esses problemas.

Além disso, é importante que os pais sejam instruídos a manter seguros os filhos no mundo da *internet*, devendo ser equipados com instrumentos e conhecimentos para navegarem com segurança e confiança.

Em suma, este projeto pretende capacitar alunos a protegerem-se dos perigos e riscos na *internet*, fornecendo-lhes os recursos e informações necessários.

PROBLEMA DE INVESTIGAÇÃO E PERTINÊNCIA DO ESTUDO

No domínio da cibersegurança, a investigação das ameaças cibernéticas e dos dados são sem dúvida de primeira linha. Por conseguinte, com o crescente desenvolvimento dos sistemas tecnológicos e da digitalização crescente da sociedade, também surgiram novos desafios em matéria de segurança na *Internet*. E ainda com o aumento do cibercrime e o desenvolvimento da natureza das ameaças, é crucial encontrar e desenvolver medidas de proteção de dados e de segurança na *Internet*. Este estudo poderá identificar algumas ameaças cibernéticas que se perfilam, assim como encontrar e desenvolver medidas e atividades competentes para mitigar essas situações, enfatizando o interesse de tais investigações no estado atual, especialmente dos alunos do 1.º CEB.

Este estudo aborda dificuldades legais relacionadas no uso da *Internet*, como destacado por Sobrinho e Grott (2022) Santos et al. (2023), que sublinham que estas não acompanham o rápido desenvolvimento do crime cibernético, dificultando a obtenção de provas.

Além disso, os desafios jurídicos associados ao uso da *internet*, resultam da circunstância de a legislação não ter acompanhado o desenvolvimento do cibercrime, dificultando a localização e a responsabilização dos sujeitos. De acordo com Santos et al. (2023), isto tem efeito na privacidade, minando a confiança dos utilizadores no ambiente digital. No entanto, segundo o autor, podem ser estabelecidas medidas proativas de proteção, como políticas de segurança digital; parcerias com empresas de segurança; organizações civis, mediante campanhas de consciencialização; proteção contra *bullying* cibernético e uma cultura de segurança *online*. Sendo de primordial importância a introdução sobre cibersegurança nas aprendizagens, por meio de uma abordagem multidisciplinar, preparando as gerações futuras para os desafios da segurança digital.

QUESTÃO DE INVESTIGAÇÃO E OBJETIVOS

O foco deste estudo consiste em examinar: **Qual a eficácia das ações voltadas para a alfabetização das habilidades de segurança digital dos alunos do primeiro ciclo?**

Com a questão de investigação traçada, a educação em cibersegurança centra a investigação na compreensão de como ensinar os alunos a protegerem-se dos riscos *online*.

Por isso, este projeto mostra uma organização, abordando questões essenciais de segurança digital no 1.º CEB. Ressaltando a importância do ensino seguro na *internet* para os alunos, integrando teoria e prática, ajudando a compreender e destacar como a importância das estratégias educativas podem reduzir as ameaças cibernéticas, enfatizando a importância da educação em segurança digital.

Tal metodologia vai além da transmissão de regras de segurança *online*, propondo um ensino que incorpore o uso de tecnologias como ferramentas pedagógicas, como sugerido por García Aretio (2019).

A finalidade é compreender como a educação em cibersegurança pode proteger os alunos dos novos dos riscos *online*, estabelecendo modelos pedagógicos que usem a tecnologia de forma segura. É necessário fornecer informações valiosas sobre métodos úteis, observar e analisar as preconceções dos alunos relativamente à segurança digital, incorporar esses conhecimentos no quotidiano e avaliar o progresso das aptidões em cibersegurança.

Dada a segurança digital assumir uma importância crescente no setor educativo, é importante abordar a questão para compreender cuidadosamente as conceções dos alunos, integrar tais estratégias durante o ensino e, em seguida, avaliar como tal prática afeta o desenvolvimento das competências. Portanto, o estudo pretende **identificar** as preconceções sobre segurança digital, **descrever** estratégias de integração da segurança digital no 1.º CEB e **analisar** como o relacionamento dos alunos com as atividades planeadas contribuirá para o desenvolvimento das competências. Pelo que se traçam os seguintes objetivos específicos:

1.Identificar as preconceções dos alunos sobre segurança digital: com este objetivo será possível compreender as conceções e os conhecimentos dos alunos sobre a segurança digital para posteriormente adaptar atividades e estratégias;

2. **Descrever estratégias de integração da segurança digital no 1.º CEB**: criação e implementação, na sala de aula, de estratégias integradas da segurança digital, com o intuito de garantir que cada aluno esteja fornecido atempadamente e detentor de informações corretas e ajustados sobre a matéria

3. **Analisar em que medida o envolvimento dos alunos nas atividades de segurança digital contribui para o desenvolvimento de competências**: investigar e avaliar em que medida a participação e envolvimento dos alunos nas atividades de segurança digital,

incidem na prática das atividades desenvolvidas, e quanto às competências adquiridas acarretando a compreensão sobre a forma como a educação para a segurança digital, faz melhorar e desenvolver as potencialidades e competências.

Desta forma, com este projeto, pretende-se obter informações através da utilização de jogos e atividades em sala de aula para estimular o envolvimento dos alunos. Além disso, será feita uma análise da literatura com o intuito de desenvolver estratégias educativas que envolvam os alunos nas aprendizagens relacionadas com a Segurança Digital.

ESTRUTURA DO TRABALHO

Este trabalho apresenta uma estrutura para abordar questões relevantes de segurança digital no contexto do 1.º CEB, enfatizando a importância da educação e de estratégias práticas para promover uma navegação segura na *internet* para crianças.

Tabela 1 - Navegar com Segurança: Estratégias de Educação Digital no 1.º CEB

Secção	Descrição
Enquadramento Teórico	O projeto tem como foco principal a segurança na *internet*, incluindo uma revisão da literatura sobre segurança *online*, conceitos fundamentais e teorias de suporte. Aborda a crescente relevância da segurança digital e apresenta estratégias práticas de segurança, de modo a corroborar as teorias apresentadas.
Metodologia	A metodologia é definida conforme o tipo de estudo, com os participantes, técnicas e instrumentos de recolha e análise de dados e considerações éticas, assegurando a clareza no processo investigativo.
Projeto	Dedicado ao planeamento e à execução do projeto e ao trabalho dos alunos nas aulas sobre segurança na *internet*, apresenta dados sobre as atividades pedagógicas desenvolvidas e a participação ativa dos alunos.
Apresentação e Discussão dos Resultados	Apresenta e discute os resultados alcançados, bem como uma análise das consequências em relação à segurança na *internet*. Inclui uma discussão sobre os problemas identificados, as estratégias de mitigação, o comportamento dos utilizadores e a análise do *feedback* dos alunos, permitindo a realização de melhorias metodológicas.

Secção	Descrição
Conclusões	Desfecha o projeto apresentando as principais conclusões do estudo, as contribuições teóricas e práticas para o campo da segurança na *internet*, identificando as limitações e dando recomendações para futuras pesquisas.

Nota - Este projeto aborda a importância da educação em segurança digital no 1.º CEB, oferecendo estratégias para proteger crianças online. Combina teoria e prática para promover uma navegação segura na internet.

I ENQUADRAMENTO TEÓRICO

1.1. PERTINÊNCIA DA INTRODUÇÃO DA SEGURANÇA NA INTERNET NO CONTEXTO ESCOLAR EUROPEU E NACIONAL

A evolução das tecnologias digitais transformou a sociedade e a educação, repercutindo-se na forma como comunicamos, aprendemos e trabalhamos.

A UNESCO (2017) definiu diretrizes que destacam a responsabilidade da educação, na promoção de competências para o progresso sustentável e inclusivo, realçando a necessidade de uma educação que desenvolva competências essenciais para lidar com os desafios do século XXI. Destacando, também, a urgência de alinhar a educação às eficácias e expectativas atuais. As instituições de ensino necessitam adotar estratégias que promovam a sustentabilidade e a integração social (UNESCO, 2019).

Mattar et al. (2020) analisam a perspetiva da União Europeia (EU) relativamente ao processo de digitalização na sociedade e na economia. Mattar et al. (2020) salientam que a União Europeia precisa estabelecer diretrizes estratégicas para aplicações e avaliar as habilidades digitais. O estudo abordou a metodologia de pesquisa, incluindo buscas na *internet*, revisão sistemática de literatura e análise crítica de documentos. Os *frameworks DigComp*, *DigCompConsumers*, DigCompEdu e *EntreComp DigComp* 1.0, o *DigComp* 2.0, o *DigComp* 2.1, o *DigComp* em ação, o *DigCompEdu*, o *DigCompOrg*, o *OpenEdu*, o DigCompConsumers e o *EntreComp* foram os focos da pesquisa, direcionada a profissionais da educação. Os resultados destacaram a importância de combinar competências e *frameworks*, na prática educativa, apontando para a necessidade de considerar tendências no uso de tecnologias digitais.

Cada uma das atividades foi realizada a partir de grupos e áreas de atividade diversas, desde a educação básica até as empresas, sublinhando a centralidade das competências digitais para o trabalho e a vida quotidiana. No entanto, a aplicação dos quadros é frequentemente complexa e apresenta dificuldades em considerar, separar e analisar os *skills* (habilidades). Além disso, é igualmente importante ter em vista as novas tendências em tecnologia educativa, tais como *MOOCs (Massive Open Online Courses ou Cursos Massive Open Online*), *makerspaces*, *analytics* para aprendizagem, pensamento computacional e *blockchain*, entre outros, que configuram o futuro da educação digital. Estas tendências apresentam a necessidade de um ajuste contínuo dos quadros de

competências digitais em consideração a novas habilidades e conhecimentos (Mattar et al., 2020). A UE deve ter uma abordagem completa, inclusiva e atenta a cidadãos, professores e organizações em relação às competências digitais. A avaliação e a implementação são os principais problemas ventilados para o desenvolvimento destas competências. Portugal está comprometido com a integração das TIC na educação primária, apoiada por legislações (Decreto-Lei n.º 55/2018 e Despacho n.º 6478/2017) e pelas Orientações Curriculares para as TIC do 1.º CEB, que estabelecem um currículo flexível e transdisciplinar; orientado para o desenvolvimento de competências digitais básicas para preparar os alunos para as mudanças constantes do mundo digital, focando no desenvolvimento do pensamento crítico, criatividade e ética digital de acordo com o Perfil dos Alunos à Saída da Escolaridade Obrigatória (PASEO) (Martins et al., 2017).

Na execução da Estratégia Nacional para a Educação Digital, a Direção Geral da Educação, os Centros de Competência TIC e algumas universidades uniram forças para garantir a acessibilidade à *internet* nos cursos. Essa medida visa a melhoria da qualidade do ensino técnico e do ensino vocacional em Portugal, preparando os alunos para enfrentar os desafios do presente e do futuro que a sociedade digitalizada comporta. Tal como relatam Meirinhos e Osório (2015), ao enfatizarem a importância da cooperação entre o Ministério da Educação de Portugal, os Centros de Educação em Tecnologia da Informação e diversas instituições e associações. A cooperação é essencial para alinhar os requisitos educativos com as necessidades tecnológicas.

O programa *SeguraNet*, iniciado em 2004, é um indicador do compromisso de Portugal em proteger crianças e jovens na *Internet* e contribuir para os objetivos da UE para um ambiente *online* seguro. É um modelo de colaboração entre os governos, as ONGs e o setor privado, por um lado, de consciencialização do público para o risco da *Internet*, e por outro, de promoção de ferramentas de mitigação desses riscos.

Neste ecossistema, o Centro de Sensibilização *SeguraNet* (CSSN) possui um papel central em desenvolver atividades, campanhas e materiais de apoio a professores e instituições envolvidas, promovendo a cidadania digital nos alunos. O CSSN está alinhado aos princípios das Aprendizagens Essenciais (AE) e da Estratégia Nacional de Educação para a Cidadania (ENEC), abordando temas que vão desde media, até direitos humanos, segurança e educação financeira.

O estudo de Pereira e Moura (2022), destaca uma série de atividades promovidas pelo SeguraNet, validando a escolha da educação digital e a capacitação para a cidadania

digital entre alunos em Portugal. As ações incluem competições tais como os Desafios *SeguraNet*, formação de Líderes Digitais e campanhas como o Dia da *Internet* Mais Segura e o Mês da Cibersegurança nas Escolas, na sua abrangência, desde o 1.º CEB ao Secundário, em conjunto com programas como Estudo em Casa: Dicas para te Manteres Seguro e a Linha *Internet* Segura nas Escolas, de recomendações de segurança a discentes, professoras e encarregados de educação no âmbito da educação a distância, durante o estado de emergência.

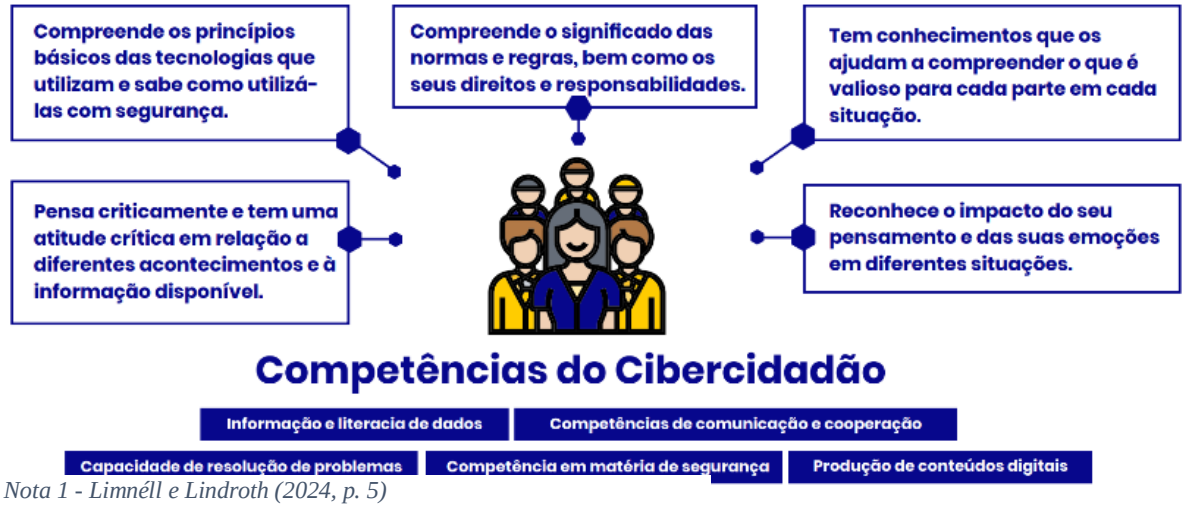
O efeito destas medidas foi avaliado por dirigentes escolares e professores, revelando que contribuíram significativamente para as competências de literacia e de cidadania digital dos alunos. Refira-se ainda que a *International Save the Children Alliance* e a *Insafe* reforçam a importância de uma *internet* segura e inclusiva, além da inclusão destas competências no currículo. Esta estratégia colaborativa e adaptada permite que os alunos se preparem para um mundo digital em constante evolução, legitimando as competências digitais como essenciais para o futuro pessoal e profissional do país.

Nesse contexto, a abordagem integrada e colaborativa de Portugal, voltada para uma educação digital sólida, está alinhada com a visão de Prensky (2019) sobre a adaptação às mudanças num mundo cheio de desafios.

O uso crescente de *smartphones* por crianças portuguesas em detrimento de computadores ou *tablets*, com um aumento de 87% no acesso à *internet* e um decréscimo no uso de computadores portáteis para 41%, conforme o estudo de *EU Kids Online* Portugal (Ponte & Batista, 2019) destaca essa mudança. Essa mudança acentua a necessidade de reformular as políticas educativas para refletir a realidade digital dos jovens. Defronte dessa modificação, Picone et al. (2019) salientam a importância de navegar de forma responsável sob a monitorização de adultos. A tecnologia, um veículo de informação e comunicação, poderá tornar os jovens dependentes de plataformas digitais. Por isso, é importante desenvolver desde a Educação Básica as competências e a cidadania digital, sendo fundamentais para lidar com segurança no ambiente digital.

A Figura 1 destaca competências essenciais para o uso seguro e eficiente da *internet*. Sendo assim, está dividida em seções, como Literacia da informação e Pensamento crítico, proporcionando uma visão das competências necessárias para os cibercidadãos. Essas competências são cruciais para a educação digital atual, formando utilizadores que naveguem de forma ética e eficiente no mundo digital globalizado.

Figura 1 - Competências do Cibercidadão



Nota 1 - Limnéll e Lindroth (2024, p. 5)

Esta preparação é reforçada pelos dados do DQInstitute (2020), que destaca que 60% das crianças entre 8 e 12 anos estão vulneráveis a variados ciber-riscos. O relatório da Organização das Nações Unidas para a Educação (2019), ecoa esta realidade e argumenta a favor de uma abordagem holística que compreenda tanto políticas de segurança robustas quanto iniciativas educativas eficazes. A adoção de práticas que garantam uso responsável do digital e desenvolvam competências digitais é crucial, alinhadas aos padrões nacionais.

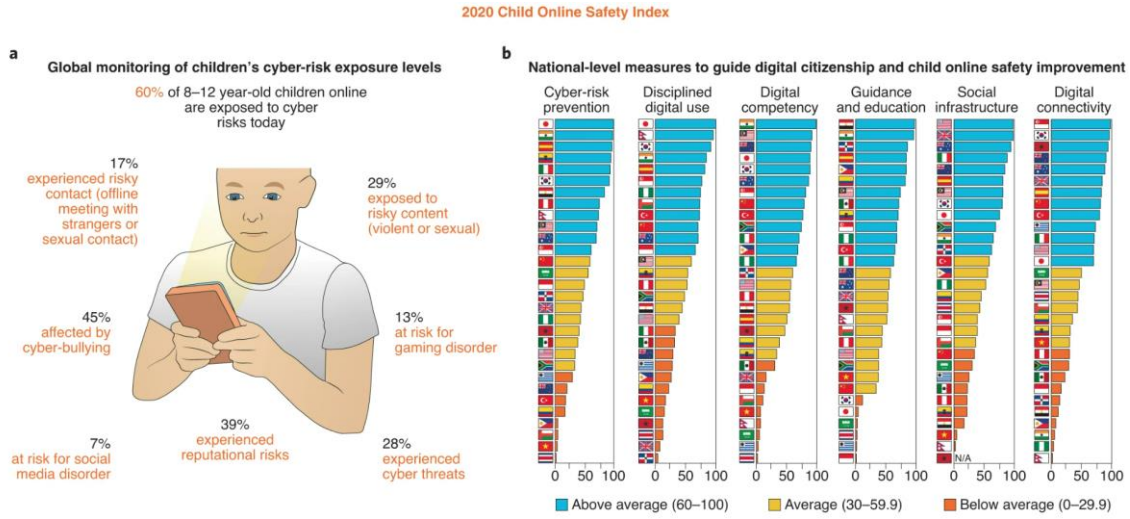
Desta forma, a escola tem um papel crucial na promoção da informação, comunicação, conhecimento e desenvolvimento de competências fundamentais para a cidadania no mundo digital. O relatório *Save de Children* (2002) e A Aliança Internacional *Save the Children e a Insafe*, robustecem essa demanda, priorizando o compromisso mundial de garantir a segurança *online* das crianças. Com a crescente digitalização, a proteção dos direitos das crianças na *internet* torna-se ainda mais relevante. A combinação desses esforços com a consciencialização dos pais sobre a utilização das redes sociais é essencial para garantir um ambiente seguro para o desenvolvimento dos jovens.

Nesta sequência, Venter et al. (2019) e Limnéll e Lindroth (2024) revelam preocupação com o facto de os alunos não possuírem uma cidadania digital robusta e uma segurança *online* eficaz. Nesta linha, também a investigação de Jackman et al. (2021) evidencia a discrepância entre a evolução tecnológica e a educação relativamente à segurança *online* dos alunos. Os estudos mostram que é fundamental instruir os alunos no uso seguro das tecnologias digitais para enfrentar os desafios riscos da *internet*.

Jackman et al. (2021) analisam o efeito profundo do mundo digital na vida dos alunos. Muitas crianças enfrentam riscos cibernéticos, evidenciando a disparidade entre a evolução tecnológica e a adaptação das esferas educativas, políticas e culturais.

A Figura 2, segundo Jackman et al. (2021), revela o descompasso no Índice de Segurança Infantil *Online*, destacando a relevância de avaliar o desempenho das nações em áreas como prevenção de riscos cibernéticos, educação digital e infraestruturas. Os dados mostram que casos de *cyberbullying* e exposição elevada a conteúdos inadequados são sinais que requerem cautela e ações integradas. As competências para proteger as crianças no ciberespaço devem ser multifacetadas, abrangendo desde a prevenção de riscos até a promoção da cidadania digital ativa. Defende-se a integração entre políticas nacionais e educação digital para reduzir os riscos no ciberespaço e criar um ambiente digital estimulante para o crescimento dos jovens. Ao passo que Bittencourt e Pimenta (2023) defendem que a cooperação internacional facilita o intercâmbio de informações e a investigação de casos de exploração sexual infantil. Além disso, promove a criação de legislações uniformes e políticas públicas eficazes, fortalecendo a resposta global ao problema. Essa colaboração é essencial para proteger as vítimas, além de prevenir a venda de crianças e a pornografia infantil.

Figura 2 - Segurança Online para Crianças 2020



Nota 2 - (Jackman et al., 2021, p. 543).

Esses estudos apontam para uma tese central: os riscos do mundo digital exigem uma urgente reavaliação dos paradigmas educativos.

A educação deve preparar as pessoas para navegar de forma segura e produtiva na *internet* com responsabilidade e criticidade, prontas para enfrentar os desafios de um mundo conectado. Como as instituições educativas e os formuladores de políticas abordam essa

tarefa, define a eficácia com que a sociedade pode proteger e empoderar a próxima geração no espectro digital global.

Mudanças nos padrões de acesso digital entre as crianças portuguesas, conforme o *EU Kids Online* Portugal de Ponte e Batista (2019) e Limnéll e Lindroth (2024), indicam uma tendência crescente no uso de dispositivos móveis. Essa tendência sugere a importância de adequar as políticas educativas à realidade digital dos jovens e promover competências digitais essenciais. Fortalecendo a ideia de que a cibersegurança e a cidadania digital devem ser ensinadas desde cedo e integradas no contexto educativo e social.

Do mesmo modo, Picone et al. (2019), Leaning (2019), Tavares e Melo (2019), Chicava e Nhanombe (2020) e Vilaça e Araújo (2016) concordam sobre a importância de analisar a navegação na *internet* de forma crítica. Efetivamente também Tavares e Melo (2019), destacam que a tecnologia pode ser usada para fins educativos, valorizando as interações sociais e a conexão entre professor e aluno, tornando a aprendizagem mais significativa. Defendem uma escola alinhada com a era digital, onde os professores possam integrar recursos digitais na prática letiva, adotando métodos de ensino que correspondam às experiências dos alunos e promovam debates sobre ética digital e segurança *online*. Devem estimular o trabalho colaborativo, usando a *internet* como ferramenta de pesquisa e criação, fomentando o pensamento crítico e a análise reflexiva com o uso de plataformas digitais.

De forma similar, os estudos de Pinheiro e Silva (2020), Freitas et al. (2023) e Souza et al. (2022) promovem uma visão inclusiva de uma educação digital adaptada e holística. Essa abordagem atende às demandas do ambiente digital. Integrar literacia e segurança digital no currículo do 1.º CEB, com uma abordagem colaborativa e adaptativa, estabelece a base para desenvolver competências digitais, garantindo que a tecnologia promova o desenvolvimento inclusivo, seguro e produtivo.

Em consonância com essa visão, Sales et al. (2019) destacam a necessidade de adaptação das instituições educativas às transformações na sociedade digital. As escolas são vistas como veículos de transmissão de conhecimento e comunicação, fundamentais na formação de competências vitais para a cidadania digital. Isso inclui competências em segurança na *internet* e a capacidade de discernir informações confiáveis. Este estudo sublinha a importância de uma abordagem educativa alinhada às rápidas mudanças tecnológicas, onde as competências digitais são vistas como ferramentas pedagógicas auxiliares fundamentais para capacitar os alunos a se envolverem de forma ativa e responsável no contexto digital. Os autores defendem a necessidade de os educadores

possuírem habilidades essenciais para guiar os alunos na navegação segura e crítica pelo ambiente *online*. Essa exigência realça a relevância da educação digital, na capacitação técnica, como promotora de uma cidadania consciente e informada.

No contexto da educação para o século XXI, a UNESCO e Trindade e Moreira (2017), com base no relatório *New Visions for Education: Unlocking the Potential of Technology*, publicado pelo *World Economic Forum* em 2015, destacam a relação entre a tecnologia e as competências necessárias para o século XXI. Essa observação destaca a urgência de reformular a educação para capacitar os alunos e profissionais com as competências necessárias para enfrentar as exigências de um ambiente laboral em constante mudança e em rápida inovação tecnológica. Portanto, deve haver alinhamento entre os desafios e as aspirações do século XXI, visando valores e habilidades que promovam o progresso sustentável e inclusivo (UNESCO, 2017). Esta perspetiva destaca a necessidade de uma educação que promova valores e competências fundamentais para o progresso sustentável e inclusão social.

Reconhecendo a crescente relevância da segurança cibernética, o Ministério da Educação publicou um quadro sobre segurança, defesa e paz para orientar a cooperação segura na sociedade. Isso mostra que a educação em segurança cibernética exige mais profissionais qualificados. Essa exigência faz parte de uma sociedade europeia digitalmente segura e conectada, uma visão compartilhada por Caseiro (2021) e Duarte et al. (2022). Esses autores defendem a importância de aprender sobre segurança na *internet* para criar uma comunidade forte e preparada para enfrentar problemas futuros. O objetivo é garantir que todos usem a *internet* com segurança aprendendo e adaptando-se às mudanças digitais.

Em Portugal, a tecnologia digital traz desafios e oportunidades para os alunos do 1º CEB, exigindo uma abordagem pedagógica alinhada ao rápido avanço das TIC e que promova uma cidadania digital segura, responsável e competente.

Desde a década de 1980, com a introdução de computadores nas escolas, o ensino passou por uma modernização significativa, incorporando métodos de ensino a distância e modelos semipresenciais ao longo do século XX.

A pesquisa de Filho e Cardoso (2024) revela que os alunos devem adotar estratégias como aprendizagem baseada em projetos, discussões e simulações, promovendo a participação ativa dos alunos no processo de aprendizagem. Essas abordagens permitem a flexibilidade e conetividade, facilitando a adaptação a um ambiente de ensino híbrido e conectado.

Deste modo, a educação deve promover o protagonismo e autonomia dos alunos. Os métodos com recurso às tecnologias estimulam a criatividade, o pensamento crítico e o

desenvolvimento de competências básicas dos alunos, preparando-os para o século XXI, paralelamente tornando a aprendizagem mais dinâmica e eficiente.

Esse processo facilitou o acesso ao conhecimento, porém gerou desafios e obstáculos, tais como a exigência de atualização na área pedagógica, capacitação adequada e constante, para que a integração das tecnologias na aprendizagem dos alunos seja eficaz, referindo ainda, a necessidade de infraestruturas tecnológicas adequadas. O estudo realça preocupação sobre o acesso equitativo e justo dos alunos às tecnologias, evitando a exclusão digital. Finalmente, é fundamental adaptar currículos e métodos de ensino para refletir as novas realidades e demandas do ambiente tecnológico, garantindo que a educação continue relevante e eficaz, proporcionando uma experiência de aprendizagem inclusiva e significativa para todos os alunos.

As inovações tecnológicas digitais provocaram mudanças significativas na sociedade e na educação, tendo um efeito significativo na comunicação, na aprendizagem e no trabalho. A UNESCO (2017) elaborou diretrizes que destacam a importância de promover competências e conhecimentos primordiais para o progresso sustentável e inclusivo, alinhando-se com as exigências atuais. É relevante ter diretrizes e iniciativas direcionadas para a integração de tecnologias digitais na educação para formar os alunos para os desafios do século XXI. Complementando esta perspetiva global, Mattar et al. (2020) assinalam a importância da tecnologia no desenvolvimento de competências digitais, para enfrentar as ações atuais e futuras.

Em Portugal, a inserção das TIC no ensino básico segue padrões, orientações e diretrizes que propiciam um currículo versátil e interdisciplinar. Iniciativas como o programa SeguraNet comprovam a magnitude da segurança *online* e da cidadania digital.

A parceria entre diferentes entidades educativas é decisiva para capacitar os alunos a enfrentar um ambiente digital em constante transformação.

O próximo capítulo, A Fronteira Digital: Confrontando Ameaças Cibernéticas, abordará a contextualização geral das ameaças cibernéticas, definindo e explicando implicações específicas. Essa análise permitirá entender os desafios e estratégias necessárias para proteger e capacitar a próxima geração no mundo digital globalizado.

1.2. A FRONTEIRA DIGITAL: CONFRONTANDO AMEAÇAS CIBERNÉTICAS

A relação das crianças com a *internet* envolve riscos de segurança e o desenvolvimento de habilidades tecnológicas. Ataide et al. (2019) sugerem que as crianças têm aptidões e habilidades para comunicarem *online*. Os autores apontaram que essa habilidade se deve à experiência e à capacidade no hábito de utilização de ferramentas tecnológicas, assim como ao desenvolvimento das competências de navegação e comunicação *online*.

Entretanto, o uso excessivo das TIC também pode ter efeitos negativos, levando a dependências e dificuldades na administração do tempo *online*, evidenciando a importância de compreender e monitorizar os efeitos dessas tecnologias na rotina diária dos jovens. Tocantins e Wiggers (2021) realizaram uma investigação, na qual demonstraram que 83% dos intervenientes dominam a tecnologia, dedicando-lhe, em média 70% do seu tempo diário.

A incorporação das TIC no domínio do ensino inaugurou uma nova era, enriquecendo as práticas pedagógicas com uma vasta gama de instrumentos digitais, como evidenciado por Machado et al. (2023) e Moro (2021). No entanto, essa evolução enriquece as práticas com uma panóplia quase infinita de instrumentos digitais, especialmente para alunos do 1.º CEB. Esses desafios abrangem a implementação eficaz das tecnologias em sala de aula, bem como a promoção de uma cultura de uso seguro e responsável da *internet* ao nível de alunos, profissionais, educadores, professores e toda a comunidade escolar.

Consoante evidenciado por Cruz e Costa (2022), Sales et al. (2019) e reiterado pelas observações de Schlemmer et al. (2020), a educação deve incluir a promoção de habilidades digitais para que os alunos possam navegar na *internet* e se envolver na sociedade digital. Esta visão é refletida no trabalho, que, ao abordar os perigos do ambiente digital, mostra a necessidade de estratégias educativas para a segurança digital.

Apesar da *internet* facultar inúmeras oportunidades de aprendizagem e socialização, também carrega diversos perigos que podem afetar crianças e adolescentes (Barros, 2024). Entre os principais riscos destacam-se o *cyberbullying*, pedofilia, pornografia infantil, *sexting*, violação de privacidades, crimes virtuais.

Sani et al. (2021) realizaram um estudo entrevistando 560 pais de crianças entre 6 e 17 anos, focando-se na perceção sobre o *online grooming (aliciamento online)*. Cerca de 50% dos participantes desconheciam o termo, mas 97% o consideraram um fenómeno grave. Por outro lado, em termos de riscos comportamentais um estudo, conduzido por

Ayinmoro et al. (2020), examinou a relação entre *sexting* e comportamentos sexuais de risco, em alunas da Universidade do Delta do Níger. O estudo, envolveu 200 alunas, utilizou questionários estruturados na recolha de informação. Constatando-se que o envio de fotos nuas (2.504) e a utilização de *smartphones* (16.139) estão significativamente associados a condutas sexuais de risco. Além de que esses comportamentos também são afetados pela idade e etnia. A definição de *Sexting* refere-se ao ato de enviar imagens ou mensagens sexuais por email, ou outro meio eletrónico, podendo envolver atos criminosos.

O artigo de Alvarenga e Rocha (2023) aborda o fenómeno de ***sharenting***, relacionando com as caraterísticas do compartilhamento e os direitos das crianças e adolescentes, com exposição exagerada nas redes sociais, pelos pais.

Malecki et al. (2021) explicam o objetivo principal do ódio *online* e dos ***haters*** como forma de expressar uma atitude negativa relativamente a uma pessoa ou objeto, independentemente de causar danos reais, provocar reações em outros ou diminuir o valor de um grupo social, expressando intensamente os seus sentimentos e pensamentos de forma negativa.

O ***Phishing*** é usado para obter informações confidenciais por meio de emails falsos e páginas fraudulentas, sendo uma ameaça crescente na internet. Medon (2022) investiga como é que as redes sociais são usadas e os efeitos negativos que podem implicar para as crianças e adolescentes, nomeadamente quando os pais partilham informações pessoais dos filhos. Além disso, a segurança digital envolve a proteção contra ameaças como *malware* e *phishing*, Desta forma, Ribeiro et al. (2022) evidenciam como é crucial garantir a manutenção da legalidade e proporcionalidade dessas tecnologias nas investigações criminais, definindo *malware* como um conjunto específico de *softwares* que, instalados de modo oculto em um equipamento ou sistema informático, permitem a um utilizador externo o acesso às informações e dados neles contidos, além de um controle contínuo e secreto sobre uma pluralidade de suas funcionalidades. Rui et al. (2020) reforçam essa preocupação, utilizando um método de aplicação de um questionário que continha respostas quantitativas e qualitativas para análise dos dados. Os dados mostraram que parte dos entrevistados sabiam que foram vítimas de *phishing*, mostrando a importância da consciencialização e da segurança na *Internet*, como fatores agravantes. Rathee e Mann (2022) explicam que os ataques de ***phishing*** utilizam técnicas de engenharia social para enganar as vítimas, através da instalação de *malware*.

Nesse contexto, uma ameaça significativa é o *cyberbullying*, definido como práticas de consequências psicológicas, ansiedade, depressão e, em caso extremos, suicídio. No ambiente escolar pode prejudicar o desempenho e bem-estar dos alunos (Baldry et al., 2019). Tristão et al. (2022) destacam que o ***Cyberbullying*** é uma questão grave que afeta muitas crianças na *Internet*, caracterizado por condutas agressivas e constantes que conduzem a problemas psicológicos e mentais. Ambos os autores, destacam a importância de enfrentar e combater o problema e garantindo um ambiente *online* seguro e saudável. O *Bullying*, por seu lado envolve atos repetitivos de violência, com desequilíbrio de poder agredindo ou humilhando, enquanto o *cyberbullying* é a violência virtual com ataques repetitivos por meio de ferramentas tecnológicas, garantindo anonimato. Além disso, Machado et al. (2023), apresentam um estudo complementar que chama a atenção para os perigos para as crianças e adolescentes na *internet*, como o *cyberbullying*, o acesso a conteúdos inapropriados e exposição de predadores *online*. Os autores recomendam um enfoque educativo que assinale estes riscos e, ao mesmo tempo, também otimize o desenvolvimento de competências tecnológicas cruciais para a prática segura e esclarecida na web interativa. Ao mesmo tempo, igualdade de acesso para produzirem e partilharem eles próprios um conteúdo ético responsável, respeitando os direitos de autor e privacidades dos outros.

Enquanto a cidadania digital é essencial, a segurança *online*, basicamente no que diz respeito ao *cyberbullying*, permanece uma preocupação central.

Júnior (2021) reforça a importância de integrar a cidadania digital no currículo, de modo a preparar os alunos para interagir de maneira segura e ética com as tecnologias eletrónicas. Este autor argumenta que, além de alertar para os riscos, os alunos também devem ser capacitados a explorar de modo informado e responsável o mundo virtual. Neste contexto, é essencial que o aluno seja instruído a usar competentemente as ferramentas digitais e que compreenda os direitos, responsabilidades e riscos ligados à sua utilização. Tudo isto ajuda a dispor-se para a aplicação de um olhar crítico sobre a sua presença digital e pegada *online*.

Além disso, as redes sociais têm desempenhado um papel significativo no aumento do *cyberbullying*, como discutido por Chaves-Álvarez et al. (2020). A utilização contínua de tecnologias, plataformas e redes sociais facilita o ***cyberbullying*** entre adolescentes, permitindo o anonimato e a disseminação de mensagens prejudiciais.

1.3. COMO INTRODUZIR A LITERACIA E SEGURANÇA DIGITAL NO ENSINO BÁSICO?

Dada a situação atual, a Segurança digital na educação exige colaboração entre centros educativos e famílias. A segurança e a alfabetização digitais desempenham um papel importante na sociedade atual. Portanto, para enfrentar estes desafios, os Professores devem adotar uma abordagem proativa e integrar a literacia digital no contexto educativo (Neumann & Missel, 2019).

A importância de avaliar a fiabilidade das informações *online* é ressaltada como competência crítica. Portanto, a educação deve-se transformar para atender aos desafios digitais, preparando os alunos para uma participação ativa, responsável e informada, indo além do ensino tradicional e integrando o desenvolvimento de habilidades digitais como parte essencial do processo educativo. Nesta linha, Pires (2019) valoriza as TIC na medida em que desempenham um papel decisivo na educação contemporânea através de ambientes de aprendizagem mais interativos e ricos. Considera ainda, que adquirir competências, confiança e satisfação na utilização das Tecnologias permite que os alunos se habituem à utilização das aplicações, bem como aprendam desde cedo a avaliar potencialidades e limitações. Não esquecendo que, isto significa, sobretudo, um grande apoio, principalmente para alunos com necessidades específicas.

García Aretio (2019) destacam a importância urgente de uma incorporação profunda das tecnologias digitais na educação. Uma situação que força o sistema de ensino a reformular suas estratégias. O autor propõe uma alteração de paradigma na educação, considerando a inclusão de novas ferramentas tecnológicas em métodos educativos como algo imprescindível.

Essa mudança vai além da aprendizagem dos alunos e também se preocupa com a importância do desenvolvimento profissional constante dos Professores. Contudo, o foco de Júnior (2020) na preparação para a utilização segura e eficiente das tecnologias digitais traz uma reflexão importante sobre os possíveis perigos relacionados ao seu uso inadequado.

Agregando as considerações propostas por Noleto et al. (2019), ao garantir a inclusão e equidade na educação, vislumbra-se uma educação que excede o tradicional, legitimando a literacia digital como pilar para uma educação realmente inclusiva e equitativa.

À medida que navegamos por um mundo em constante mutação, a procura por oportunidades de evolução e aperfeiçoamento ininterrupto torna-se impreterível. Das estratégias de ensino-aprendizagem ao progresso da segurança *online*, transpondo a pesquisa científica e evolução de aptidões, procura-se promover a inclusão e equidade no acesso às tecnologias.

Dentro deste contexto mais amplo, o realce nas **estratégias de aprendizagem** representa a base do progresso educativo, influenciando seguramente o presente e fortificando o suporte de conhecimento para o futuro.

Para abordar a segurança digital de forma prática, projetos que abordam diretamente a segurança digital, como a criação de senhas seguras, a proteção de dados pessoais e a identificação de fontes confiáveis e promoção de comportamentos seguros, destacam a relevância de processos de aprendizagem, tornando-os mais interativos e envolventes. Essa abordagem, capta a atenção dos alunos de forma eficiente, apetrechando-os com competências essenciais para uma navegação segura na *internet* (Freitas et al., 2023).

Além disso, Sales et al. (2021) previnem para os riscos de usar muita tecnologia, sugerindo que as escolas, famílias e comunidades trabalhem unidas para utilizar a *internet* de forma saudável. Enquanto isso, Ponte et al. (2018) analisam distintas formas de auxiliar as crianças na *internet*, classificando-as e salientando que é preciso ter aptidões características para orientar as crianças num ambiente *online* cada vez mais difícil. Daí, a importância da educação participativa, sublinhada por Chicava e Nhanombe (2020), no sentido de ensinar segurança digital e gerar um ambiente de aprendizagem colaborativo. Esse método capacita os alunos a serem consumidores habilitados e criativos e cidadãos responsáveis.

A inovação pedagógica, patenteada pelo projeto *Self Protect*, de Farias et al. (2019), indicia um caminho promissor para lidar com esta questão, utilizando um método lúdico e interativo para ensinar conceções elementares de segurança *online* para crianças e adolescentes.

Contudo, Moro (2021), propõe um método prático para ensinar sobre segurança na *internet*, ressaltando que a utilização de projetos de aprendizagem e colaboração para ensinar segurança *online* motiva os alunos a criarem um ambiente digital mais seguro e inclusivo. Dessa forma, a integração dos diferentes esforços e perspetivas destaca a necessidade de uma abordagem multifacetada para a educação em cidadania digital,

harmonizando o benefício didático das TIC com uma educação robusta em segurança *online*. Esta harmonia impõe uma habilidade educativa holística que previna sobre os riscos relacionados ao mundo digital e diligencie a evolução de capacidades digitais, estimulando uma atitude ética, consciente e responsável no uso da *internet*.

Para fortalecer essas iniciativas, Farias et al. (2019) fazem um esforço inovador para instruírem os jovens sobre os riscos *online* de uma forma envolvente e informativa. Gomes e Souza (2022) dizem que é preciso mudar as formas de ensinar usando tecnologia e mudando como ensinamos.

Por outro lado, Silva e França (2023) fornecem uma análise crítica acerca de estratagemas reais e praticáveis para a educação em cidadania digital nas escolas. Eles sugerem uma representação cautelosa dos recursos, programas e iniciativas disponíveis, identificando e nomeando lacunas e probabilidades para robustecer a educação.

Logo, a integração das TIC na educação, em concordância com Júnior (2021), Machado et al. (2023) e Bernardo e Moro (2021), exprimem uma mudança fulcral para um modelo educativo que valoriza a segurança *online* e a cidadania digital. Através da concretização de estratégias inovadoras, como jogos educativos para ensinar segurança na internet *Self Protect* e iniciativas que exploram a mudança digital na educação, ergue-se uma possibilidade educativa que conecta as tecnologias e evidencia a *pertinência* de uma utilização consciente e responsável dessas ferramentas. Essa atitude integrada prepara os alunos para percorrer com segurança o ambiente digital, capacitando-os como cidadãos digitais ativos, responsáveis e conscientes, prontos para cooperar seguramente para a sociedade digital.

As ações educativas ao nível da Segurança Digital são essenciais para fortalecer o senso de segurança e a aplicação no ambiente escolar, conforme apontado por Pereira e Moura (2022), abrangem diversas abordagens, visando diligenciar procedimentos seguros no ambiente *online*. Por um lado, a consciencialização dos alunos é despertada através de programas e campanhas que alertam para a proteção de riscos, fraudes e perigos. Por outro lado, a elaboração de códigos de conduta estabelece diretrizes claras para condutas conscientes no uso da tecnologia.

Entre as iniciativas mais importantes para reforçar a segurança digital nas escolas, destacam-se a Campanha Mês da Cibersegurança, que consciencializa a comunidade escolar sobre práticas seguras *online*, e a Campanha Linha *Internet* Segura, que fornece

recursos para o uso seguro da *internet* nas instituições de ensino. Na verdade, devido à interconexão das coisas, tanto o que se faz como o que os outros fazem são muito importantes para termos um futuro melhor. Ao promover tais situações, o resultado é, de facto, prepararmos o terreno para um amanhã mais fulgurante e seguro.

Essa integração da educação digital no currículo escolar promove discussões sobre ética e privacidade *online* e fornece orientação decisiva sobre formas de reconhecimento de ameaças digitais, fortalecendo a preparação dos alunos para navegar de forma segura e responsável no ambiente *online*.

As **Atividades de Pesquisa** devem abranger a investigação científica na área de segurança cibernética, com foco nos alunos. Essas ações visam avaliar tendências e ameaças *online*, procurando identificar as melhores práticas para os proteger enquanto exploram o mundo virtual.

As **atividades de desenvolvimento**, em conjunto, pretendem criar recursos e ferramentas *online* de segurança para alunos, incluindo plataformas de aprendizagem seguras, aplicativos educativos e ambientes virtuais, bem como proteger contra riscos, assegurando a segurança.

Além disso, as **Atividades de Promoção** concentram-se na sensibilização e, sobretudo, na capacitação dos alunos para os desafios e novidades que surgem na navegação, sobretudo no que diz respeito à segurança digital.

Por último, as **Atividades de Treino** incluem a capacitação dos alunos facultando-lhes conhecimentos e proficiência a nível da segurança digital, envolvendo programas de treino e preparando-os para reconhecerem ameaças, tomarem medidas preventivas e reagirem a situações de risco *online*. Os treinos de segurança digital ensinam os alunos a lidar com ameaças, tomar medidas preventivas e lidar com situações de risco *online*.

As atividades, quando concertadas, provocam um conjunto coeso de estratégias e habilidades que fortificam a educação digital e a segurança *online*.

1.4. O DESIGN THINKING COMO FERRAMENTA PARTICIPATIVA PARA PROMOÇÃO DA LITERACIA EM SEGURANÇA DIGITAL

O ***Design Thinking*** é uma metodologia de resolução de problemas que se destaca por ser centrada no aluno, priorizando a empatia, a identificação clara de problemas, na prototipagem de soluções e na sua testagem.

De acordo com Baričević e Luić (2023) a integração de metodologias ativas de aprendizagem como o *Design Thinking*, proporcionam a retenção de conhecimentos e a capacidade de os desenvolver de modo dinâmico e inovador. Dessa forma, o *Design Thinking* pode modernizar a educação, habilitando os alunos a compreenderem o conteúdo e a utilizá-lo para criar soluções.

Complementarmente, o estudo de Pande e Bharathi (2020) conduz uma investigação teórica do *Design Thinking* sob o prisma do construtivismo. Os autores destacam como a prototipagem e os testes são vitalizadores para os principiantes construírem o seu raciocínio, reiterando a ideia de que o *Design Thinking* resolve problemas e auxilia a aprendizagem profunda por meio da experimentação ativa.

Na metodologia do *Design Thinking*, a etapa da **Empatia**, é decisiva para compreender profundamente as dificuldades, adversidades e desafios dos utilizadores, neste caso, alunos e professores, envolvendo o entendimento e observação, inserindo o lado emocional desde o início. A seguir, na etapa de **Ideação**, sucede o *brainstorming* gerando diversas soluções para o problema. Posteriormente, na fase de **Prototipagem**, é elaborado um protótipo da ideia, transformando-a em algo tangível para avaliação. Por fim, na etapa de **Testagem**, há a planificação para executar os projetos, avaliação dos encontros e relatos para validar a solução proposta (Santos et al., 2020; Lewrick et al., 2020). Sendo todas as etapas cruciais para o desenvolvimento de soluções educativas mais eficazes e ajustadas às necessidades reais dos alunos e professores (Santos et al., 2020).

Adaptando-se à empatia profunda, implementando ideias práticas por meio de prototipagem e *feedback* contínuo do processo de teste, tal como destacado por Lewrick et al. (2020), o *Design Thinking* afirma-se como uma arma poderosa para a inovação amplificada pelas contribuições tecnológicas e teóricas discutidas por Chang et al. (2022) e Barragem (2024), que exploram o efeito virtual (VR) no processo de *Design Thinking* e criatividade.

Chang et al. (2022) demonstram como a Realidade Virtual (VR) pode intensificar a empatia e a criatividade durante o processo de *design*, possibilitando aos alunos experiências imersivas que contribuem para melhoramento da ideação e prototipagem e resultam em soluções mais inovadoras e adaptadas às necessidades reais.

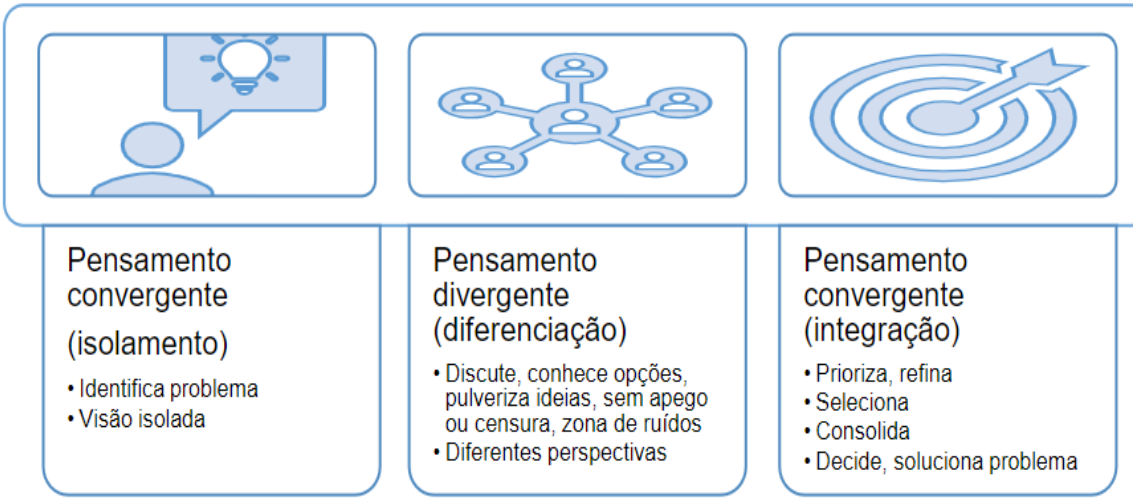
Por conseguinte, combinar a metodologia *Design Thinking* com as inovações tecnológicas, torna-a uma ferramenta mais eficaz para promover uma aprendizagem ativa, criativa, robusta e integrada, fundamental segundo Barragem (2024).

Santos et al. (2020) realizou um estudo em que utilizou a metodologia de *Design Thinking* para identificar e redefinir problemas educativos, mediante abordagem qualitativa. O estudo sustentou-se na observação participativa e em narrações de uma experiência que envolveu alunos, professores, pais e gestores de uma escola privada do Rio Grande do Sul, Brasil, realizado em seis oficinas ao longo de três meses, com encontros quinzenais. Os resultados mostraram um aumento na colaboração, criatividade e satisfação dos participantes, além de fortalecer as relações interpessoais e melhorar a dinâmica do processo educativo. Santos et al. (2020), Apocalypse et al. (2022) e Stumm e Wagner (2019) concordam que a aplicação de metodologias criativas como o *Design Thinking* pode ser uma ferramenta poderosa para transformar as práticas educativas tradicionais, promovendo o desenvolvimento de habilidades cognitivas e sociais, uma educação mais dinâmica, colaborativa e adaptada às exigências do mundo moderno, preparando os alunos para colaborar e inovar no contexto atual.

Entretanto, é importante reconhecer que segundo Panke (2019) o pensamento de *design* tem limitações e pode produzir efeitos negativos quando aplicado à educação: o *Design Thinking* impõe tensões entre o conteúdo do processo de *design* e aprendizagem, podendo tornar este método difícil de aplicar em ambientes educativos; aponta-se, também, a falta de tempo para avaliação completa e crítica das ideias, bem como a ausência de oportunidades de avaliação. Dessa forma, o *Design Thinking*, ao enfrentar esses desafios com uma orientação centrada no aluno e na cooperação, eleva o primeiro e proporciona soluções para problemas complexos, guiando-os para adquirirem habilidades-chave no século XXI. Esse ponto vai ao encontro de Stumm e Wagner (2019), que destaca a empatia como a base do processo de *Design Thinking*, permitindo aos educadores e alunos entenderem-se melhor uns aos outros, resultando em soluções mais eficazes e personalizadas e específicas. O processo de *Design Thinking* opera de maneira direcionada para atender necessidades específicas, conforme exemplificado na figura 3.

Passa por divergências e convergências para as coisas poderem ser compreendidas sob diferentes perspetivas. Neste sentido, é importante distanciar-se, criar muitas ideias, perspetivas diferentes (divergência) e cruzar, escolher e definir (convergência) para alcançar bons resultados. (Rosado & Dias, 2024).

Figura 3 - Processo de pensamento divergente e convergente

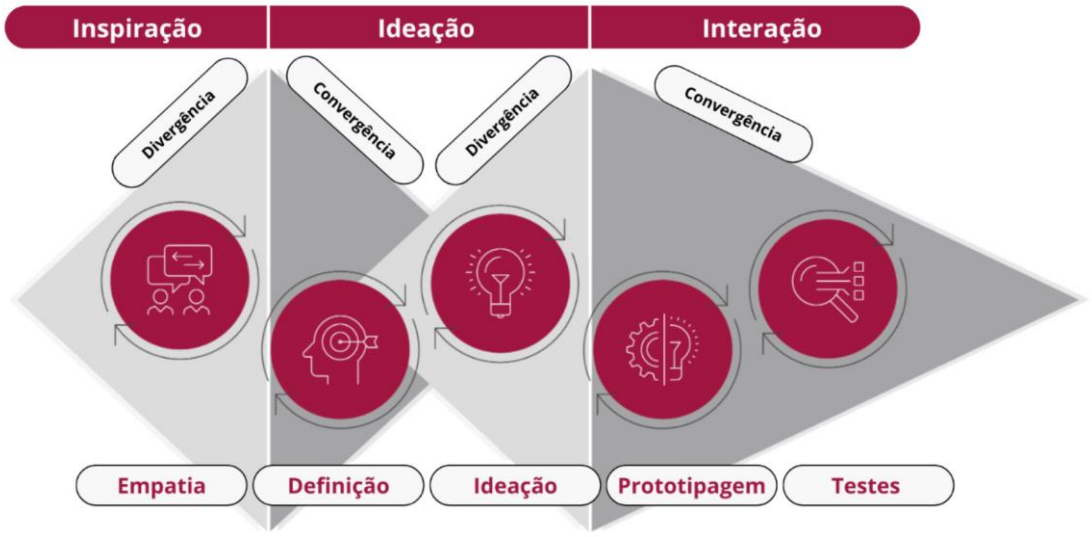


Fonte - Rosado e Dias (2024, p. 9).

Essa metodologia valoriza a voz dos alunos e, também contribui para a formação de cidadãos críticos e autónomos, essenciais para uma comunidade democrática *(Rosado & Dias, 2024)*.

A Figura 4 ilustra as fases do DT:

Figura 4 - Fases do Design Thinking



Fonte – Apocalypse et al. (2022, P. 8)

- **Empatia:** Nesta fase, procura-se compreender as necessidades e inquietações das principais partes interessadas, como alunos, educadores, pais e a comunidade. Pode ser feita por observação direta, entrevistas e trabalhos em contexto de sala de aula, para adquirir conhecimento sobre experiências e desafios, como a segurança cibernética na educação. Segundo Apocalypse et al. (2022), esta fase é decisiva para obter um discernimento holístico dos desafios enfrentados pelos utilizadores.
- **Definição (Define):** Com base nas intuições alcançadas na fase de empatia, definem-se os problemas e momentos relacionados com a segurança *online* na educação. Identificam-se os principais desafios enfrentados pelos alunos, educadores e pais, bem como as lacunas nas abordagens educativas presentes para promover a segurança *online*.
- **Ideação (Ideate):** Nesta fase, gera-se uma vasta gama de soluções criativas para os problemas identificados, que podem incluir brainstorming de estratégias de ensino inovadoras, utilização de recursos educativos *online* interativos e conceção de instrumentos de resolução digital para alunos e professores. O objetivo é criar uma direção clara para o desenvolvimento de soluções. Farias e Mendonça (2021) enfatizam a importância de pesquisar o maior número possível de soluções inovadoras.
- **Prototipagem:** As melhores ideias geradas durante a fase de ideação são usadas para criar protótipos, como recursos educativos *online*, simulações e panoramas de segurança *online*, que são testados e reiterados. Estes protótipos são experimentados e ajustados com base no *feedback* recebido (Rosado & Dias, 2024).
- **Teste:** Finalmente, entrega-se o protótipo aos utilizadores para obter *feedback* e intuições, verificando a eficácia das soluções e identificando pontos fracos, com possibilidade de fazer mudanças se necessário. Isso demonstra a eficácia e flexibilidade das soluções desenvolvidas, ajustadas às necessidades do utilizador.

O primeiro passo na implementação deste processo é identificar um desafio claro, um problema específico e intencional que precisa ser resolvido. Esta definição baseia-se na observação do que pode ser melhorado ou alterado. A partir daí inicia-se a execução das diversas etapas, conforme o Instituto Educadigital (2014) e mencionado na Tabela 2:

Tabela 2 - Processo de Design Thinking para a Educação

Fase	Descrição
Descoberta	Procura-se observar e recolher dados, conhecer o problema e seus objetivos, o grupo envolvido e o contexto no qual está inserido, a fim de provocar a inspiração para a geração de ideias.
Interpretação	As descobertas transformam-se em *insights* valiosos, visando transformá-los em oportunidades de ação, onde são selecionados e condensados, a fim de encontrar uma justificativa convincente para seguir para a fase da ideação.
Ideação	O uso das sessões de *brainstorming* auxilia no pensar expansivo, sem medos podendo render centenas de ideias valiosas. O uso de mapas mentais e de *Post-its* auxiliam nesta fase. É importante também, definir algumas regras como: evitar o julgamento, ser visual, etc., para que a sessão seja focada, eficiente e divertida.
Experimentação	Dá vida às ideias, construindo-se protótipos, tornando tangível aquilo que se pensou, dividindo-se isso com outras pessoas. Isso dá oportunidade de melhorar e refinar a ideia.
Evolução	Tem-se o desenvolvimento do conceito no seu tempo, planeando-se os próximos passos, comunicando com as pessoas que podem auxiliar na execução, documentando-se o processo, com o auxílio de lembretes que mostrem o progresso que se teve ao longo do tempo.

Fonte - Adaptado de Educadigital (2014) por ***(Stumm & Wagner, 2019, pp. 15–16)***

Em consonância, com a tabela 4 do estudo de Stumm e Wagner (2019), o ***Design Thinking*** é uma metodologia inovadora, que está cada vez mais a ser utilizada na educação. Com isso, propicia-se um ambiente de aprendizagem colaborativo e dinâmico. Permite, a priorização das necessidades dos alunos, o estimulo à **empatia** e o incentivo à colaboração no trabalho entre os professores e os alunos, sobretudo na identificação de desafios e na elaboração de soluções criativas e inovadoras.

II METODOLOGIA.

Embora partilhemos e abordemos o conhecimento em segurança na *internet*, concebemos um campo mais amplo de aprendizagem quando se trata de falar sobre este tema problema. Queremos que os alunos se envolvam ativamente no estudo, mas também envolvam a comunidade escolar na totalidade, incluindo os pais. Esta abordagem alargada da matéria visa criar uma rede de apoio ao aluno, ininterrupta entre a escola e a casa. Com o aumento do contacto das crianças com a tecnologia, é importante olhar a eficácia das formas de ensinar no digital. Desta forma, este projeto pretende uma abordagem baseada em quatro pilares principais: consciência, participação ativa de alunos, professores e aprendizagem na comunidade escolar. O foco central é ver como essas abordagens, especialmente em áreas como segurança digital no 1.º CEB podem auxiliar a mudança do ensino tradicional para um ensino baseado em metodologias que permitam a aprendizagem mais ativa e lúdica, com recurso às tecnologias digitais.

Dado que a exposição ao ambiente digital é precoce para muitos alunos, é preciso sensibilizá-los para os problemas relacionados com os riscos digitais e treiná-los para a segurança digital, pelo que se coloca a seguinte questão: **Qual a eficácia das ações voltadas para a alfabetização das habilidades de segurança digital dos alunos do primeiro ciclo?**

Para saber a resposta a esta questão, de modo a assegurar o sucesso das abordagens educativas, é preciso garantir a eficácia das políticas educativas associadas à inovação. Desta forma, este estudo propõe-se a concretizar os seguintes **objetivos específicos**:

i) Identificar as preconceções dos alunos sobre a segurança digital.

ii) Descrever estratégias de integração da segurança digital no 1.º CEB.

iii) Analisar em que medida o envolvimento dos alunos nas atividades de segurança digital contribui para o desenvolvimento de competências.

2.1. CENÁRIO DE INVESTIGAÇÃO E PARTICIPANTES

O projeto ocorreu em duas escolas do 1. º CEB. A primeira escola tem alunos do 1. º CEB e da educação pré-escolar, enquanto a segunda escola inclui alunos do 1. º até o 9.º ano, assim incluindo o 1.º, 2.º e 3.º CEB.

A escola que tem o 1.º CEB e a Educação Pré-Escolar tem boa infraestrutura tecnológica para desenvolver atividades de aprendizagem baseadas em tecnologias digitais, dispondo de uma sala equipada com computadores e projetor, além de outra sala para usar *kits* digitais. Ambas as salas têm bom acesso à *internet* permitindo a boa integração da tecnologia no processo de ensino-aprendizagem.

A segunda escola, que abrange os três níveis do ensino básico, tem *kits* digitais, como parte das ferramentas de ensino, dando aos alunos uma experiência de aprendizagem mais divertida e moderna. Esta escola tem uma sala para usar esses *kits* digitais e também fornece um bom acesso à *internet*.

O projeto incluiu 84 alunos, todos do 4. ano do 1.º CEB, com idades entre 8 e 9 anos. Três turmas do 4.º A, 4.º B e 4.º C, pertencem à escola que inclui alunos do 1.º CEB e Educação Pré-Escolar, enquanto a turma do 4. º D está na segunda escola.

Para salvaguardar a proteção de dados dos alunos, estes foram organizados segundo os seguintes códigos:

4.º A: 23 alunos; identificados pelos códigos 1 a 23.

4.º B: 23 alunos; identificados pelos códigos 24 a 46.

4.º C: 23 alunos; identificados pelos códigos 47 a 69.

4.º D: 15 alunos; identificados pelos códigos 70 a 84.

Entre os 84 alunos 38 são raparigas e 46 são rapazes. Todos tem um nível simples de conhecimento do uso de computadores e outros dispositivos digitais, que vem tanto por meio das atividades normais na escola quanto das vivências pessoais em casa.

O uso dos computadores, dos conjuntos digitais e a boa qualidade das estruturas tecnológicas foram vistas como aspetos chaves para uma aprendizagem mais envolvente e que se encaixa nas exigências do tempo digital.

2.2. TIPO DE ESTUDO E ABORDAGEM INVESTIGATIVA

Neste capítulo, delineamos a abordagem de pesquisa a ser realizada, enfatizando a seleção da estrutura qualitativa para estudo. Esta estrutura é essencial, pois influencia como as informações serão recolhidas, avaliadas e explicadas. O estudo visa compreender perspetivas, pontos de vista e motivações dos participantes por meio de vários métodos, como atividades em sala de aula, discussões, palestras e discussões/debates em grupo. Essas abordagens facilitam a obtenção de *insights* completos e abrangentes sobre comportamentos e ocorrências. O paradigma qualitativo desafia as visões convencionais associadas aos métodos quantitativos, dando prioridade à interpretação, significância e ação para se aprofundar nas experiências reais daqueles que estão sendo estudados.

Enquanto Sátyro e D'Albuquerque (2020) destacam a **flexibilidade na metodologia** de **estudos de caso**, enfatizando a forma como essa abordagem permite o uso de vários métodos para recolher dados, como entrevistas, observações e análise de documentos. Segundo eles, essa diversidade aprimora e enriquece a análise ao permitir uma exploração profunda da complexidade do fenómeno estudado. Isso, por sua vez, leva a conclusões fortes e inferências robustas que podem auxiliar no desenvolvimento da teoria. Filho et al. (2024) abordam o **estudo de caso** sob uma perspetiva educativa, descrevendo-o como uma forma dos alunos analisarem situações reais e resolverem problemas concretos, especialmente em ambientes de grupo. Usar esse método como instrumento pedagógico, ajuda os alunos a aprender fazendo, com foco no pensamento crítico e nas habilidades de trabalho em equipa por meio de experiências práticas com cenários autênticos.

Por um lado, Sátyro e D'Albuquerque (2020) priorizam a adaptabilidade e as habilidades analíticas dos estudos de caso para desenvolver *insights* teóricos e investigar complexidades sociais; por outro lado, Filho et al. (2024) destacam o uso prático de estudos de caso na educação e seu alinhamento com o *Design Thinking* para aprimorar experiências de aprendizagem interativas centradas no aluno. Ambos reconhecem a importância dos estudos de caso, embora para objetivos e cenários distintos: um para investigações sociopolíticas, enquanto o outro para a prática pedagógica inovadora.

Neste contexto, o método de estudo escolhido para o presente trabalho é o estudo de caso, na medida em que se destaca pela sua flexibilidade, permitindo ao investigador modificar os procedimentos de recolha de dados e formular novas perguntas investigativas durante

o processo. Assim, o estudo de caso alinhado com o *Design Thinking* coloca os alunos no centro de todo o processo de inovação, combinando de forma harmoniosa a teoria e aplicação prática, proporcionando a criação de soluções inovadoras e eficientes ao compreender de forma abrangente os requisitos do aluno.

Antes de iniciar o processo formal do *Design Thinking*, uma fase de **diagnóstico inicial** é realizada para identificar as principais questões sobre segurança digital. Como parte deste processo, os alunos utilizam ***Post-its*** para anotar e categorizar os problemas que identificam com o uso da *Internet*.

Após a **identificação dos problemas**, a primeira etapa formal do *Design Thinking*, **empatia**, é crucial para aprofundar a compreensão das necessidades e desafios dos alunos. Para trabalhar esta fase recorrer-se-á à visualização de **vídeos instrucionais**, que apresentam exemplos reais sobre os riscos existentes na *internet*, desempenhando um papel importante na promoção da empatia. Este método visa a sensibilização para os tornar cientes dos perigos digitais, enquanto os ajuda a relacionarem-se emocionalmente com os cenários mostrados, criando uma base de empatia que orientará as fases seguintes do processo.

Após a fase da empatia, a fase de **observação** permite uma análise completa das interações dos alunos com a *internet* nas rotinas diárias, identificando padrões comportamentais e riscos potenciais. Este método interativo facilita a observação direta das respostas e escolhas dos alunos em cenários de segurança digital. Consequentemente, comportamentos de risco e eficácia de conhecimento serão, eventualmente, identificados para abordagem nas fases subsequentes.

No entanto, também trazem riscos notáveis, como tempo excessivo de tela, levando a vários problemas, como alterações de comportamento, distúrbios do sono e desafios de saúde mental. Portanto, é essencial que os pais e educadores entendam esses riscos e incentivem o uso responsável da tecnologia para crianças e adolescentes (Eisenstein, 2023).

Após recolher informações durante os estágios de empatia e observação, a fase que se segue consiste na **definição** dos problemas a serem abordados. Esta etapa é crucial para garantir que as soluções desenvolvidas estivessem alinhadas com as necessidades reais dos alunos. Naturalmente, esse método garante uma definição clara e centrada no aluno com base nas suas necessidades.

Após a identificação dos problemas, a fase de *brainstorming* envolve a criação de resoluções inovadoras. Nessa etapa, a ênfase é colocada na exploração de inúmeras opções para impulsionar a criatividade dos alunos. Essa plataforma permite uma representação clara e tangível de soluções, auxiliando na comunicação eficaz de ideias e na preparação para a fase de **prototipagem**.

Durante esta fase, os conceitos da fase anterior são convertidos em modelos tangíveis para testes práticos. Esses modelos iniciais serão, então, ajustados com base no *feedback* recebido.

Finalmente, a fase de **testagem**, é essencial para confirmar e validar os protótipos. Nesta etapa, os alunos utilizam o ***Nearpod*** (*quiz* interativo) para avaliar a eficácia das soluções na retenção de conhecimento.

A sequência das atividades, alinhada com as etapas do *Design Thinking*, garante programas educativos práticos, acessíveis e flexíveis. Ferramentas *como* ***Post-its***, jogos interativos, questionários *online* e plataformas como ***Canva*** e ***Nearpod*** enriquecem o processo de desenvolvimento, garantindo resultados e soluções finais, bem estruturados e viáveis.

Devido a estas características, o pensamento de *design* é especificamente frutífero para a educação. Isto inclui a capacidade de criar artefactos, prática reflexiva, atividade de resolução de problemas de modo a fazer sentido. Além disso, o pensamento de *design* é aplicado em diferentes contextos educativos, como no desenvolvimento de currículos, como uma abordagem de ensino-aprendizagem e no treino de professores. Ele também se caracteriza por uma série de ferramentas, técnicas e métodos, sendo considerado uma abordagem para o desenvolvimento de habilidades do século XXI (Panke, 2019).

2.3. TÉCNICAS E INSTRUMENTOS DE RECOLHA DE DADOS

Ao elaborar uma metodologia de trabalho, é crucial distinguir entre técnica, como métodos de avaliação, e instrumento, como ferramenta concreta utilizada para implementar técnicas (Cunha et al., 2024). Estas técnicas orientam o processo de recolha de dados e especificam como informações vitais são adquiridas. **Instrumentos** são ferramentas utilizadas para aplicar essas técnicas, incluindo **diários de bordo**, **grelhas de observação** ou **guias de entrevista**.

Para assegurar uma metodologia confiável e explícita, é fundamental selecionar técnicas e ferramentas adequadas que se alinhem com os objetivos da pesquisa.

A **observação direta** facilita a análise do comportamento verdadeiro dos alunos num ambiente de supervisão, mostrando ideias sobre a eficácia das práticas de ensino. Como referem Sølvik e Glenna (2022), os principais desafios na implementação da educação digital no currículo escolar incluem a falta de formação adequada para os professores, resistência à mudança por educadores e alunos, e desigualdade no acesso à tecnologia entre escolas e comunidades diferentes. A prática da **observação participante** detalhada por França et al. (2022) é crucial para as ciências humanas e sociais. Por meio disso, o pesquisador é capaz de ingressar verdadeiramente no quotidiano do ambiente estudado. Não se pode subestimar a pertinência da **observação participante** na investigação educativa. O seu objetivo principal é observar e analisar o comportamento de alunos e Professores com base em situações reais de sala de aula. Assim, através da observação participante, podem-se adquirir dados não só extensos, mas também ricos em qualidade que posteriormente ajudam a elaborar análises detalhadas sobre os fenómenos educativos em estudo no seu contexto específico (Batista et al., 2017).

Neste sentido, a **observação direta** será a técnica predominante, utilizada para conseguir obter informação acerca do envolvimento e comportamento dos alunos em tempo real. A grelha de observação será o instrumento principal para documentar estas atividades, e os dados recolhidos serão analisados para identificar padrões de comportamento seguro *online*.

A **análise documental** é abordada, detalhadamente, por Pereira e Oliveira (2024) como sendo uma técnica valorizada pelos autores, pois oferece um contexto histórico e teórico que ajuda a fundamentar, tanto as observações feitas no estudo da observação participante, como a interpretá-las. A análise dos documentos enriquece a compreensão

dos dados recolhidos, fornecendo um nível de profundidade crucial para uma investigação assaz pertinente. Na presente investigação, o foco da análise recai nos vários trabalhos elaborados pelos alunos no decorrer do projeto.

O **diário de bordo**, de acordo com Hoernig (2021), é fundamental para a avaliação quantitativa e o registo qualitativo, proporcionando um método individualizado pelo qual acrescenta conhecimento à experiência. Sendo o projeto composto por diversas atividades pedagógicas interligadas e orientadas para a promoção da **segurança digital,** os resultados obtidos pelos alunos serão registados num **Diário de Bordo** no *Padlet*, que funcionará como um repositório central para monitorização e reflexão contínua ao longo do projeto.

Grupos focais ou ***focus group*** segundo Sá et al. (2021), são métodos de pesquisa qualitativa que envolvem conversas em grupo sobre um assunto específico, permitindo a recolha de informações aprofundadas dificilmente obtidas através de entrevistas individuais. A execução de um grupo focal necessita de um moderador para direcionar o diálogo com um roteiro predeterminado e também de um observador para documentar as atividades. Os elementos cruciais incluem a quantidade de participantes, o local da discussão e os detalhes das sessões de moderação. Deste modo, os grupos focais desempenham um papel crucial na pesquisa qualitativa, permitindo a exploração completa dos pontos de vista e experiências dos alunos. Em derradeira instância, outras táticas do grupo serão repetidas para garantir que todas as proporções da segurança digital sejam ponderadas, desde a formalidade até a utilização prática na escola.

2.4. TÉCNICAS DE ANÁLISE DE DADOS

A intersecção entre teoria e prática é vital para forjar novas compreensões educativas e fomentar uma educação significativa e holística. Como Farias et al. (2020) evidenciam, a prática reflexiva e o meticuloso tratamento dos dados recolhidos em campo são cruciais para fundamentar e validar o conhecimento científico no contexto educativo. Deste modo, a análise é crucial para estabelecer conexões entre o conhecimento prévio e os *insights* emergentes do estudo, atuando como uma ponte vital no acompanhamento do progresso do aluno. Segundo Francisco et al. (2021), o rigor metodológico na análise de conteúdo e a clareza na interpretação dos dados são decisivos para a qualidade do processo investigativo em educação.

A análise de conteúdo é frequentemente empregue quando os dados recolhidos são **qualitativos**, como no caso de textos, vídeos, expressões ou comportamentos, possibilitando aos pesquisadores interagir diretamente com o ambiente social dos casos sociológicos. Estes eventos têm como objetivo promover debates abertos e críticos sobre questões de ética e privacidade na internet, que são fundamentais para uma alfabetização digital eficaz. Ao dividir dados e reconhecer categorias, permite deduções sobre a criação e receção de informações. Este tipo de análise tem significância na pesquisa, pois facilita a compreensão profunda do assunto que está sendo estudado ao conectar dados factuais com teorias pertinentes, aumentando assim a robustez da análise e a validade dos resultados (Loureiro et al., 2021).

Assim, a **análise de conteúdo** será a técnica de eleição para categorizar e interpretar os dados qualitativos recolhidos. Reflexões e discussões estruturadas, como a **Discussão de Estratégias de Segurança** e a **Discussão sobre Comportamentos Seguros nas Redes Sociais**, permitirão aos alunos explorar e consolidar as suas práticas seguras *online*, enquanto a análise de conteúdo fornecerá uma visão profunda sobre a eficácia dessas reflexões. Para facilitar a expressão dos conhecimentos adquiridos, ferramentas digitais como o ***Mentimeter*** e o ***Canva*** serão incorporadas, permitindo aos alunos criar conteúdos digitais, como **nuvens de palavras** e ***posters***, que serão analisados para avaliar a sua compreensão da segurança digital.

Em resumo, todas as atividades do projeto serão analisadas através de uma combinação de técnicas de observação e análise de conteúdo, com o objetivo de fornecer uma visão detalhada e integrada da eficácia das estratégias pedagógicas implementadas.

2.5. QUESTÕES ÉTICAS

A relevância da ética na área educativa está ligada à manutenção da harmonia e do equilíbrio social no ambiente escolar. Biombe (2023) sustenta que a ética é um conjunto de princípios que norteiam como as pessoas de um grupo social se comportam e agem, sendo crucial para assegurar um comportamento adequado e legal, incluindo o respeito pelos direitos alheios. A metodologia garante confidencialidade, privacidade dos participantes, coincidente com os padrões éticos estabelecidos pela comunidade académica e pela legislação em vigor, as pessoas em última análise devem ser protegidas.

O processo começa com uma carta dirigida à Diretora do Agrupamento de Escolas, onde se explicita o âmbito da investigação, os seus objetivos específicos e o método proposto (ANEXO A).

Após obtenção de permissão institucional, esclarecem-se os participantes e os pais. A carta de informação do estudo (ANEXO B), detalhada e acessível, distribuída aos pais, enfatiza a natureza voluntária da participação e o direito de qualquer pessoa poder sair do estudo em qualquer altura, sem penalização. A confidencialidade dos dados foi garantida pelo anonimato de todos os alunos intervenientes e os dados pessoais tratados com descrição máxima, apenas acessíveis à professora de investigação e sob estreita vigilância no que toca à segurança do computador.

Os instrumentos de recolha de dados, artefactos produzidos pelos alunos, observações em sala de aula, notas de campo e cadernos - foram cuidadosamente escolhidos para criar um ambiente onde os participantes se sentissem à vontade e fossem respeitados na sua privacidade. Os artefactos dos alunos, informações valiosas sobre a sua compreensão e atitudes tomadas no domínio da segurança digital, são recolhidos e analisados no segredo absoluto para que os seus contributos pudessem revisitar sem revelar de quem eram os proprietários. As notas de campo registadas em diário de bordo e grelhas, mantidas pelos investigadores, foram registos fidedignos de interações, reflexões e desenvolvimento dos alunos ao longo do projeto, e fundamentais para a análise e interpretação do material recolhido.

Como conclusão dos trabalhos, todas as informações foram arquivadas segundo regras de confidencialidade e apenas os resultados agregados e despersonalizados foram utilizados para a redação do projeto e eventuais publicações ou apresentações, daí a proteção contínua dos dados dos participantes.

III DESCRIÇÃO DO PROJETO

Ao longo deste capítulo, será apresentado o projeto de investigação que se insere no domínio da Cidadania Digital, focado na promoção de uma navegação segura e direcionado para alunos do 4.º ano, durante o ano letivo 2023/2024, distribuídos de acordo a tabela 3:

Tabela 3 - Caracterização da turma

Ano	9 anos		10 anos		11 anos		12 anos		**Total**
Turma	Rapazes	Raparigas	Rapazes	Raparigas	Rapazes	Raparigas	Rapazes	Raparigas	
4.º A	12	7	1	3	0	0	0	0	**23**
4.º B	9	7	4	1	1	0	1	0	**22**
4.º C	6	10	4	2	1	0	0	0	**22**
4.º D	6	8	1	0	0	0	0	0	**15**
Total	**33**	**30**	**10**	**6**	**2**	**0**	**1**	**0**	**82**

Assim, o projeto tem como objetivos operacionais:

- introduzir práticas seguras durante a navegação na *Internet*;
- aumentar a consciência sobre a segurança digital;
- envolver os alunos em atividades interativas que ajudem a consolidar o que aprenderam.

Para além dos objetivos operacionais, pretende-se, com este projeto, dar resposta aos objetivos de investigação, nomeadamente: 1) **identificar as preconceções dos alunos sobre a segurança digital**, através de uma atividade de diagnóstico dos conhecimentos que os alunos têm, o que permitirá; 2) **descrever estratégias de integração da segurança digital no 1.º CEB**, as quais serão apresentadas sinteticamente no ponto seguinte 'Atividades de Segurança na Internet' e que, na apresentação de resultados, serão aprofundadas considerando a participação dos alunos, para que seja possível; 3) **analisar em que medida o envolvimento dos alunos nas atividades de segurança digital contribui para o desenvolvimento de competências** previstas nos instrumentos enquadradores de referência – Perfil dos Alunos à Saída da Escolaridade Obrigatória (Martins et al., 2017) e Aprendizagens Essenciais.

Atividades de Segurança na Internet

A sequência de atividades sobre segurança na Internet para os alunos do 4.º ano foi desenhada seguindo os princípios do *Design Thinking*, para que seja eficaz e, também divertida, considerando as características, necessidades e interesses dos alunos envolvidos.

Após a descrição de cada atividade é possível encontrar a referência ao respetivo ANEXO de: a) planificação de aula, com a identificação com os domínios educativos a explorar, as áreas de competência a desenvolver, as ações/estratégias/Atividades, a respetiva duração, os recursos a utilizar e a forma de avaliação; b) de análise de conteúdo relativa à implementação da atividade.

Diagnóstico inicial

Objetivo: Criar curiosidade nos alunos e identificar lacunas no conhecimento.

Descrição: O primeiro passo é o diagnóstico inicial, no qual a professora estabelece uma conexão com os alunos e tenta entender o que eles já sabem sobre segurança na *Internet*. Este processo é um dos mais importantes, para a maioria dos alunos, pois pode criar curiosidade, ao passo que a professora pode encontrar as lacunas nos conhecimentos relativos à segurança na internet, já que o diagnóstico ajuda a perceber os conhecimentos que os alunos possuem. Esta atividade foi posta em prática com o uso de ***Post-its***, com vista a identificar o que os alunos sabem sobre os perigos da *internet*, gerar discussão e reflexão sobre a temática. Com esta atividade, pretende-se desenvolver competências relativas ao pensamento crítico e criativo; de informação e comunicação; e de relacionamento interpessoal.

ANEXOS associados à atividade:

- ANEXO C - Planificação da Aula – Tema: Atividade com ***Post-its***
- ANEXO C1 - Grelha de Análise de Conteúdo - Tema: Atividade com ***Post-its***

Pesquisa e consciencialização

Objetivo: Adquirir conhecimento teórico sobre cidadania digital e áreas perigosas.

Descrição: Após a análise dos resultados do diagnóstico, continua-se com a fase de pesquisa e consciencialização. Neste passo a professora ensinará os alunos a procurar informações na *internet* de maneira segura, com o intuito de adquirirem conhecimento teórico sobre a cidadania digital e áreas perigosas, (*phishing*, *cyberbullying* e proteção de

dados). Este conhecimento é fundamental, pois ajudará os alunos a aplicá-lo em situações práticas futuras. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de pensamento crítico e criativo; de linguagens e textos; e de relacionamento interpessoal.

ANEXOs associados à atividade:

- ANEXO D - Planificação da Aula – Tema: Pesquisa na *Internet*
- ANEXO D1 - Grelha de Análise de Conteúdo - Tema: Pesquisa na *Internet*

Interação e jogos

Objetivo: Manter os alunos atentos e envolvidos, consolidando as aprendizagens adquiridas.

Descrição: Com a forte base teórica, prossegue-se com a etapa de interação e jogos. Os jogos são muito divertidos para os alunos porque ajudam a transformar a sabedoria teórica em experiências práticas. Isso ajudará os alunos a manterem-se atentos e envolvidos, enquanto estão a consolidar as aprendizagens adquiridas. Tal como refere Eisenstein (2023) os jogos *online* são uma parte importante da vida dos jovens, oferecendo diversão e interação social. No entanto, também apresentam riscos como vício, problemas de comportamento e saúde mental. A OMS considera o vício em *videogames* uma preocupação séria, alertando para os perigos de certos jogos e reconhecendo os transtornos relacionados como condições capazes de gerar dependência, refletindo a sua atenção aos riscos envolvidos (Almeida et al., 2020). É crucial que pais e educadores promovam o uso responsável da tecnologia. Assim, para compreender a relação entre os conhecimentos obtidos e a aplicação em prática, pretende utilizar o jogo 'Segurança na *Internet'* da *SeguraNet*. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de relacionamento interpessoal; de linguagens e textos; e de pensamento crítico e criativo.

ANEXOs associados à atividade:

- ANEXO E - Planificação da Aula – Tema: Jogo de segurança na *internet*
- ANEXO E1 - Grelha de Análise de Conteúdo - Tema: Jogo de segurança na *internet*

Vídeos e discussões

Objetivo: Promover reflexão e discussão para aprofundar o entendimento.

Descrição: Para fortalecer a experiência prática, pretende-se exibir vídeos que permitam aos alunos discutirem temáticas em grupo. Esta atividade permitirá reflexão sobre o que acabaram de ver e a discussão em grupo, seguindo-se a partilha das experiências, conclusões e as lições aprendidas. Desta forma, serão partilhados vídeos educativos da plataforma *SeguraNet* sobre a temática da segurança na *internet*. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de relacionamento interpessoal; de linguagens e textos; e de pensamento crítico e criativo.

ANEXOs associados à atividade:

- ANEXO F - Planificação da Aula – Tema: Visualização de vídeos
- ANEXO F1 - Grelha de Análise de Conteúdo - Tema: Visualização de vídeos

Uso do *Mentimeter*

Objetivo: Tornar as aulas mais interativas e permitir a aquisição de mais conhecimento sobre segurança *online*.

Descrição: Para deixar as aulas mais interativas, o *Mentimeter* é utilizado nas aulas, para que os alunos adquiriram mais conhecimento sobre o tópico, mediante o uso de nuvens de palavras, de forma a precaverem-se dos riscos e perigos, enquanto navegam pela *internet*. Neste sentido, os alunos fazem uma pesquisa, através de *sites* fidedignos e utilizando a navegação anónima, com vista a elaborarem uma lista de perigos *online*, sistematizarem a informação e criarem uma nuvem de palavras e colocarem no *Google Docs*. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de pensamento crítico e criativo; de linguagens e textos; de relacionamento interpessoal; de saber científico técnico e tecnológico; e de sensibilidade estética a artística.

ANEXOs associados à atividade:

- ANEXO K - Planificação da Aula – Tema: *Mentimeter*
- ANEXO K1 - Grelha de Análise de Conteúdo - Tema: *Mentimeter*

Criação de *posters* digitais

Objetivo: Oferecer aos alunos uma oportunidade para mostrar o seu conhecimento de forma tangível e concreta.

Descrição: Na fase da aplicação, pretende-se incentivar os alunos a utilizar os conceitos por meio da criação de posters digitais no ***Canva*** sobre segurança *online*. A atividade oferece aos alunos uma oportunidade para 'mostrarem' o seu conhecimento, sendo o processo de aprendizagem tangível e concreto. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de pensamento crítico e criativo; de linguagens e textos; e de relacionamento interpessoal.

ANEXOs associados à atividade:

- ANEXO L - Planificação da Aula – Tema: Criação visual no *Canva*
- ANEXO L1 - Grelha de Análise de Conteúdo - Tema: Criação visual no *Canva*

Quizzes interativos

Objetivo: Avaliar o conhecimento dos alunos de forma competitiva e divertida, identificando áreas que precisam ser melhoradas.

Descrição: Após a criação do poster digital, pretende-se que os alunos consolidem o conhecimento por meio de *quizzes* interativos no *Nearpod*. Esta ferramenta digital facilita a avaliação e fornece um *feedback* imediato sobre as aprendizagens adquiridas, desta forma reforçam os conhecimentos, de forma competitiva e divertida. Com esta atividade, pretende-se o desenvolvimento de competências associadas a Saber científico, técnico e tecnológico que implicam que os alunos sejam capazes de: compreender processos e fenómenos científicos que permitam a tomada de decisão e a participação em fóruns de cidadania (Martins et al., 2017, p. 29), relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; e de pensamento crítico e criativo.

ANEXOs associados à atividade:

- ANEXO M - Planificação da Aula – Tema: *Nearpod*
- ANEXO M1 - Grelha de Análise de Conteúdo - Tema: *Nearpod*
- ANEXO M1 – Perguntas frequentemente respondidas incorretamente no *Quiz Nearpod*

Dia Internacional da Internet Segura

Objetivo: Consciencializar os alunos sobre os perigos *online* e conectá-los com especialistas para aprenderem a proteger-se de situações de perigo da vida real.

Descrição: A presente atividade 'Dia Internacional da *Internet* Segura' pretende contribuir para o aumento de conhecimentos dos alunos, relativamente à segurança na *internet*, através de testemunhos de profissionais da Guarda Nacional Republicana (GNR) e da experienciação de cenários de risco. Desta forma, com a GNR, professores das turmas e da AEC de TIC os alunos são expostos, de forma segura, aos perigos que podem ocorrer *online* experienciando situações de perigo *online* da vida real. Com esta atividade, pretende-se desenvolver competências relativas à informação e comunicação; Raciocínio e resolução de problemas; Relacionamento Interpessoal; e Linguagens e textos.

ANEXOs associados à atividade:

- ANEXO N - Planificação da Aula – Tema: Dia Internacional da Internet Segura (GNR)
- ANEXO N1 - Grelha de Análise de Conteúdo - Tema: Dia Internacional da Internet Segura (GNR)

Direitos digitais: A voz das crianças na Internet

Objetivo: Permitir que os alunos adquiram conhecimento abrangente e prático sobre segurança na *internet*, integrando a aprendizagem de forma clara e sucinta.

Descrição: Nesta atividade, a metacognição, a reflexão e o debate são incentivados para que os alunos sejam capazes de processar, sozinhos, o que aprenderam ao longo do projeto. Com esta atividade, pretende-se desenvolver competências relativas ao desenvolvimento pessoal e autonomia; de informação e comunicação; de pensamento crítico e criativo; de linguagens e textos; e de relacionamento interpessoal.

ANEXOs associados à atividade:

- ANEXO O - Planificação da Aula – Tema: Direitos Digitais: A Voz das Crianças na *Internet*
- ANEXO O1 - Grelha de Análise de Conteúdo - Tema: Direitos Digitais: A Voz das Crianças na Internet

Explorando a Segurança Digital: Comprovando conhecimentos na Prática

Objetivo: Capacitar os alunos a reconhecer e utilizar práticas seguras na *internet*, promovendo uma compreensão prática e abrangente dos princípios de segurança digital.

Descrição: A tarefa envolve aprimorar habilidades práticas relacionadas com segurança cibernética usando reflexão e discussão de metacognição. A sessão começa enfatizando

a importância da segurança *online*, para uma tarefa em que cada aluno preenche um questionário do *Google Forms* sobre práticas seguras *online*. Após a recolha de dados, os alunos participam em grande grupo para determinar comportamentos seguros e explorar maneiras de implementar essas práticas diariamente. Em última análise, a realização desta atividade deseja desenvolver competências referentes ao desenvolvimento pessoal e autonomia; de informação e comunicação; de pensamento crítico e criativo; de linguagens e textos; e de relacionamento interpessoal.

ANEXOs associados à atividade:

- ANEXO P - Planificação da Aula – Tema: Formulário Avaliação da Eficácia das Atividades
- ANEXO P1 – Análise descritiva – Tema: Avaliação da Eficácia das Atividades
- ANEXO P2 – Análise descritiva – Tema: Avaliação da Eficácia das Atividades

Questionário Demonstração de Conhecimentos sobre Segurança Digital

Objetivo: Avaliar de forma prática o conhecimento dos alunos sobre segurança na internet, reforçando o pensamento crítico e a capacidade de refletir sobre o que foi aprendido.

Descrição: ao longo da realização das atividades, os alunos responderam a diversas questões, abordando situações relacionadas com segurança *online*. As respostas dos alunos foram utilizadas para fomentar debate e reflexão em grupo, onde discutiram as melhores práticas e estratégias para navegar de forma segura na *internet*. Este trabalho reforçou competências em pensamento crítico, autonomia, comunicação e trabalho em grupo.

ANEXOs associados à atividade:

- ANEXO Q - Questionário – Questionário – Tabela de Correspondência de Respostas dos Alunos sobre Práticas de Segurança Digital
- ANEXO Q1 – Questionário: Tabela de Correspondência de Respostas dos Alunos sobre Práticas de Segurança Digital

Aplicação Estruturada do Design Thinking nas atividades desenvolvidas

No contexto do ***Design Thinking*** aplicado à educação, as atividades desenvolvidas ao longo do processo foram cuidadosamente estruturadas para orientar os alunos desde a perceção inicial dos problemas até a aprovação das soluções.

O procedimento começou com atividades como a **Consciencialização Inicial**, em que os alunos partilharam experiências pessoais e reflexões sobre a segurança digital. Essas atividades, ocorreram ao longo de várias aulas, incluindo: **Atividade com *Post-its***, **Pesquisa - Perigos na Internet**, **Jogo de Segurança na *Internet***, **Visualização de Vídeos**, ***Mentimeter***, **Criação Visual no *Canva***, ***Nearpod***, **Dia Internacional da *Internet* Segura (GNR)**, **Direitos Digitais: A Voz das Crianças na Internet** e **Explorando a Segurança Digital: Comprovando Conhecimentos na Prática**. Essas práticas foram essenciais para captar as perceções dos alunos e estabelecer uma base empática, orientando as etapas conforme defendido por Stumm e Wagner (2019) e Lewrick et al. (2020).

As atividades acima mencionadas focaram-se na estruturação dos *insights* obtidos, permitindo que os alunos consolidem as informações necessárias para uma clara definição dos desafios, conforme mencionado por Rosado e Dias (2024).

A geração de ideias criativas ocorreu através de **Discussão em Grupo** e a **Apresentação dos Resultados**, que facilitaram o processo de resolução. A **Atividade no *Mentimeter*** ajudou a condensar ideias e refletir sobre preocupações comuns, encorajando a inovação, como sublinhado por Farias e Mendonça (2021).

Transformar essas ideias em protótipos tangíveis, foi realizado através de atividades como a **Criação Visual no *Canva*** e ***Mentimeter***. Estas atividades permitiram aos alunos materializarem as suas ideias e prepararem-se para testes e refinamentos, de acordo com Pande e Bharathi (2020).

O processo culminou com a avaliação e o refinamento das soluções baseados no *feedback*, realizado na **Atividade com *Post-its***, **Jogo de Segurança na *Internet*** e ***Nearpod***. Estas etapas garantiram que as soluções desenvolvidas fossem eficientes e refletissem as necessidades reais dos alunos, como defendido por Lewrick et al. (2020) e Chang et al. (2022).

As atividades cobriram todas as fases do *Design Thinking*, desde a compreensão inicial dos problemas até à avaliação de soluções. Assim, o *Design Thinking* transformou-se numa ferramenta preponderante para modernizar a educação, preparando os alunos para enfrentar os desafios do mundo digital de forma crítica e inovadora.

IV APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

Para que um recurso pedagógico alcance a sua finalidade, é preciso garantir o rigor científico e ser atrativo. A criação de um recurso precisa ter como fundamento a promoção de aprendizagens num contexto específico, contribuindo efetivamente para a qualidade e o sucesso educativo (Abreu et al., (2018).

Com base nestes princípios, neste estudo, foi gerada e executada uma sequência de atividades estratégicas, procedimentos e planos delineados para se alinharem com os objetivos definidos no projeto, no empenho e no envolvimento dos alunos.

Após a conclusão dos trabalhos, os alunos submeteram-nos na plataforma *Classroom*, a qual, permitindo a partilha digital, facilitando o debate e *feedback*, servindo, também, como um espaço de *feedback* contínuo e de avaliação, parte integral do processo de *Design Thinking*.

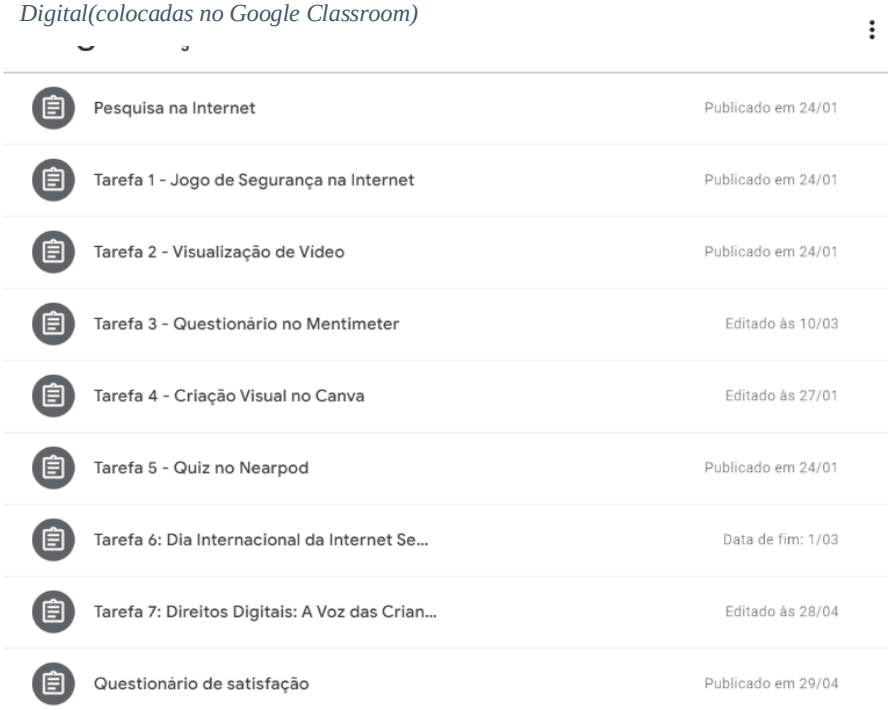
As atividades relacionadas com a segurança digital estão organizadas e disponibilizadas no ***Padlet*: https://padlet.com/mariaelisaborges/di-rio-de-bordo-uizzhuqhggncynzw**. O *Padlet*, é um diário interativo, facilita o acesso aos materiais educativos. É uma plataforma prática e acessível que incentiva a interação do utilizador e que promove a aprendizagem contínua em segurança digital.

4.3. ESTRATÉGIAS DE INTEGRAÇÃO DA SEGURANÇA DIGITAL EM SALA DE AULA

A segurança digital deve ser integrada na sala de aula através de estratégias que envolvam a segurança dos alunos de forma ativa e lúdica, garantindo proteção no ambiente. Dada a resposta positiva dos alunos e a análise da literatura, foram refletidas estratégias mais apropriadas para incluir o tema da segurança digital em sala de aula. As estratégias escolhidas foram interativas, participativas e lúdicas, envolvendo ativamente os alunos no processo de aprendizagem (Chicava & Nhanombe, 2020; Farias et al., 2019; Freitas et al., 2023; Moro, 2021; Tavares & Melo, 2019).

A Figura 5 apresenta a lista de atividades, que serão explicadas de seguida.

Figura 5 Organização das Atividades de Segurança Digital(colocadas no Google Classroom)



4.3.1. PODER DOS POST-ITS: FERRAMENTAS SIMPLES PARA GRANDES IDEIAS

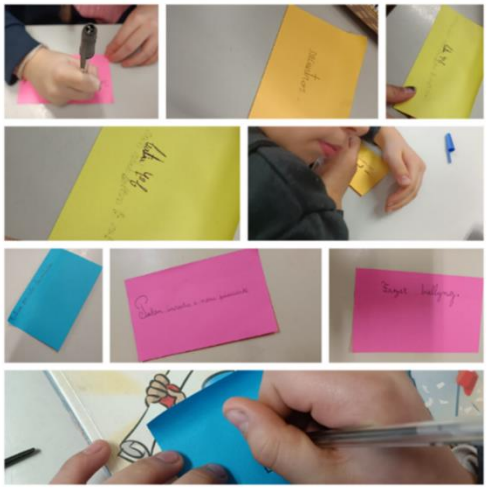
Para começar foi realizado um **Diagnóstico** para identificar as ideias pré-concebidas dos alunos sobre segurança cibernética. Os alunos utilizaram *Post-its* para identificarem e compartilharem as perceções iniciais sobre vulnerabilidades *online*, que foram organizadas por temas (Figura 6). Esse método visual colaborativo auxiliou a recolha de dados e o desenvolvimento de estratégias (ANEXO C). Os alunos discutiram temas como *phishing*, *cyberbullying* e *malware*. Alguns alunos demonstraram perceção limitada com riscos mais complexos, como *spyware*, *ransomware* e roubo de identidade, o que evidenciou uma disparidade no conhecimento.

Os principais riscos identificados foram: *phishing*, *cyberbullying*, *malware*, *spyware*, *vírus*, *ransomware*, *hacking*, roubo de identidade, fraudes *online* e exposição a conteúdo inadequado (Figura 6). Assim, os riscos variam entre *phishing*, que envolve o roubo de dados a *malware* que compromete a segurança dos dispositivos. A exposição a conteúdo inadequado destaca a necessidade de filtros e controles parentais.

Posteriormente, os alunos colaboraram no **Agrupamento de Palavras-Chave** (Figura 7), no qual organizaram os termos-chave em categorias ligadas aos riscos *online* (ANEXO C1). Essa dinâmica promoveu compreensão das ameaças digitais e uma discussão sobre segurança *online*. Esses riscos foram agrupados em categorias, como fraude eletrónica

(*phishing*, roubo de identidade, fraudes *online*) e ameaças ao *software* e *hardware* (*malware*, *spyware*, *vírus*, *ransomware*).

*Figura 6 - Sessão de Diagnóstico com **Post-its***



*Nota - Alunos do 4.º ano participam numa atividade de identificação de perigos online, utilizando **Post-its** para registar riscos.*

Figura 7 - Agrupamento de Palavras-Chave

Nota - Alunos organizam palavras-chave identificadas em temas relacionados a perigos online no quadro branco.

Conforme sugerido por Rosado e Dias (2024), os alunos utilizaram métodos de *brainstorming* e técnicas criativas para debater e compreender os problemas identificados, desenvolvendo habilidades de pensamento crítico. A Tabela 4 sintetiza os resultados, destacando os principais perigos apontados, áreas de melhoria e necessidades de suporte identificadas nas diferentes turmas envolvidas.

Tabela 4 - Desempenho dos Alunos na Pesquisa sobre Perigos na Internet

Turma	Principais Perigos Identificados	Alunos com Maior Participação	Áreas de Melhoria	Alunos a Necessitar de Suporte
4º A (1-23)	*Phishing*, *Cyberbullying*, *Malware*, *Spyware*, *Sexting*, Vírus	Al 5, Al 12, Al 20, Al 21	*Grooming*, Engenharia Social	Al 17, Al 18, Al 19, Al 22
4º B (24-46)	Vírus, *Phishing*, *Ciberbullying*, Golpes	Al 25, Al 32, Al 33, Al 36	*Doxxing*, *Sexting*	Al 44, Al 45, Al 46, Al 39
4º C (47-69)	Exposição a Conteúdos	Al 50, Al 57, Al 60, Al 63	*Phishing*, *Grooming*	Al 67, Al 68, Al 69, Al 62

Turma	Principais Perigos Identificados	Alunos com Maior Participação	Áreas de Melhoria	Alunos a Necessitar de Suporte
	Impróprios, *Sexting*, *Happy Slapping*			
4º D (70-85)	*Cyberbullying*, *Grooming*, *Sexting*, Vírus	Al 72, Al 79, Al 82, Al 85	Abuso Sexual, Predadores Virtuais	Al 70, Al 71, Al 73, Al 76

Houve diferenças no nível de compreensão, com alguns alunos mais familiarizados com termos como *phishing* e *malware* e outros precisando de mais suporte para ameaças mais complexas. Isso evidenciou a necessidade de mais aprendizagem para equilibrar o nível de conhecimento. Alunos mais velhos (11 anos), mostraram um entendimento mais profundo dos perigos *online.* Os alunos que mencionaram termos como roubo de dados ou *software* malicioso demostram um grau de conhecimento sobre os perigos da *Internet*. Contudo, essa consciência pode ser superficial ou restrita. A compreensão limitada tornou-se mais clara na tarefa, quando os alunos identificaram e classificaram riscos comuns, mas encontraram dificuldades ao analisar e investigar assuntos mais elaborados.

A utilização de *Post-its* foi fundamental para organizar as etapas seguintes, facilitando a identificação das perceções iniciais. Alunos, como **Al 20** e **Al 33**, mostraram um bom domínio de conceitos essenciais, como a relevância de senhas robustas e a verificação da segurança em páginas na *internet*. Já outros, como **Al 6** e **Al 52**, focaram-se nos perigos do *malware* e *hacking*.

O estudo também mostrou que certos alunos ainda encontram obstáculos ao lidar com ameaças menos populares, como *ransomware* e *spyware*, reforçando a necessidade de intervenções educativas mais específicas (ANEXO C).

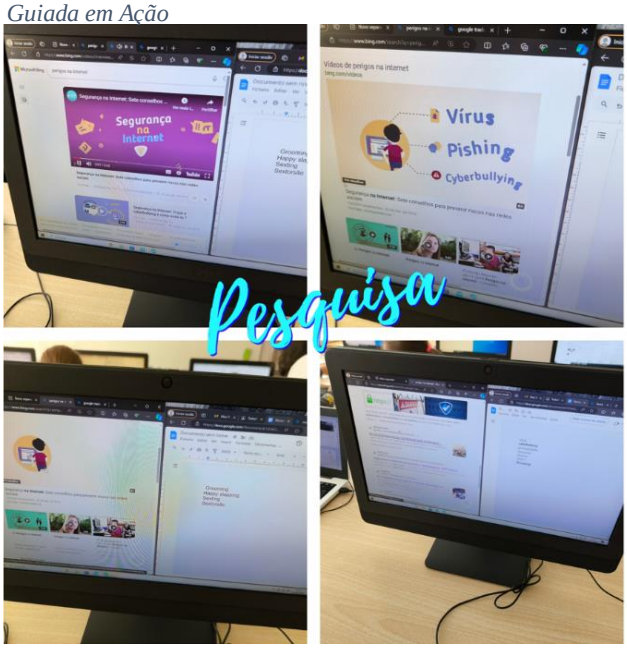
A tarefa permitiu constatar que alunos, com 9 e 10 anos, revelaram uma habilidade mais avançada para generalizar e abstrair conceitos, enquanto, os mais jovens, 8 anos, precisaram de mais apoio para compreender as relações entre diferentes riscos. Esses dados foram essenciais, independentemente do nível inicial, para assegurar que todos progrediam na compreensão das técnicas de proteção *online*.

A avaliação dos resultados obtidos na atividade com *Post-its* mostra que os alunos identificaram diferentes ameaças *online*, revelando bom conhecimento dos principais riscos. Por exemplo, o **Al 5** identificou o *phishing* como uma ameaça significativa, enquanto o **Al 12** destacou o *cyberbullying*. A organização por temas, mostrou preocupação comum em relação à privacidade *online* e à segurança de dados, como evidenciado pelo **Al 12** e **Al 33**, que ressaltaram a importância de proteger informações pessoais. A conversa em grupo revelou consciência sobre práticas seguras, com o **Al 20** declarando que **nunca compartilha suas senhas** e **Al 60** enfatizando a necessidade de **utilizar antivírus** para prevenir *malware* e *vírus*. Estes resultados demonstram boa compreensão sobre as ameaças digitais e as medidas de segurança necessárias, destacando a eficácia da atividade em promover a consciencialização para a segurança *online*.

4.3.2. PESQUISA NA INTERNET

A aula sobre **Pesquisa na *Internet*** (ANEXO D) apresentou noções fundamentais de segurança digital, usando exemplos simples para facilitar a compreensão, como *phishing*, *cyberbullying* e *malware (Figura 8)*. A professora destacou a importância de proteger a privacidade *online*, utilizando ferramentas como Modo Privado, Janela Anónima e *DuckDuckGo*. Após a explicação, os alunos foram encorajados a conduzir suas próprias pesquisas utilizando tais ferramentas. Deste modo, aprimoraram habilidades de pesquisa, destacando a relevância da privacidade na era digital (ANEXO D1).

Figura 8 - Explorando a Segurança na Internet: Pesquisa Guiada em Ação



A análise geral dos resultados da pesquisa *online*, revelou uma gama diversificada de perspetivas dos alunos sobre riscos *online* e medidas de segurança digital. Alguns alunos exibiram uma compreensão sólida de riscos específicos, como, *phishing* *malware* e vírus, reconhecendo o potencial de danos. Esses avanços confirmam a relevância de uma formação que os capacite a reconhecer e mitigar riscos, como defendido por Mattar et al. (2020).

No que diz respeito à privacidade *online*, **Al 25** mencionou a importância da proteção de dados, enquanto **Al 36** destacou os perigos associados ao *Hacking* e a necessidade de proteger dispositivos contra acessos não autorizados. Essas considerações refletem os princípios defendidos pelo projeto *SeguraNet* em Portugal e a necessidade de educar alunos sobre proteção cibernética desde cedo (Pereira & Moura, 2022). Segundo a UNESCO (2017) é fundamental incluir competências digitais na educação para preparar os alunos para os desafios do século XXI (Mesquita et al., 2022) .

Os alunos refletiram sobre práticas *online* seguras. O **Al 25** destacou a importância de compartilhar essas informações com a família para promover comportamentos seguros. Segundo Batista (2019) e Mattar et al. (2020) a participação ativa dos alunos ressalta a eficácia das propostas educativas em proteção digital, demonstrando como podem auxiliar no desenvolvimento de competências digitais. Essa interação, como destacada por ambos os autores, fortalece o envolvimento dos alunos e promove uma maior consciencialização sobre comportamentos seguros no ambiente *online*, tanto na escola quanto em casa.

A Tabela 5, resume os conceitos-chave aprendidos. Os alunos demonstraram compreensão das principais ameaças digitais e começaram a incorporar esse conhecimento nas atividades diárias, o que é fundamental para a construção de cidadãos digitais capacitados e conscientes. Segundo Mattar et al. (2020) a preparação para enfrentar os obstáculos de uma sociedade em constante transformação digital é essencial.

Tabela 5 - Descrição dos Conceitos relacionados som a segurança online

Conceitos relacionados com a segurança *online*	**Descrição feita pelos alunos**	**Código Al**
Phishing	Quando alguém tenta enganar-nos para partilharmos informações pessoais, como senhas, fingindo ser uma pessoa em que confiamos.	Al 5, Al 21, Al 25
Cyberbullying	Quando alguém nos trata mal na *internet*, dizendo coisas más ou fazendo pouco de nós.	Al 12, Al 32
Malware	Programas prejudiciais que podem danificar o nosso computador ou roubar informações.	Al 20, Al 33

Conceitos relacionados com a segurança *online*	Descrição feita pelos alunos	Código AI
Spyware	Software usado por espiões para roubar informações sem que saibamos.	AI 21
Vírus	Programas que se espalham e causam danos ao computador.	AI 22
Ransomware	Software que bloqueia o acesso ao computador até pagarmos um resgate.	AI 36
Hacking	Quando alguém invade o nosso computador sem permissão.	AI 36
Golpes *Online*	Fraudes para roubar dinheiro ou informações.	AI 57
Catfishing	Quando alguém finge ser outra pessoa para nos enganar.	AI 79
Invasão de Privacidade	Quando alguém acede às nossas informações pessoais sem permissão.	AI 25
Sexting	Enviar mensagens ou fotos sexualmente explícitas.	AI 63
Pornografia Infantil	Conteúdo sexual envolvendo crianças, que é ilegal e prejudicial.	AI 79

No decorrer da análise dos dados, **AI 25** destacou a importância da proteção da privacidade e segurança de dados pessoais. A UNESCO (2017), também salienta a relevância da consciencialização sobre a privacidade e a proteção de dados pessoais nas habilidades essenciais para o século XXI. Por outro lado, aspetos de **segurança cibernética**, que não mencionados diretamente, foram discutidos por outros alunos. O **AI 36** e o **AI 57** destacaram a necessidade de proteger os dispositivos com antivírus e defender os computadores contra ataques de *hacking*. Ambos mostraram compreender as medidas de segurança necessárias para garantir a proteção das atividades *online.* De acordo com o referido por Mattar et al. (2020) tais iniciativas são fundamentais para a segurança individual e coletiva numa sociedade cada vez mais conectada.

No decorrer da análise dos dados, **AI 25** destacou a relevância da segurança de dados pessoais, ressaltando a importância da **proteção da privacidade** como fundamental para resguardar as informações pessoais. A UNESCO (2017), também salienta a relevância da

consciencialização sobre a privacidade e a proteção de dados pessoais nas habilidades essenciais para o século XXI. Com a digitalização crescente da sociedade, é essencial que a educação capacite os alunos a proteger as informações pessoais e a promoção de uma cidadania digital responsável. Por outro lado, aspetos de **segurança cibernética**, que não mencionados diretamente, foram discutidos por outros alunos. O **Al 36**, por exemplo, ressaltou a importância de manter os aparelhos protegidos, destacando a necessidade de defender os computadores de ataques, como o *hacking*. Já o **Al 57** referiu a importância de utilizar *antivírus* como uma prática fundamental para se proteger ameaças digitais. Ambos mostraram compreender as medidas de segurança necessárias para garantir a proteção das atividades *online*. Mattar et al. (2020), afirmam que a inclusão de estratégias robustas de proteção cibernética no ensino é fundamental para preparar os alunos para os desafios tecnológicos atuais, possibilitando que naveguem de modo seguro e protegido no mundo digital. Tais iniciativas são fundamentais não só para a segurança individual, mas também para a coletiva numa sociedade cada vez mais conectada.

Surgiram diversas ideias: o **Al 2**, abordou a confidencialidade de dados e a relevância de senhas seguras, enquanto **Al 21** e **Al 57** discutiram *Spyware* e Golpes *Online* e a criação de um detetive virtual. Debateram a necessidade de verificar, com um adulto, antes de fazer *download* de arquivos e evitar partilhar informações pessoais.

Esta atividade prática, alinhou-se com o desenvolvimento de competências de cidadania digital, incentivando os alunos a recolher informações, promovendo a curiosidade e envolvendo-os na pesquisa de exemplos do mundo real, utilizando recursos *online* seguros. A professora sugeriu procurar informações confiáveis sobre riscos na *internet*, no *site SeguraNet*.

À medida que a aula avançava, o pensamento crítico dos alunos tornou-se mais assertivo, revelando maior sensatez e discernimento digital, enfatizando a importância de parcerias para garantir a segurança digital.

Os alunos revelaram um avanço notável nas competências propostas. Demonstraram habilidades de pensamento crítico ao analisar os perigos *online*, utilizaram recursos tecnológicos de maneira eficiente, compartilharam as descobertas, colaboraram ativamente com os colegas e demonstraram autonomia ao conduzir pesquisas independentes e participar das conversas em grupo.

A avaliação dos resultados mostrou que os alunos, conseguiram identificar e compreender

uma diversidade de ameaças digitais, tais como *phishing*, *malware*, *cyberbullying* e *ransomware*. O **Al 20** destacou a gravidade do *malware* e dos *vírus*, apontando que eles podem prejudicar severamente os aparelhos. Em relação à privacidade, o **Al 25** realçou a importância da confidencialidade dos dados e da defesa contra a invasão da privacidade. O **Al 10** aconselhou a desconfiar de *links* suspeitos, enquanto o **Al 57** reforçou a necessidade de usar *antivírus*.

4.3.3. JOGOS DE SEGURANÇA NA INTERNET

A aula, conforme descrito no ANEXO E, foi direcionada aos jogos de segurança na *internet*. Estes jogos interativos foram uma estratégia pedagógica eficiente para fortalecer conceções conceitos de proteção de dados e segurança *online*, como *phishing* e *cyberbullying*. Essa abordagem, combinando a prática e ensino, seguem as recomendações de Freitas et al. (2019), que defendem o envolvimento dos alunos**.**

Durante a conversação, a professora questionou 'O que entendem por cidadania digital e por que devemos ser cidadãos digitais cumpridores e prudentes?'. O **Al 6** respondeu: **É ficar seguro na *internet,* tipo, não falar com pessoas que não se conhece ou contar as coisas pessoais**. A professora reforçou os conteúdos da aula anterior e os alunos participaram nos jogos *SeguraNe*t, conforme recomendado por Tavares e Melo (2019).

Os jogos utilizados durante a aula foram:

O **Grande desafio (Jogo do Leopardo)**, que aborda questões sobre segurança digital, abrangendo temas dos 1.º e 2.º ciclos. O **Descobre (Em código)**, cujo foco foi o uso seguro dos telemóveis e jogos *online*, em que o **Al 33** destacou a importância de usar senhas fortes e de evitar clicar em *links* suspeitos. O jogo **Os *griefers* (puzzle)**, abordou os comportamentos nocivos nos jogos *online*.

Outra atividade, **Usar melhor o telemóvel (Labirinto)**, sugeriu práticas seguras para o uso do telemóvel, com o **Al 20** destacando a importância de verificar as definições de privacidade ao instalar novos aplicativos. O jogo **O telemóvel (Onde estão eles?)** incentivou nos cuidados a ter com o telemóvel desafiando-os a identificar potenciais riscos. **Jogar *online* (Descobre as diferenças)**, incentivou a identificação os cuidados a ter durante os jogos *online*, com o **Al 44** mencionando que passaria a ser mais cuidadoso ao partilhar informações pessoais durante os jogos. No **Jogo dos sabichões**, **Jogar *online* (completa as frases)** e **Cuidados a ter durante os jogos *online* (jogo do galo)**, os alunos consolidaram as práticas de segurança *online*.

O **Al 5** enfatizou que tr**ocar dicas de segurança é fundamental para garantir a proteção de todos** e o **Al 12**, afirmou **ter mais cautela com *links* desconhecidos**. Esses comentários mostram a assimilação dos conteúdos e o efeito dos jogos na aprendizagem.

A atividade promoveu o desenvolvimento de competências cidadãs, despertou o interesse dos alunos e incentivou a pesquisa de exemplos reais. Ao longo da aula, consolidaram conhecimentos sobre privacidade *online*, identificação de informações falsas, entre outras.

À medida que a aula progredia, o pensamento crítico dos alunos intensificou-se, demonstrando maior conhecimento digital. A verificação das interações dos alunos e da participação nas atividades evidenciou uma assimilação concreta dos princípios de segurança cibernética. A avaliação realizada (ANEXO E1), confirmou que as práticas educativas foram eficazes na promoção do desenvolvimento pessoal, autonomia, pensamento crítico, comunicação eficaz, e capacidades de colaboração entre os alunos.

A análise dos dados mostrou que os alunos aplicaram os conceitos na prática. O **Al 6** salientou: **É importante manter a segurança *online,* evitando conversar com estranhos ou compartilhar informações pessoais**, o que revela uma compreensão clara sobre a segurança digital. Além disso, o **Pensamento Crítico e Criativo** foi evidenciado nas respostas do **Al 12** e do **Al 44**. O **Al 12** mencionou: **Sim, vou ter mais cautela com *links* desconhecidos**, evidenciando o desenvolvimento do pensamento crítico e da capacidade de tomar decisões seguras na *internet*. Enquanto, **o Al 44** afirmou: **Vou usar senhas mais seguras** e disse também que **Devemos configurar as definições de privacidade nas redes sociais para proteção**.

Em termos de **Desenvolvimento Pessoal e Autonomia**, o **Al 33** mostrou proatividade ao dizer que iria conversar com os pais sobre as aprendizagens sobre segurança digital. Em termos de **Informação e Comunicação**, o **Al 20** ressaltou a relevância de verificar as fontes antes de aceder a *links*, destacando: É essencial validar a origem antes de clicar nos *links*, evidenciando a habilidade de transferir conhecimento em situações práticas.

Em suma, **as ações alcançaram os objetivos**, promovendo a consciencialização e a autonomia, conforme mostrado pelas participações dos alunos citados, validando, dessa forma, a efetividade a estratégia educativa e alinhando-a às competências do PASEO.

4.3.4. VISUALIZAÇÃO DE VÍDEOS

Durante a visualização de vídeos (ANEXO F), foi destacada a importância da consciencialização digital. Essa estratégia reforça a importância da educação digital para formar cidadãos conscientes. De acordo com Cunha et al. (2024), a inclusão de recursos audiovisuais no ensino é essencial para criar consciência sobre as práticas seguras na *Internet*. O site *SeguraNet* oferece vídeos educativos essenciais para a formação de cidadãos digitais críticos e responsáveis, conforme defendido por Pereira e Moura (2022).

Os recursos visualizados pelos alunos, podem ser categorizados em três áreas principais:

1. Cidadania Digital:

- → **Não à Violência *Online*!** - combate ao *cyberbullying*.
- → **Desinformação em Contexto de Guerra** – combate à desinformação.
- → ***Cyberbullying*: Quem avisa, amigo é!** - sensibilização sobre o efeito do *cyberbullying*.
- → **Ciberbullying: O que é e como prevenir?** - prevenção do *cyberbullying*.
- → ***Internet* Segura: É fácil como uma Bola de Sabão!** - reflexão sobre a responsabilidade digital.
- → ***Internet* Segura: Clica, mas com moderação!** - uso consciente da *internet*.

2. Segurança *Online*:

- → **Como Proteger os teus Dados?** - proteção de dados e privacidade.
- → **Reconhecer e Evitar Fraudes *Online*** - evitar fraudes na *internet*.
- → **Jogo de Segurança na *Internet*** - comportamentos seguros em jogos *online*.
- → **Segurança no Jogo *Online*: Protege a tua Identidade!** - Segurança em jogos *online*.
- → **Mitos e Verdades sobre a Segurança na *Internet*** - desmistificação sobre segurança digital.

3. Educação para o Uso da Tecnologia:

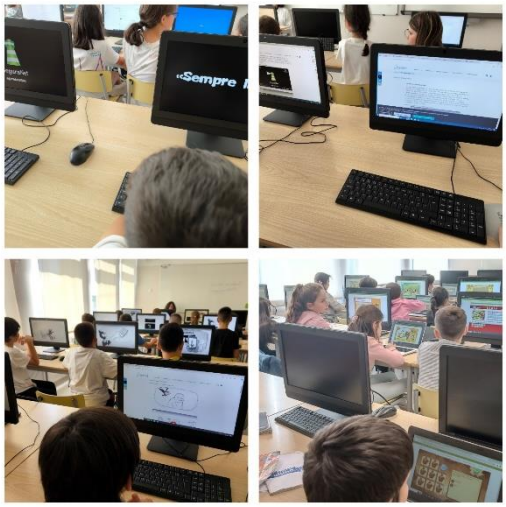
- → **Práticas *Online* Seguras e Saudáveis** - uso seguro e saudável de dispositivos e redes sociais.

→ **Etiqueta Digital: Comportamento *Online* Importa!** - importância da etiqueta digital.

→ **Navegar em Segurança: Respeito e Responsabilidade** - uso responsável da *internet*.

Esses vídeos (Figura 9) serviram para consolidar aprendizagens adquiridas. O **Al 33** afirmou: **Ser mais cuidadoso com *links* desconhecidos**, evidenciando como as aprendizagens foram incorporadas às suas práticas digitais.

Figura 9 - Segurança Online em Ação



Seguindo as diretrizes do **Al 12** que recomenda: **Usando combinações de letras, números e símbolos e não reutilizando senhas**, revelou avanço nos conhecimentos nesta área. **Al 44** após assistir aos vídeos, referiu: **Gostei da dica sobre verificar links antes de clicar**, evidenciando a aplicação prática do conteúdo

No vídeo **Jogar *online***, os alunos exploraram o *cyberbullying* e desenvolveram soluções concretas para o problema, como denunciar comportamentos abusivos para as plataformas, evitar interagir com estranhos, criar ambiente de apoio entre os jogadores, e fomentar respeito e a empatia nos jogos.

Com a realização desta atividade foi percetível o progresso no desenvolvimento das habilidades dos alunos em relação à cidadania digital e segurança na *internet*, conforme descrito no documento PASEO (Martins et al., 2017). Por exemplo, o **Al 20** mostrou compreensão ao dizer: **Podemos ser *hackeados* e perder dados importantes**. Essa afirmação revela uma perceção dos perigos digitais, especialmente ligados à divulgação de dados pessoais, o que é uma habilidade fundamental na era digital. Além disso, a reflexão do **Al 33** sobre a necessidade de cautela ao lidar com *links* desconhecidos. Ser **mais cuidadoso com *links* desconhecidos**, reforça a relevância de adotar práticas seguras *online*. Os comentários indicam uma **evolução nas competências de pensamento crítico e criativo** e na **autonomia**, à medida que os alunos começam a aplicar o conhecimento de forma prática.

O aprimoramento dessas competências foi reforçado ao assistir a outros vídeos, os que

tratam da desinformação e dos golpes *online*, possibilitando-lhes reconhecer fontes pouco confiáveis e assumir atitudes mais prudentes na *internet*.

A atividade foi acompanhada de uma avaliação contínua da participação dos alunos, sendo claro que os conceitos foram assimilados de maneira eficaz.

Além disso, os conteúdos audiovisuais apresentados, como **Não à Violência na *Internet***! e **Como Proteger os Teus Dados**, foram classificados com o intuito de abordar os temas de Respeito Digital e Proteção *Online*, incentivando-os a analisar de forma crítica o comportamento virtual e a refletir sobre maneiras de promover um ambiente *online* mais protegido. O **Al 5** sugeriu a criação de *posters* sobre segurança cibernética, estimulando a participação e promovendo a construção de uma cidadania digital ativa e colaborativa.

A evolução das competências dos alunos foi observada em comentários como o de **Al 60**, que enfatizou a importância de manter um **antivírus atualizado** para garantir a segurança dos dispositivos. Isso reflete uma compreensão mais profunda sobre a segurança *online*, além das medidas básicas de proteção de dados.

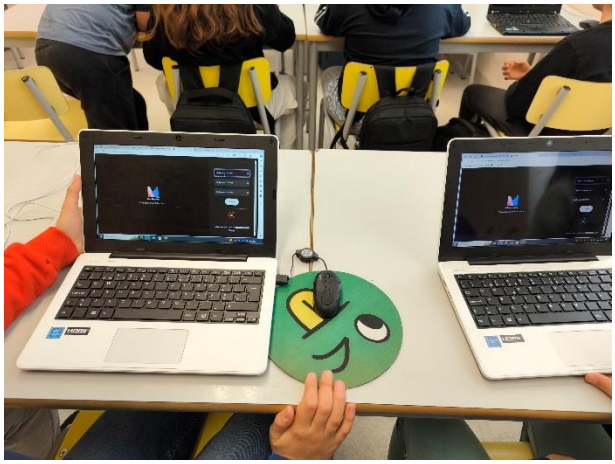
Resumindo, a combinação de vídeos educativos do ***SeguraNet***, debates em grupo e atividades interativas foi fundamental para desenvolver competências relacionadas com a **cidadania digital**, **pensamento crítico** e **autonomia**. As atividades melhoraram o comportamento *online* dos alunos, preparando-os para uma navegação segura, conforme as competências do PASEO e as diretrizes de Pereira e Moura (2022).

4.3.5. MENTIMETER NA AULA: CONHECENDO E COMBATENDO OS RISCOS ONLINE

Nesta atividade (ANEXO K), o objetivo principal foi proporcionar um entendimento aprofundado sobre os perigos da *internet* e promover competências de cidadania digital. A representação visual demonstra como os recursos digitais podem enriquecer a compreensão e a sensibilização em relação a questões cruciais sobre a cidadania digital.

A professora orientou os alunos na identificação de ameaças. O **Al 33** mencionou o ***phishing***, enquanto **Al 12** referiu o ***cyberbullying*** e o **Al 20** falou sobre o ***Malware***, demonstrando um conhecimento básico dos perigos e riscos *online*.

Figura 10 - Conexão e Colaboração: Alunos Acedendo Ferramentas de Aprendizagem Digital

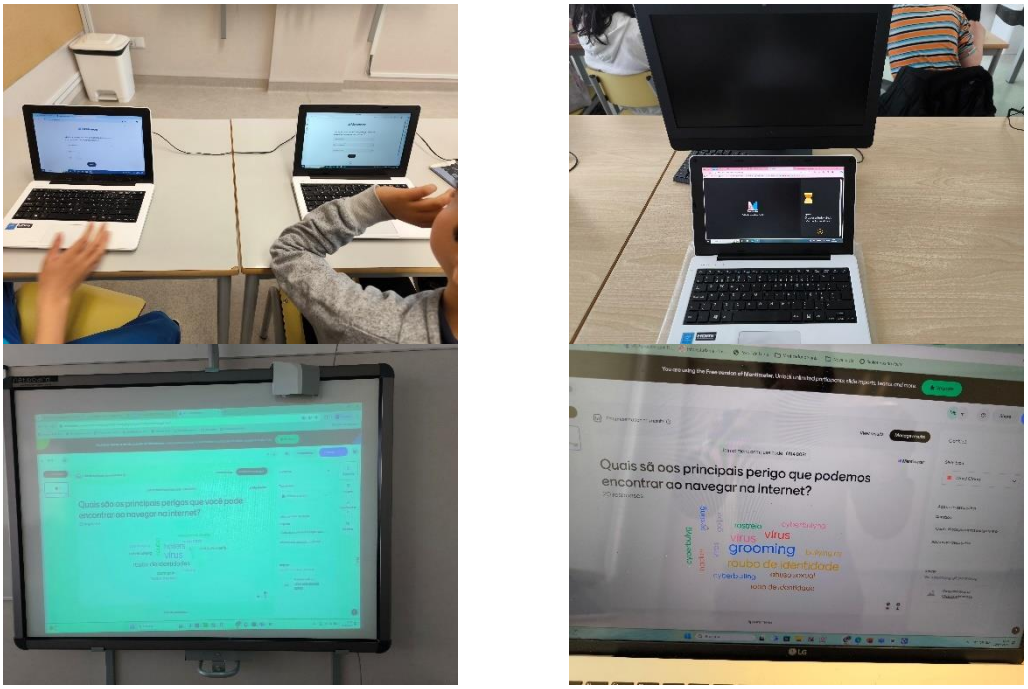


A Figura 10 ilustra o momento de interação tecnológica em que os alunos utilizaram o *Mentimeter* e identificaram três palavras-chave, relacionadas com as preocupações comuns com a segurança *online*. Durante a realização desta atividade, o **Al 20** destacou três palavras-chave que representaram os principais perigos *online*: ***Phishing***, ***Malware***, ***Privacidade***.

De forma idêntica, o **Al 33** selecionou ***Phishing*** como a ameaça mais significativa, enquanto o **Al 44** apontou ***Fraudes***, **Roubo de Identidade**, ***Spyware***, mostrando um entendimento e compreensão mais ampla sobre os desafios da segurança cibernética.

Cada aluno apresentou até três soluções, gerando 66 respostas por sala (exceto a turma 4.º D, com 45 respostas devido ao menor número de alunos).

Figura 11 - Navegando no Saber: Alunos e as Tecnologias na Educação



A análise das nuvens de palavras permitiu identificar as principais ameaças mencionadas pela maioria dos alunos. Essa abordagem prática e interativa permitiu aos alunos

aplicarem os conceitos estudados, proporcionando a segurança cibernética, incentivando-os a refletir sobre comportamentos seguros na *Internet*.

Os resultados da sessão interativa com o ***Mentimeter***, no âmbito do Projeto Cidadania Digital implementado pelo 1.º CEB, revelaram um panorama dos perigos da *Internet* sentidos pelos alunos das turmas A, B, C e D dos 4.º anos, exemplificada na Tabela 9. As nuvens de palavras geradas refletem a contribuição coletiva das turmas.

Figura 12 - Nuvem de Palavras do 4.º A sobre os Principais Perigos na Internet

No **4.º A** (Figura 12), o tema predominante foi **Cyberbullying**, com 26% das respostas (17 respostas), evidenciando a preocupação dos alunos com este comportamento nocivo. O tema ***Vírus*** foi citado em 23% (15 respostas), em seguida foi o ***Grooming*** com 17% (11 respostas). As palavras ***Sexting*** e ***Phishing*** foram agrupadas na categoria: ***Outros***, totalizando 34% (23 respostas). Estes dados demonstram o conhecimento dos alunos sobre os riscos *online*.

No **4.º B** (Figura 13), o perigo referido com mais frequência pelos alunos foi ***Vírus*** com 29% (19 respostas), indicando uma preocupação com os perigos do mundo técnico. O ***Cyberbullying*** foi mencionado 26% (17 respostas), seguido pelo **Roubo de Identidade** que também estava em 17% (11 respostas). Os outros conceitos foram colocados juntos no grupo de **Outros**, totalizando 29% (19 respostas). Este perfil pode evidenciar a necessidade de uma educação permanente sobre esses temas.

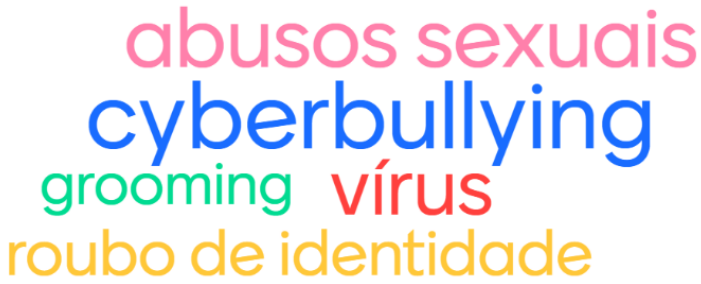
Figura 13 - Nuvem de Palavras do 4.º B sobre os Principais Perigos na Internet

No **4º C** (Figura 14), o ***Vírus*** foi a principal preocupação com 30% (20 respostas), seguido por ***Cyberbullying*** com 24% (16 respostas) e, ainda, **Roubo de Identidade** com 18% (12 respostas); **Grooming** e ***Phishing*** foram também mencionados, totalizando 28% (18 respostas). Esse padrão repetiu-se nas outras turmas, confirmando preocupações comuns em relação à segurança na *internet*.

Figura 14 - Nuvem de Palavras do 4.º C sobre os Principais Perigos na Internet

No **4.º D** (Figura 15), ***Cyberbullying*** representou a principal preocupação dos respondentes, tendo sido assinalado por 33% (15 respostas); **Abusos Sexuais** foram referidos por 27% (12 respostas); em 20% (9 respostas), os respondentes referiram ***Vírus***; ***Grooming*** e ***Roubo de Identidade*** foram assinalados na categoria **Outros**, na medida em que foram assinalados por 20% (9 respostas). Estes resultados mostram um elevado grau de consciência dos alunos em relação ao **assédio** e **exploração *online***, sem esquecer as ameaças técnicas.

Figura 15 - Nuvem de Palavras do 4.º D sobre os Principais Perigos na Internet



Nas nuvens de palavras, os termos em destaque correspondem aos perigos mais referidos, como ***Cyberbullying***, ***Vírus*** e **Roubo de Identidade**, o que demonstra a efetividade das estratégias educativas implementadas.

Em suma, a análise das respostas evidenciou uma alta perceção dos alunos sobre os perigos digitais. A evolução do conhecimento dos alunos sobre esses riscos *online* confirma o sucesso das atividades educativas na promoção de uma cidadania mais crítica, de acordo com Melo e Vieira (2020), que defendem a importância das atividades colaborativas para o desenvolvimento dessas competências.

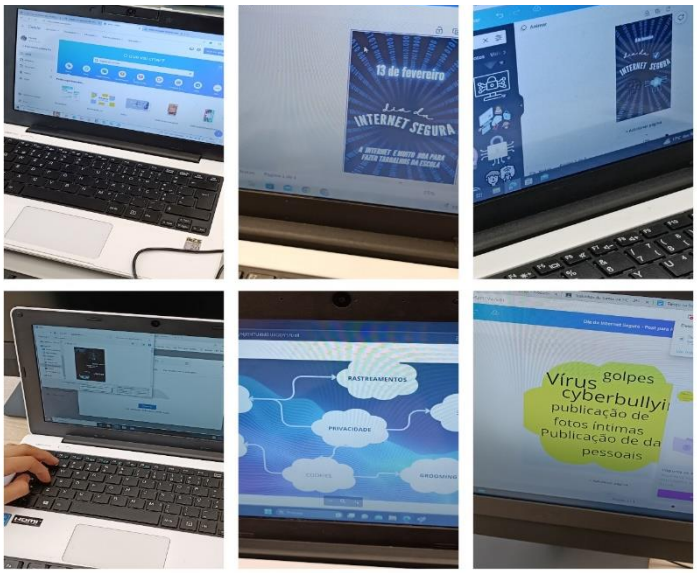
4.3.6. Criação Visual no Canva: Atividade onde os alunos criam visuais que promovem a segurança na internet

Nesta aula, centrada na temática da Cidadania Digital (ANEXO L), o objetivo foi capacitar os alunos no sentido do desenvolvimento de competências pessoais, autonomia, e comunicação segura. A atividade iniciou-se com uma reflexão sobre a importância de práticas seguras na navegação, seguida da partilha de vivências, como a exposição a *phishing*, *cyberbullying* em redes sociais e exposição acidental a conteúdos inadequados. O Al 1 referiu que: **É crucial lembrar que nunca devemos divulgar informações pessoais a indivíduos desconhecidos na web**. Isso demonstra a compreensão da privacidade *online* como fator essencial para a segurança digital.

Figura 16 - Os Perigos do Ciberespaço: Como Proteger-se Online

Os alunos utilizaram a plataforma *Canva* (Figura 16) para cada um criar um *poster* digital sobre segurança *online*.

Figura 17 - Desenvolvimento de Competências Digitais: Alunos Criando Conteúdos de Cidadania Digital no Canva



O **Al 5**, mencionou: **Vou criar um poster sobre a importância de não compartilhar senhas**. O **Al 6** referiu a necessidade de **Não clicar em *links* suspeitos**. Os alunos criaram *posters* no *Canva* sobre temas de segurança digital, aplicando o que aprenderam sobre práticas seguras, como a importância de senhas fortes e evitar colocar em *links* suspeitos.

Conforme defendem Martins et al. (2017), é imprescindível que os alunos apresentem, na produção, a aplicação do saber científico a situações práticas. A criação de *posters* permitiu aos alunos expressarem de forma gráfica e criativa, demonstrando o que aprenderam sobre segurança *online*. **A1 20** fez um ***póster*** sobre a proteção da **privacidade** nas redes sociais, ressaltando a importância do saber como guardar as informações pessoais; **A1 33** destacou a importância de discutir práticas seguras com a família, demonstrando compreensão sobre a necessidade da participação familiar na promoção da segurança digital.

Essa fase foi essencial para reforçar a aprendizagem e estimular a participação ativa dos alunos.

Os resultados demonstraram um incremento significativo nos referidos conhecimentos em competências digitais, autonomia e pensamento crítico. Os alunos transformaram o conhecimento adquirido sobre **fraudes** ao ***bullying*** virtual em *posters* visuais A atividade reforçou métodos de ensino interativos, estimulando a comunicação e colaboração na aprendizagem sobre os riscos de compartilhar informações pessoais *online* (Martins et al., 2017). O **Al 6** destacou o risco de **Não clicar em *links* suspeitos**, demonstrando compreensão dos perigos *online* e aplicação prática dos conhecimentos adquiridos em

tarefas realizadas na sala de aula, permitindo que os alunos, tal como o **Al 20** aplicassem o que aprenderam, bem como o **Al 33 É fundamental discutir práticas seguras com a família** o que revela entendimento sobre a importância de conversar e de envolver a família na proteção digital, combinando-se com conselhos de Pereira e Moura (2022) que destacam necessidade de uma abordagem coletiva e inclusiva na aprendizagem para a segurança digital. Os alunos demonstraram criatividade e clareza ao criar os seus *posters*, aplicando o que aprenderam sobre segurança *online*. Essa fase permitiu consolidar a aprendizagem e avaliar a participação dos alunos.

Os resultados da aula focada na Cidadania Digital (ANEXO L1) mostraram um desenvolvimento notável nas competências dos alunos, especialmente no que se refere às competências digitais, autonomia e espírito crítico sobre a segurança *online*. O **Al 5**, ao fazer um cartaz sobre **a importância de não compartilhar senhas**, mostrou compreensão dos perigos da divulgação de dados pessoais e conseguiu comunicar essa informação de forma simples e clara. O **Al 6** demonstrou habilidades críticas ao criar um *poster* sobre **não clicar em *links* suspeitos**. A aplicação prática dos conceitos teóricos foi claramente evidenciada na criação dos *posters* (Martins et al., (2017)

O **Al 33** destacou **a importância de discutir práticas seguras com a família** demonstrando a compreensão de que a segurança digital envolve tanto ações individuais, quanto coletivas, alinhando-se com Pereira e Moura (2022). O **Al 20** demonstrou compreensão ao criar um cartaz sobre privacidade *online*, comunicando de forma clara o que aprendeu sobre segurança na *Internet*. Tal prática equivale ao ensino defendido por Freitas et al. (2023), métodos de ensino interativos e colaborativos que exigem o envolvimento na prática do aluno, promovendo comunicação, colaboração e a triangulação da aprendizagem.

Os resultados mostraram uma evolução significativa nas competências digitais dos alunos, consolidando a integração de teoria e prática para uma navegação mais segura na *Internet*. Esses resultados coadunam-se à literatura educativa que sustenta um modelo de ensino que integra teoria e prática, proporcionando uma formação integral ao aluno.

4.3.7. QUIZ NO NEARPOD: APLICAÇÃO DE UM QUIZ PARA CONSOLIDAR E AVALIAR A APRENDIZAGEM, COM FEEDBACK INSTANTÂNEO

A atividade ***Quiz no Nearpod***, realizada na sala de aula (ANEXO M), realçou a utilização das tecnologias digitais na educação. A plataforma *Nearpod* proporciona recursos como

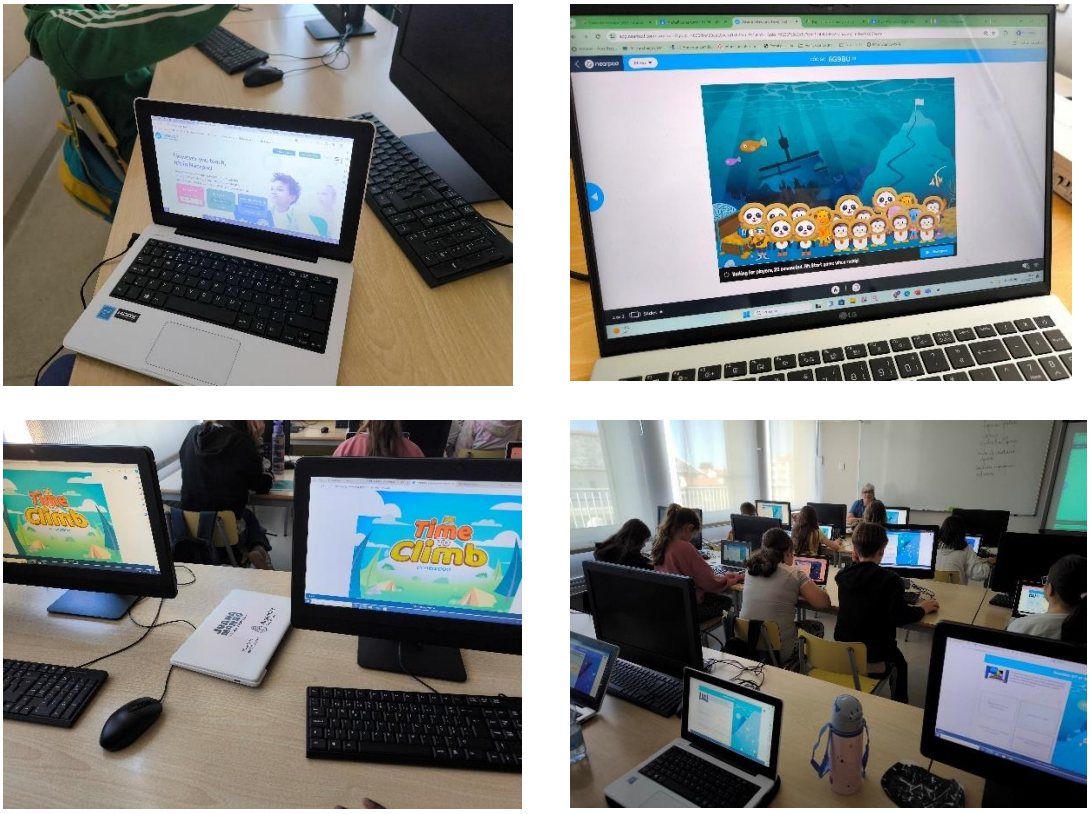
quizzes ao vivo e jogos educativos, que incentivaram a participação ativa dos alunos.

O *quiz* consistiu em 15 perguntas, que foram elaboradas visando tanto o conhecimento teórico quanto a aplicação prática dos princípios de segurança cibernética. Este formato ajudou a identificar problemas enfrentados pelos alunos em temas de atividades *online* e riscos digitais, permitindo intervenções educativas mais eficazes.

Este *quiz* consistiu em situações reais e alternativas de resposta. As perguntas avaliaram o conhecimento teórico e prático abordando temas como *phishing*, *malware* e proteção de dados, revelando lacunas de aprendizagem e necessidades específicas para ajustes educativos. Essas dificuldades demonstraram a importância de reforçar o ensino sobre segurança cibernética e de adaptar as atividades pedagógicas para que todos os alunos possam desenvolver plenamente as competências necessárias para uma navegação segura.

A aula começou com um debate sobre a importância da Cidadania Digital, promovendo o desenvolvimento pessoal, autonomia e habilidades de comunicação. A professora enfatizou a importância da segurança digital, encorajando os alunos a compartilharem vivências pessoais sobre navegação segura.

Figura 18 - Explorando Horizontes Digitais: Aprendizagem Interativo e Tecnologia na Educação



Nota – Ilustração do uso de tecnologia digital na educação, enfatizando atividades interativas que promovem o desenvolvimento de competências digitais essenciais através de uma aprendizagem lúdica

O ***Quiz*** na plataforma ***Nearpod*** (Figura 18) destacou a importância de metodologias dinâmicas e participativas que promovam o envolvimento ativo dos alunos Freitas et al. (2023) e Rosado e Dias (2024).

Uma das vantagens mais proeminentes da plataforma residia em sua capacidade de promover uma aprendizagem assertiva. O recurso ***Time to Climb*** proporcionou um *quiz* competitivo onde os alunos respondiam rapidamente e seus avatares subiam uma montanha virtual. Essa dinâmica, somada ao debate acerca da segurança na *Internet* e às vivências dos alunos, favoreceu o desenvolvimento pessoal e autoconfiança, conforme apontado por Melo e Vieira (2020).

A professora deu início ao trabalho com a atividade ***Time to Climb***, abordando temas como privacidade, proteção de dados e boas práticas de navegação *online*. Al 5 declarou: **Eu verifico sempre se o *site* é seguro antes de colocar minhas informações**, e **Al 12** e **Al 20** refere: **Uma vez eu recebi um e-mail suspeito e não cliquei no *link***, retratando-se em uma posição cautelosa sobre o tópico de segurança. O **Al 33** ressaltou a importância de manter o antivírus atualizado ao afirmar que devemos agir como adultos digitais, de acordo com os métodos de prevenção sobre ataques digitais.

O *Nearpod* fornece explicações detalhadas sobre o desempenho dos alunos, permitindo aos professores monitorar o progresso individual e, assim, fazer as correções necessárias. Os relatórios destacaram os pontos fracos e fortes, ajudando a promover uma postura crítica e responsável *online*.

A atividade revelou que o *quiz* ajudou a aprimorar o pensamento crítico e a distinguir comportamentos seguros e perigosos. O *feedback* instantâneo proporcionado pelo *Nearpod* permitiu à professora adaptar o ensino às necessidades específicas de cada aluno, garantindo que todos aprendessem as melhores práticas de segurança digital.

As quatro turmas do 4.º ano apresentaram resultados diversos nas avaliações. O **4.º A** teve uma média de 89% e a maioria dos alunos (13 em 20) teve notas a partir de 87%. Três alunos atingiram 100%. O **4.º B** apresentou uma média de 84% e as notas oscilaram de 80% a 93%. Isto indica um desempenho estável, mas com possibilidades de melhoria. O **4.º C** teve uma média de 82% e suas notas oscilaram de 40% a 100%, sendo que alguns alunos precisaram de um auxílio adicional. O **4.º D** teve uma média de 84% e a maioria variou entre 80% a 93%, sendo que dois alunos se aproximaram mais de 100%.

A análise geral mostra que as médias oscilaram entre 82% e 89%, sugerindo um bom

domínio do conteúdo, mas alguns alunos precisarão de apoio extra para melhorar os resultados.

4.3.8. DIA INTERNACIONAL DA INTERNET SEGURA

O **Dia Internacional da Internet Segura** (ANEXO N) foi um verdadeiro sucesso entre os alunos do 4.º ano, que participaram na atividade com grande entusiasmo, mostrando-se plenamente envolvidos e motivados.

A aula iniciou-se com a apresentação de elementos da GNR, que alertaram as turmas para a importância da segurança na *Internet* através da apresentação de um *PowerPoint*, com exemplos e situações reais, (Figura 19). Esta fase conforme Apocalypse et al. (2022), é a fase que envolve uma compreensão profunda dos problemas enfrentados pelos alunos. A apresentação da GNR ajudou a identificar os desafios específicos dos alunos, orientando as tarefas seguintes, como simulação de cenários e sessão de perguntas e respostas.

Figura 19 - Empoderando Mentes Jovens: Workshop Interativo Anti-Bullying da GNR

Na aula, a GNR apresentou imagens de cenários perigosos através da internet, como o *phishing* e o *cyberbullying*. **Al 70** respondeu corretamente sobre a definição de *phishing*, sendo que a GNR explicou como se pode evitar que este ataque aconteça. O **Al 53** interrompeu, dizendo que não se devem rir dos outros, salientando que **devemos tratar toda a gente, como gostaríamos de ser tratados**. A professora, posteriormente, pediu aos alunos para descreverem situações na *internet* das quais já tivessem conhecimento ou que já tivessem vivenciado. **Al 35** referiu ter recebido uma mensagem suspeita enquanto estava a jogar e a professora sublinhou a importância de se falar sempre com um adulto. Seguiu-se a apresentação do *PowerPoint*, Simulação de Cenários (*Role-Play*) e Sessão de Perguntas e Respostas. Segundo Panke (2019), nesta etapa é definido o problema para depois ser resolvido.

Seguiu-se uma atividade de exploração sobre riscos *online*, sendo utilizadas as situações

mostradas no *PowerPoint*. Pergunta ‘O que fariam se alguém *online* pedisse para fornecer o endereço de casa?’ O aluno **A1 41 nunca o daria e iria dizer imediatamente isso aos pais**; o aluno **A1 50** disse que fecharia uma página inapropriada e chamaria o adulto. Na questão sobre envio de fotos pessoais, o aluno **A1 61** disse que nunca enviaria fotos de si mesmo *online*, especialmente para estranhos**.** A professora elogiou os alunos pelas suas respostas e enfatizou a necessidade de se manter os dados pessoais privados.

Para recapitular, **Al 42** enfatizou a relevância da utilização de senhas fortes. Deveríamos **usar sempre uma senha forte e nunca compartilhar as informações**. **É isso: deve haver letras grandes, pequenas, números e símbolos**, explicou ele. **Al 39** mencionou. Se **algo me deixasse desconfortável, deveria contar aos meus pais ou professores.** Outro cenário abordado foi: ‘Como reagir ao receber mensagens de desconhecidos?’ o **Al 44** sugeriu que **nunca se deve responder e deve-se informar um adulto imediatamente**.

A professora aferiu o envolvimento dos alunos durante a aula, observando as perceções de risco e a forma como comunicavam. Os alunos evidenciaram um conhecimento sólido em segurança digital, respondendo de forma adequada às questões e demonstrando uma disposição voltada para a solvência dos problemas colocados.

A aula foi pertinente na sensibilização dos alunos para os perigos da *internet*, transmitindo habilidades essenciais para a navegação segura e cidadã. Mediante atividades interativas, os alunos ampliaram o entendimento em segurança digital e competências críticas para enfrentar desafios do mundo digital.

No Dia Internacional da *Internet* Segura, observou-se que os alunos demonstraram um grande avanço em autonomia, comunicação e pensamento crítico, envolvendo-se ativamente nos debates em relação à proteção digital. Eles compreenderam conceitos fundamentais e foram capazes de identificar e sugerir a solução para as situações de risco *online*, como: não fornecer informações pessoais, fechar as páginas inapropriadas e ignorar as mensagens de pessoas desconhecidas. Essas atividades promoveram habilidades de tomada de decisão informada e expressar-se de maneira eficaz sobre segurança na *internet*, e isto preparou-os para uma navegação mais consciente e segura.

4.3.9. DIREITOS DIGITAIS: A VOZ DAS CRIANÇAS NA INTERNET

No início da aula (ANEXO O), a professora fez uma introdução ao tema dos direitos digitais para sensibilizar os alunos em relação à sua relevância e promover a autonomia e o desenvolvimento pessoal dos alunos. Mattar et al. (2020) enfatiza a importância de sensibilizar e capacitar os alunos para uma cidadania digital consciente e responsável.

A professora começou por partilhar informações importantes sobre os direitos digitais das crianças, como o direito à proteção da privacidade, à segurança *online* e à informação. De seguida, fez uma apresentação sobre esses direitos, explicando de forma acessível os conceitos e a sua importância para a segurança digital dos alunos. Colocaram perguntas pertinentes sobre como agir se alguém divulgar os seus dados e o que devem ou não fazer para mantê-los seguros *online*.

Após a explicação, os alunos partilharam as suas experiências ancoradas nesses direitos. O **Al 41**: disse. Recebi **uma mensagem suspeita enquanto jogava *online* e avisei meus pais Al 33**: relatou. Eu **não sabia que compartilhar minha localização poderia ser perigoso, agora vou verificar as configurações de privacidade**. **Al 55**: **É importante proteger as pessoas contra assédio *online*, porque eu vi amigos passarem por isso** relatando casos de assédio virtual que presenciaram.

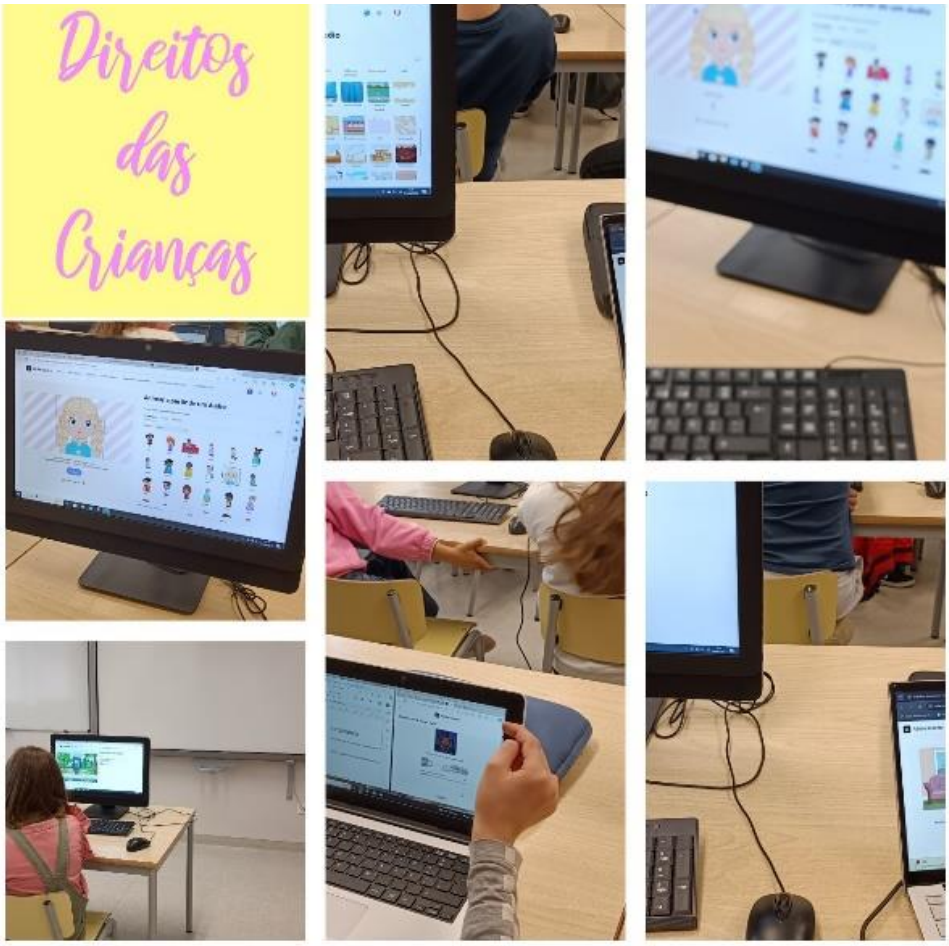
Esse período de reflexão possibilitou compreender de maneira mais profunda as vivências e preocupações dos alunos, como o contato com desconhecidos nas plataformas de jogo ou redes sociais e o acesso a aplicativos ou jogos com conteúdos impróprios. Os alunos relataram seu medo de páginas inseguras, que pedem dados pessoais ou que trazem publicidade imprópria.

Em seguida, os alunos realizaram uma tarefa de pesquisa individual acerca dos direitos digitais das crianças, numa atividade em computadores. Elaboraram uma lista de direitos no *Google Docs* e gravaram áudios apresentando os direitos mais relevantes, tendo, posteriormente, criado animações com as ferramentas para criar *avatares* falantes, no ***Voki*** *(Voki.com)* e ***Adobe Express*** (https://helpx.adobe.com/pt/express/using/how-to-animate-from-audio.html).

Os resultados mais significativos constam do Diário de bordo (Padlet). A ilustração na Figura 20 retrata o momento em que os alunos exploram esses direitos, utilizando

ferramentas digitais como avatares, elaborados dentro do projeto. Os mesmos foram compartilhados no *Google Classroom* e, além deles, os vídeos dos direitos foram gravados e postados no *Padlet*.

Figura 20 - Aprendizagem Digital sobre Direitos das Crianças



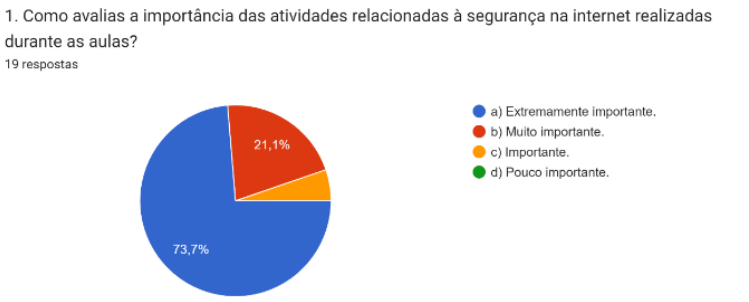
Após a apresentação dos resultados, os alunos discutiram soluções voltadas para a proteção dos seus direitos *online*. De acordo com Farias e Mendonça (2021) essa etapa é fundamental para incentivar a reflexão sobre os direitos digitais. Os alunos articularam as informações discutidas e realizaram as apresentações finais utilizando os avatares, expressando de forma criativa suas identidades e os direitos que consideraram mais importantes.

Durante as apresentações realizadas, os alunos discutiram como garantir o respeito aos direitos digitais e o que configura um comportamento seguro na *internet*. Essa discussão foi fundamental no desenvolvimento do pensamento crítico e de responsabilidade digital, como indicado por Freitas et al. (2023).

4.3. FORMULÁRIO: AVALIAÇÃO DA EFICÁCIA DAS ATIVIDADES

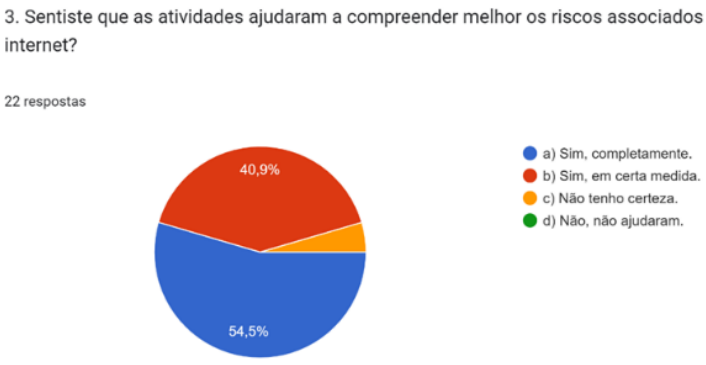
A aula (ANEXO P) foi voltada para a segurança na *internet*, enfatizando o desenvolvimento pessoal, a autossuficiência, a comunicação e o pensamento crítico dos alunos. Inicialmente, a professora fez uma revisão de segurança digital e demonstrou como preencher o formulário. Os alunos ouviram atentamente e, em seguida, procederam ao preenchimento do *Google Forms* (ANEXO P2), contém as perguntas transcritas da avaliação do conhecimento dos alunos sobre segurança digital. Apenas os gráficos mais significativos foram selecionados para análise aqui. Os gráficos completos e as respostas detalhadas podem ser consultados no ANEXO P3.

No **4.º B**, na pergunta 1: "Como avalias a importância das atividades relacionadas à segurança na *internet* realizadas durante as aulas?", 73,7% dos alunos consideraram a atividade "extremamente importante".

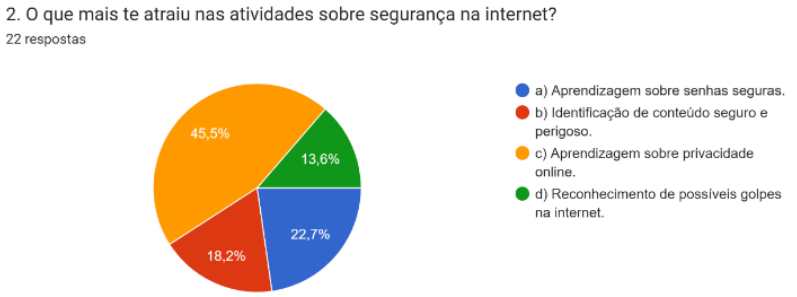


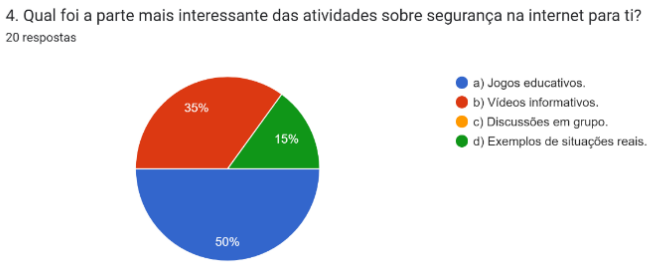
Isso demonstra uma assimilação eficaz dos conteúdos, indicando que a turma estava envolvida e beneficiou das atividades.

No **4.º D**, na pergunta 3: "Sentiste que as atividades ajudaram a compreender melhor os riscos associados ao uso da *internet*?", houve um equilíbrio nas respostas entre "Sim, completamente" e "Sim, em certa medida". Isso sugere que alguns alunos não alcançaram plenamente os objetivos, sinalizando a necessidade de ajustes nas atividades para garantir uma melhor compreensão dos conceitos, especialmente nas áreas de segurança digital e proteção de dados.



No **4.º C**, na pergunta 2: "O que mais te atraiu nas atividades sobre segurança na internet?", 31,8% dos alunos responderam que aprender sobre "privacidade *online*" foi o mais atrativo. Isso indica um entendimento mais específico sobre a proteção de dados pessoais, refletindo que as atividades que enfatizaram esse tema tiveram reação.





No **4.º A**, na pergunta 4: "Qual foi a parte mais interessante das atividades sobre segurança na *internet* para ti?", os alunos demonstraram maior interesse nos vídeos informativos , mostrando que essa ferramenta foi mais eficaz para promover a aprendizagem na turma.

A atividade proporcionou o envolvimento dos alunos na atividade, tendo-se mostrado atentos e dedicados. Quando o formulário foi preenchido, houve um debate entre os alunos, podendo cada aluno abordar comportamentos seguros na *internet*. A análise descritiva dos resultados dessa discussão pode ser consultada no ANEXO P1, na qual é descrita a eficácia das atividades no desenvolvimento dos alunos.

Esse tipo de reflexão e debate é imprescindível para a construção de um conhecimento sólido, complementando o conceito de uma cidadania digital responsável, sob a perspetiva de Melo e Vieira (2020) e Farias e Mendonça (2021).

Acerca das atividades mais interessantes, os **Jogos educativos** foram os que eles mais gostaram, sendo seguidos dos **Exemplos de situações reais** e Vídeos informativos, mostrando que as formas interativas são mais atrativas aos alunos.

Isso permitiu verificar as consequências das atividades sobre segurança na *internet* nas turmas 4.º A, 4.º B, 4.º C e 4.º D. Enquanto no 4.º B, ressaltando a valorização das aulas, no 4.º C, onde se verificou um enfoque maior em privacidade *online*. Portanto, os

resultados mostram que essas estratégias pedagógicas foram ajustadas às necessidades e especificidades das turmas.

Os alunos não deixaram de ser ativos, demonstrando empenho ao preencher o formulário no *Google Forms* (ANEXO P2). A atividade teve como objetivo desenvolver habilidades digitais, promover segurança *online* e avaliar o conhecimento dos alunos sobre cibersegurança, privacidade de dados e cidadania digital, além de servir como meio de acompanhar a evolução dos alunos e obter um retorno acerca das atividades desenvolvidas, no sentido de ajustar e melhorar as estratégias pedagógicas.

V DESENVOLVIMENTO DE COMPETÊNCIAS AO LONGO DO PROJETO

A avaliação dos resultados das atividades voltadas para os riscos da *internet* e a segurança digital permitiu mensurar a proficiência dos alunos no pensamento crítico, comunicação, desenvolvimento pessoal e autonomia. Estas competências, conforme previstas em orientações como o PASEO, as AE e a ENEC, serviram de referência para a identificação de pontos fortes e de necessidades específicas de apoio ao desenvolvimento dos alunos.
Os desempenhos mostraram grande dispersão, com alguns alunos a revelarem aptidão a aplicar os conceitos de segurança digital, enquanto outros evidenciaram necessidade de um acompanhamento pedagógico ajustado, para a compreensão e a adesão a práticas de navegação segura.

1. **Pensamento Crítico e Criativo**

- **- Atividades:**

↳Atividade com *Post-its*

↳Pesquisa sobre Perigos na *Internet*

- **- Intervenções dos Alunos:**

↳**Al 5**: Os *hackers* são perigosos porque podem roubar informações.

- **Análise**: Demonstrou um entendimento básico, mas carece de uma análise mais profunda dos riscos associados ao *hacking*.

↳**Al 12**: *Phishing* é perigoso porque as pessoas podem se passar por alguém confiável.

- **Análise**: Mostra um bom entendimento do conceito, mas necessita de aprofundamento em como identificar e evitar essas ameaças.
- **Fundamentação**:

Mattar et al. (2020): O estudo menciona a importância da combinação de competências digitais com os *frameworks* de educação, como o *DigComp*, para desenvolver habilidades críticas e criativas nos alunos, ajudando-os a enfrentar os desafios digitais.

→ Relação com a Estratégia Nacional de Educação para a Cidadania:

O desenvolvimento do pensamento crítico e criativo é um dos pilares da Estratégia Nacional de Educação para a Cidadania, que visa capacitar os alunos para analisar, avaliar e resolver problemas complexos, como os relacionados com a segurança digital.

2. **Comunicação e Relacionamento Interpessoal**

- **Atividades**:

↳Discussão em Grupo

↳Apresentação de Resultados

- **Intervenções dos Alunos:**

↳**Al 20**: Eu sempre aviso meus amigos para não clicarem em *links* suspeitos.

→ **Análise**: Mostrou habilidades sólidas de comunicação ao alertar colegas sobre perigos *online*, refletindo a capacidade de compartilhar informações importantes de forma clara.

↳**Al 33**: Acho que deveríamos ter uma senha forte e não a compartilhar com ninguém.

- **Análise**: Demonstrou uma compreensão adequada de práticas seguras e soube expressar isso durante a discussão, mas a assertividade pode ser melhorada.
- **Fundamentação**:

A UNESCO (2017) destaca a responsabilidade da educação em promover habilidades de comunicação e colaboração, essenciais para a vida em sociedade e a prática de uma cidadania digital responsável.

→ Relação com a Estratégia Nacional de Educação para a Cidadania:

A promoção da comunicação e do relacionamento interpessoal é crucial para a educação para a cidadania, pois estas competências permitem que os alunos se envolvam em diálogos construtivos, essenciais para a vida em sociedade e para a prática de uma cidadania digital responsável.

3. Crescimento Pessoal e Autonomia

- **Atividades**:

↳Reflexão e *Feedback* após Visualização de Vídeos

↳Criação Visual no *Canva*

- **Intervenções dos Alunos:**

↳**Al 44**: Eu gosto de fazer *backup* dos meus arquivos regularmente para garantir que não os perca.

- **Análise**: Demonstra uma forte capacidade de autonomia na aplicação de práticas seguras, refletindo uma compreensão sólida dos conceitos.

↳- **Al 55**: Eu não sei se estou seguro ao usar as redes sociais.

- **Análise**: Indica a necessidade de orientação adicional para fortalecer a autonomia e a autoeficácia na gestão da segurança digital.
- **Fundamentação**:

- Pereira e Moura (2022): Salientam a importância de desenvolver a autonomia digital e a responsabilidade, algo que é essencial para alunos que ainda mostram incertezas quanto à aplicação prática dos conceitos de segurança.

→ Relação com a Estratégia Nacional de Educação para a Cidadania:

O crescimento pessoal e a autonomia são fundamentais para a formação de cidadãos responsáveis, capazes de tomar decisões informadas e éticas no ambiente digital, em consonância com os objetivos da Estratégia Nacional de Educação para a Cidadania.

4. Competências em Cidadania Digital

- **Atividades**:

↳Jogo de Segurança na *Internet*

↳Discussão sobre Direitos Digitais

- **Intervenções dos Alunos:**

↳**Al 60**: Eu sempre verifico se o *site* é seguro antes de colocar meus dados.

- **Análise**: Mostra uma aplicação prática das competências em cidadania digital, destacando a importância da privacidade e da segurança *online*.

↳**Al 70**: Acho importante denunciar *ciberbullying*, pois pode machucar muito as pessoas.

- **Análise**: Demonstrou uma compreensão profunda dos direitos digitais e a responsabilidade social *online*.
- **Fundamentação**:

A UNESCO (2017) enfatiza a importância de preparar os alunos para serem cidadãos digitais responsáveis, algo claramente refletido na forma como alguns alunos compreendem e aplicam práticas de segurança digital.

→ Relação com a Estratégia Nacional de Educação para a Cidadania:

A promoção da cidadania digital é central para a Estratégia Nacional de Educação para a Cidadania, que procura formar indivíduos capazes de atuar de forma consciente, crítica e ética no mundo digital, respeitando os direitos e deveres associados à vida *online*.

→ Integração com a Literatura

- Mattar et al. (2020) reforçam a necessidade de integrar práticas de segurança digital no currículo escolar, algo observado na variação das competências entre os alunos.

- A UNESCO (2017) sublinha a necessidade de preparar os alunos para os desafios digitais do século XXI, incluindo a promoção de cidadania digital.

- Pereira e Moura (2022) destacam a importância de promover autonomia e responsabilidade digital, essencial para o desenvolvimento de práticas seguras e eficazes entre os alunos.

→ Resultados e Implicações Pedagógicas

- **Variedade nos Desempenhos:**

↳**Al 33** e **Al 55**: mostram diferenças significativas na capacidade de comunicação e aplicação prática de conceitos, indicando a necessidade de abordagens pedagógicas mais personalizadas.

→ Eficácia das Estratégias Pedagógicas:

↳**Al 44**: demonstrou autonomia e aplicação prática dos conceitos aprendidos, refletindo a eficácia das atividades lúdicas e interativas.

↳**Al 12**: apesar de um bom entendimento dos conceitos, necessita de estratégias mais focadas em aprofundar a análise crítica.

→ Fundamentação:

Martins et al. (2017) destacam a importância de atividades que promovam a navegação segura e responsável, algo essencial para o desenvolvimento integral dos alunos.

Síntese dos Resultados do Desenvolvimento de Competências Digitais

A avaliação das atividades relacionadas com a segurança cibernética e com os perigos da rede possibilitou a análise das habilidades dos alunos em áreas importantes como raciocínio crítico, comunicação, independência e responsabilidade digital. Foi percebido que apresentaram um entendimento fundamental, porém diversificado, dos termos de segurança cibernética, onde alguns conseguiram identificar e evitar ameaças *online*, enquanto outros precisam de mais auxílio educativo.

Essas competências estão alinhadas com a ENEC e o PASEO. A análise destaca a importância de práticas de ensino apropriadas para incentivar uma cidadania digital responsável e consciente, capacitando os alunos para lidar com os desafios da rede mundial do uso de computadores.

5.1. EFICÁCIA DAS AÇÕES DE ALFABETIZAÇÃO DIGITAL NO 1.º CICLO

O foco deste projeto é avaliar a eficácia das iniciativas de alfabetização digital no aprimoramento da proficiência das competências em segurança digital dos alunos do 1.º CEB. Para atingir esse propósito, desdobraram-se três objetivos específicos, associados a determinadas atividades pedagógicas:

1. **Identificar as preconceções dos alunos sobre a segurança digital**: este objetivo é operacionalizado através do aumento da consciência sobre segurança digital, utilizando atividades como **Diagnóstico Inicial**. A atividade com ***Post-its*** (ANEXO C) foi desenvolvida para investigar as perceções iniciais dos alunos sobre os perigos da *internet*. Os alunos registaram palavras-chave, sobre segurança digital e proteção *online*, para avaliar o nível de conhecimento e planear intervenções. Tal abordagem está alinhada com as diretrizes da UNESCO (2017), que destacam a urgência de integrar a educação com competências básicas essenciais para enfrentar os desafios do século XXI, promovendo uma educação que se estende para além da transmissão de conhecimento, pensamento crítico e resolução de problemas.

2. **Descrever estratégias de integração da segurança digital no 1.º CEB**: Para incluir a segurança digital eficientemente em contexto escolar, foram realizadas as seguintes atividades: **Pesquisa na *Internet*** (ANEXO D), **Jogo de Segurança *Online*** (ANEXO E), **Visualização de Vídeos** (ANEXO F) e **uso no *Mentimeter*** (ANEXO K), como destacado por Mattar et al. (2020), que reforça a necessidade de equilibrar habilidades tecnológicas e pensamento crítico. Portanto, as atividades alinham-se às Áreas de Competência: **Informação e Comunicação**, **Desenvolvimento Pessoal e Autonomia**, e **Pensamento Crítico e Criativo**, estabelecidas no **PASEO**.

3. **Analisar em que medida o envolvimento dos alunos nas atividades de segurança digital contribui para o desenvolvimento de competências** As **Discussões em Grupo**, **Debate e Reflexão Final** e **Apresentação dos Resultados** foram essenciais para avaliar como a participação e o empenho dos alunos nas atividades de segurança digital. Esta abordagem segue as recomendações de Pereira e Moura (2022), sobre a importância de uma educação digital consciente. Estas ações promovem o desenvolvimento dos alunos, espelhando o interesse de uma educação além do ensino tradicional.

O projeto reafirma a relevância de aprendizagens que diligenciem a proteção digital, promovendo e fomentando a autonomia e pensamento crítico, competências essenciais

para a navegação segura na *internet*, conforme descrito por Martins et al. (2017) e Mattar et al. (2020). Assim sendo, as atividades solidificam o conhecimento dos alunos em segurança digital, preparando-os para enfrentar o mundo digital de forma segura.

As atividades realizadas tiveram como meta alcançar objetivos operacionais de implementar medidas de segurança sobre segurança cibernética e envolver os alunos, estimulando o desenvolvimento completo das habilidades essenciais para uma navegação segura e responsável na *Internet*

5.2. Alinhamento de Objetivos Educativos e Atividades em Segurança Digital no 1.º CEB

A Tabela 6 resume uma visão da relação entre os objetivos de aprendizagem em segurança digital no 1.º CEB, atividades de aprendizagem e a progressão das competências dos alunos. As atividades foram planeadas cuidadosamente para abordar as conceções dos alunos sobre segurança digital, incorporar medidas de segurança nas rotinas escolares diárias e promover competências como o pensamento analítico. Essas atividades tiveram um caráter educativo, também permitiram uma adaptação dinâmica, diversidade de métodos, como jogos, pesquisas e ferramentas digitais, *feedback* constante, visível na Tabela 6, garantindo que os conceitos fossem abordados de forma mais eficaz à medida que as atividades se desenrolavam.

A Tabela 6 destaca ainda a integração das estratégias no currículo e como elas abordaram as competências essenciais. Enquanto a Tabela 6 apresenta como as atividades influenciaram o desenvolvimento de competências, como pensamento crítico e tomada de decisão responsável. O envolvimento ativo dos alunos, observado nas atividades de **Visualização de Vídeos** e **Discussão e Reflexão Final**, foi fundamental para promover a autonomia e a capacidade de aplicar práticas seguras no ambiente digital.

Por fim, o *feedback* obtido através de ferramentas como o **Formulário no Google *Forms***, ***Nearpod*** e ***Mentimeter***, ajudaram a ajustar as atividades em tempo real, proporcionando uma visão das conceções que necessitavam de maior atenção, permitindo uma progressão contínua nas competências de segurança digital.

.

Tabela 6 - Síntese dos Objetivos e Estratégias de Segurança Digital no 1.º CEB

Objetivos	Descrição	Atividades / Anexos	Áreas de Competência	Autores
Identificação das Preconceções dos Alunos	Compreender o conhecimento prévio dos alunos sobre privacidade, proteção de dados e riscos *online*, articulando com o objetivo de ajustar as estratégias educativas para preencher lacunas e reforçar áreas de maior vulnerabilidade.	Atividade com Post-its (ANEXO C), Discussões Iniciais (ANEXO D)	Pensamento Crítico e Criativo, Desenvolvimento Pessoal e Autonomia	**Mattar et al. (2020)** destacam a importância da identificação das preconceções iniciais para ajustar as estratégias educativas.
Estratégias de Integração da Segurança Digital no 1.º CEB	Explorar a integração da segurança digital no currículo através de pesquisa orientada, jogos e debates, em articulação com o objetivo de desenvolver um currículo que fortaleça o entendimento dos alunos sobre os perigos *online* e as melhores práticas para se proteger.	Pesquisa - *Perigos* na Internet (ANEXO D), Jogo de Segurança na *Internet* (ANEXO E), Visualização de Vídeos (ANEXO F), *Mentimeter* (ANEXO K)	Informação e Comunicação, Relações Interpessoais, Saber Científico e Tecnológico	**UNESCO (2017)** e **Pereira e Moura (2022)** enfatizam a necessidade de estratégias pedagógicas inovadoras para integrar a segurança digital.
Qual é a eficácia das ações voltadas para a alfabetização das habilidades de segurança digital dos alunos do primeiro ciclo?	Avaliar como a participação ativa dos alunos contribui para o desenvolvimento de competências e a aplicação de práticas seguras, articulando com o objetivo de promover uma evolução no pensamento crítico, na tomada de decisões responsáveis, e na adoção de práticas seguras na internet.	Discussão e Reflexão Final (ANEXO M), Criação Visual no *Canva* (ANEXO L), Debate e Reflexão	Pensamento Crítico, Tomada de Decisão Responsável, Autonomia	**Ponte & Batista (2019)** e **Limnéll e Lindroth (2024)** discutem a importância do envolvimento ativo dos alunos para o desenvolvimento de competências digitais.

.

Tabela 6 - Relação entre Objetivos Educativos, Atividades de Aprendizagem e Desenvolvimento de Competências em Segurança Digital

Objetivo	Atividades	Descrição da Atividade	Justificação	Resultados Observados
i) Identificar as preconceções dos alunos sobre a segurança digital.	- Pesquisa na Internet - *Mentimeter*: Conhecendo e Combatendo os Riscos *Online* - Dia Internacional da Internet Segura - Atividade com *Post-its*	Atividade de pesquisa para identificar riscos *online*. Uso do *Mentimeter* para criar nuvens de palavras. Discussão com a GNR. Identificação de perigos na *Internet* por meio de *Post-its.*	As atividades esclareceram as noções previas dos alunos, estabelecendo uma base para a aprendizagem.	Alunos demonstraram uma compreensão inicial limitada, identificando principalmente riscos mais comuns.
ii) Descrever estratégias de integração da segurança digital no 1.º CEB.	- Pesquisa na *Internet* - Jogos de Segurança na *Internet* - Criação Visual no *Canva*	Atividades práticas e colaborativas usando ferramentas digitais para promover a segurança *online*. Criação de cartazes no *Canva*.	As estratégias envolveram os alunos em práticas de segurança digital com métodos diversificados e lúdicos	Alunos criaram recursos visuais que demonstraram entendimento de conceitos chave.
iii) Analisar em que medida o envolvimento dos alunos nas atividades contribui para o desenvolvimento de competências.	- Visualização de Vídeos - *Quiz* no *Nearpod* - Formulário no *Google Forms*: Avaliação da Eficácia das Atividades - Atividade com ***Post-its.***	Atividades interativas e de avaliação formativa com *quizzes* e debates. *Feedback* instantâneo com revisão de conceitos de segurança. Discussão e reflexão sobre os perigos identificados.	As atividades promoveram pensamento crítico, autonomia e comunicação	Melhorias notáveis na articulação de ideias sobre segurança *online* e maior confiança em discutir os temas abordados.

CONCLUSÃO

Durante a condução deste estudo, foram evidentes as práticas pedagógicas como essenciais para a promoção das competências digitais dos alunos do 1.º CEB. O primeiro objetivo, **Identificação das Preconceções dos Alunos**, foi cumprido através de atividades como debates iniciais e *post-its*, que possibilitaram o apanhado do conhecimento prévio dos alunos sobre os conceitos de privacidade, proteção de dados e riscos *online*, permitindo a adequação das práticas educativas a estabelecer de que forma as lacunas existentes poderiam ser abordadas e de que forma conseguiria reforçar as áreas mais vulneráveis.

O segundo objetivo, **Estratégias de Integração da Segurança Digital no 1.º CEB**, foi abordado de forma recorrente, através de atividades como jogos, pesquisas ou vídeos. Por exemplo, em diversas ocasiões, os alunos participaram de jogos interativos que simularam situações reais de risco *online*, incentivando decisões seguras. A reação dos alunos a essas atividades foi muito positiva, demonstrada pelo entusiasmo ao participar. Apesar de alguns alunos demonstrarem alguma dificuldade na compreensão de alguns conceitos mais abstratos. Com base no *feedback* dos alunos, que relataram dificuldades na compreensão de determinados conceitos, as atividades foram ajustadas, incorporando explicações mais acessíveis e exemplos práticos para facilitar a assimilação. Além disso, realizaram pesquisas sobre boas práticas digitais e assistiram a vídeos educativos que enfatizavam a importância da proteção *online*. Essas atividades contribuíram para o desenvolvimento das competências dos alunos, uma vez que se procurou melhorar a capacidade de pensamento crítico e a promoção de boas práticas de proteção em contexto digital.

O terceiro objetivo, **Analisar em que medida o envolvimento dos alunos nas atividades de segurança digital contribui para o desenvolvimento de competências**, referiu a necessidade da participação ativa dos alunos no desenvolvimento das suas competências digitais. Atividades como debates, criação visual no *Canva* aumentam a participação dos alunos, levando-os a aplicar de forma prática os seus saberes em diferentes sítios.

O **envolvimento dos alunos** nas atividades contribuiu diretamente para o desenvolvimento das suas competências digitais, refletido pelo seu **entusiasmo nas tarefas interativas** e **maior compreensão dos conteúdos abordados**.

Em conclusão, e dando resposta à questão de investigação. **Qual a eficácia das ações voltadas para a alfabetização das habilidades de segurança digital dos alunos do primeiro ciclo?,** podemos afirmar que as metodologias lúdicas e a participação ativa dos alunos foram extremamente importantes para que pudessem interiorizar os conceitos de segurança *online*. Estas metodologias lúdicas possibilitaram que as crianças adquirissem práticas de proteção de dados e prevenções de riscos, evidenciando a eficácia de tais metodologias. A pesquisa reitera a necessidade de integrar a formação digital no currículo escolar, de modo a permitir aos alunos tornarem-se mais críticos e responsáveis frente aos desafios da sociedade digital. Assim, a formação digital, desde o 1.º CEB, como um meio de formar a geração mais autónoma e bem-adaptada às tecnologias, é indispensável. Neste contexto, cabe à escola um papel de destaque, devendo garantir a continuidade dessas iniciativas para que as crianças, posteriormente, possam utilizar as suas competências digitais nas suas interações quotidianas em ambientes *online*.

Limitações

Embora tenha trazido resultados relevantes, o estudo, foi desenvolvido em quatro turmas, teve algumas limitações que ainda abrem espaço para melhorias consideráveis. Entre os desafios, destaca-se o de ter de pedir turmas de outros professores, o que limitou o envolvimento dos alunos e prejudicou uma possível construção de vínculo de confiança, fundamental para um trabalho de acompanhamento próximo e minucioso dos alunos no comportamento *online*. Adicionalmente, o estudo ocorreu quase exclusivamente no ambiente escolar, desprezando o contexto familiar, o qual tem um papel fundamental na formação de hábitos digitais seguros. A baixa participação das famílias, devida à falta de tempo, oportunidade e, possivelmente, a um desconhecimento sobre o papel que poderiam desempenhar, impediu que se registasse uma ação mais significativa no envolvimento dos pais na segurança na *internet* dos filhos. Este estudo ocorreu numa realidade socioeconómica relativamente homogênea, o que pode condicionar em grande parte a extensão das conclusões a outras realidades. Neste caso, o texto também sugere o desconhecimento da possibilidade do papel dos pais.

Propostas de trabalho futuro

1. **Turma única e constante**: Para resultados mais robustos, conta-se com a necessidade de turmas próprias, permitindo um acompanhamento contínuo e uma maior confiança dos alunos com o(s) pesquisador(es) para que se tenha dados mais profundos e seguros sobre o efeito das intervenções na segurança *online*.

2. **Participação das famílias**: Um ponto chave para o futuro é a participação ativa das famílias. Sabemos que o ambiente digital dos alunos não é exclusivo da escola; os pais têm um papel crucial na forma como eles utilizam a *internet* em casa. Chamar pais e cuidadores para discussões e intervenções sobre segurança na *Internet* aumentaria o efeito do estudo, tornando-o mais realista e abrangente.

3. **Análise Comportamental Fora da Escola**: A ampliação do estudo, a fim de analisar a forma como os alunos utilizam a *internet* fora do ambiente escolar, em casa ou em instituições públicas, é crucial para compreender as discrepâncias nos comportamentos considerando outros ambientes onde a supervisão e a legislação divergem profundamente.

4. **Diversidade Socioeconómica**: Deve-se desenvolver um futuro para o estudo incluindo escolas de diferentes ambientes socioeconómicos, ampliando a pesquisa para captar como elas percebem e implementam a segurança na *internet* em diferentes realidades, permitindo uma avaliação mais abrangente e representativa dos requerimentos para crianças de origens diversas.

5. **Intervenção familiar e educativa com Ferramentas Tecnológicas**: A utilização de novas tecnologias permitindo a monitorização e proteção *online* tanto em ambiente escolar quanto em casa seria uma enorme soma ao estudo, cujo efeito pode ser apreciado em termos de prevenção das ameaças *online*, oferecendo soluções práticas para a segurança digital utilizada por alunos em todos os ambientes da sua vida.

LISTA DE REFERÊNCIAS BIBLIOGRÁFICAS

Abreu, J., Dinis, R., & Teixeira, R. C. (2018). Recursos didáticos, experiências na construção e gestão de materiais pedagógicos inspirados no método de Singapura na educação pré-escolar e no 1.º ciclo do ensino básico. *Jornal Das Primeiras Matemáticas*, 65–106.

Almeida, M. S. C., Sousa Filho, L. F. de, Rabello, P. M., & Santiago, B. M. (2020). Classificação Internacional das Doenças - 11ª revisão. *Revista de Saúde Pública*, *54*, 104. https://doi.org/10.11606/s1518-8787.2020054002120

Alvarenga, F. R. V., & Rocha, J. M. S. (2023). Sharenting e a (in)violabilidade do direito de personalidade: aspectos quanto a atuação da rede de proteção dos direitos da criança e do adolescente. *Revista Foco*, *16*(5), e2088. https://doi.org/10.54751/revistafoco.v16n5-153

Apocalypse, S. M., Jorente, & Vicentini, M. J. (2022). O Método Design Thinking e a pesquisa em Ciência da Informação. *O Método Design Thinking e a Pesquisa Em Ciência Da Informação*, *27*, 1–21.

Ataide, M. W. O. de, Ferreira, A. R., & Francisco, D. J. (2019). A criança e a Internet: análise bibliográfica acerca dos riscos e benefícios percebidos por crianças. *Revista EDaPECI*, *19*(2), 165–176. https://doi.org/10.29276/redapeci.2019.19.211396.165-176

Ayinmoro, A. D., Uzobo, E., Teibowei, B. J., & Fred, J. B. (2020). Sexting and other risky sexual behaviour among female students in a Nigerian academic institution. *Journal of Taibah University Medical Sciences*, *15*(2), 116–121. https://doi.org/10.1016/j.jtumed.2020.02.007

Baldry, A. C., Sorrentino, A., & Farrington, D. P. (2019). Cyberbullying and cybervictimization versus parental supervision, monitoring and control of adolescents' online activities. *Children and Youth Services Review*, *96*, 302–307. https://doi.org/10.1016/j.childyouth.2018.11.058

Baričević, M., & Luić, L. (2023). From Active Learning to Innovative Thinking: The Influence of Learning the Design Thinking Process among Students. *Education Sciences*, *13*(5). https://doi.org/10.3390/educsci13050455

Barragem, R. (2024). *As 5 etapas do processo de Design Thinking . Fundação de Design de Interação* . IxDF. Https://Www.Interaction-Design.Org/Literature/Article/5-Stages-in-the-Design-Thinking-Process.

Barros, M. M. (2024). Resenha do artigo intitulado "Prevenção de crimes virtuais contra crianças e adolescentes." *Revista Processus Multidisciplina*, *V*(9).

Biombe, F. K. (2023). Ética e Deontologia Profissional na Educação: revisão bibliográfica narrativa. *Revista de Ciências de Saúde Da Universidade Lúrio*, 1–6. https://doi.org/10.5281/zenodo.10051129

Bittencourt, F. D., & Pimenta, S. P. M. (2023). A proteção da criança e do adolescente diante do crime cibernético de comercialização de pornografia infantil: a efetividade do ordenamento jurídico brasileiro. *Anais Da Mostra Científica* , *15*(1), 1–21. https://estacio.periodicoscientificos.com.br/index.php/

Caseiro, I. B. (2021). Tertúlia EDJ A Segurança do Ciberespaço Europeu. In *Ministério da Defesa Nacional* (pp. 1–9).

Chang, Y. shan, Kao, J. Y., & Wang, Y. Y. (2022). Influences of virtual reality on design creativity and design thinking. *Thinking Skills and Creativity*, *46*. https://doi.org/10.1016/j.tsc.2022.101127

Chaves-Álvarez, A. L., Morales-Ramírez, M. E., & Villalobos-Cordero, M. (2020). Ciberbullying desde la perspectiva del estudiantado: "lo que vivimos, vemos y

hacemos.” *Revista Electrónica Educare*, *24*(1), 1–24. https://doi.org/10.15359/ree.24-1.3
Chicava, A. K. A., & Nhanombe, A. A. (2020). John Dewey e Paulo Freire: duas visões da educação. *Revista Amor Mundi*, *1*(1), 63–74. https://doi.org/10.46550/amormundi.v1i1.3
Conselho Nacional de Educação. (2023). Recomendação n.º 3/2023 - Uma Infraestrutura Digital para o Sistema de Educação e Formação. In *Diário da República, 2.ª série (N.º 231* (pp. 176–183).
Costa, T. A. F., & Badaró, A. C. (2021). Impacto do uso de tecnologia no desenvolvimento infantil: uma revisão de literatura. In *Cadernos de Psicologia* (Vol. 3, Issue 5, pp. 234–255).
Cruz, E., & Costa, F. A. (2022). Referencial de Competências Digitais para Alunos do 1.º CEB. Projeto Escol@s Digitais. In *Referencial de Competências Digitais para Alunos do 1.º CEB* (Vol. 1, pp. 1–10). https://doi.org/10.13140/RG.2.2.12562.53444
Cunha, E. de P., Moreira, C. A., Vilela, G. P. de A., Lorrane, J., Silva, J. L. M., & Carneiro, S. de S. (2024). Os instrumentos da avaliação no 1º ciclo de alfabetização. *Revista Eletrônica Interdisciplinar*, 159–170.
DQInstitute. (2020). 2020COSIReport. In *#DQEveryChild* (pp. 2–15).
Duarte, A. P., Barbas, J., Santos, J., Picoito, J. M., Saraiva, M. F., Azevedo, L., Pereira, L. M., Meireles, P., & Mendonça, P. (2022). Referencial de educação para a segurança, a defesa e a paz. In Ministério da Educação (Ed.), *Ministério da Defesa Nacional*.
Eisenstein, E. (2023). Crianças, adolescentes e a era digital. *Revista Acadêmica Licencia&acturas*, *11*(1), 7–14. https://doi.org/10.55602/rlic.v11i1.283
Farias, A. N., Impolcetto, F. M., & Benites, L. C. (2020, September 18). A análise de dados qualitativos em um estudo sobre educação física escolar: o processo de codificação e categorização. *Pensar a Prática*, *23*. https://doi.org/10.5216/rpp.v23.57323
Farias, M. S. F. de, & Mendonça, A. P. (2021). Design Thinking como percurso metodológico para construção de produto educacional. *Revista de Estudos e Pesquisas Sobre Ensino Tecnológico (Educitec))*, *7*, e103621. https://doi.org/10.31417/educitec.v7.1036
Farias, F. L. de O., Medeiros, N. A. A. de, Rocha, S. L. da, Medeiros, D. F. de, Nóbrega, E. C. da, Burlamaqui, A., & Madeira, C. (2019). Self Protect: Um jogo para auxílio no ensino de conceitos relacionados a Segurança na Internet para Crianças e Adolescentes. In *Instituto Metrópole Digital –Universidade Federal do Rio Grande do Norte* (pp. 246–255). Sociedade Brasileira de Computacao - SB. https://doi.org/10.5753/cbie.wie.2019.246
Filho, E. B. dos S., Lira, E. G., Gonçalves, F., Santos, L. C. B., & Silva, S. da. (2024). Design Thinking e metodologias ativas na educação do século XXI. *Revista Ilustração*, *5*(1), 217–223. https://doi.org/10.46550/ilustracao.v5i1.265
Filho, J. H. L., & Cardoso, L. M. (2024). Tecnologias e educação na práxis docente: pertinência do letramento digital e da formação continuada para o desenvolvimento de habilidades e competências tecnológicas. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, *9*(12), 782–806. https://doi.org/10.51891/rease.v9i12.12590
França, A. de, Costa, F. L. P., Costa, R. dos S., Mota, W. de L., Denise, M., & Gutierrez, D. M. D. (2022). A observação participante: um panorama histórico-

conceitual do uso da técnica. In *RECH-Revista Ensino de Ciências e Humanidades –Cidadania, Diversidade e Bem Estar: Vol. VI* (Issue 2, pp. 106–117).

Francisco, D. J., Ferreira, A. R., & Azevedo, E. (2021). Analise de Conteúdo: como podemos analisar dados no campo da educação e tecnologias. In *Metodologia de pesquisa científica em informática na educação: Abordagem qualitativa. SBC*.

Freire, K. M. de A., Menezes, N. L. B. de, Moraes, L. S., Neto, R. A. dos R., Santos, M. M. de O., & Amorim, L. M. (2023). O uso da tecnologia na construção de ambientes de aprendizagem colaborativos e inclusivos. *Revista Internacional de Estudos Científicos*, *1*(2), 51–70. https://doi.org/10.61571/riec.v1i2.118

Freitas, M. S., E Silva, W. de Q., Rodrigues, A. M., Araújo, C. C. da S., Aguiar, V. C. F., Moura, J. B. F., Araújo, S. B., & Soares, S. L. (2023). Tecnologias digitais: mediações pedagógicas no combate à evasão escolar. *Cuadernos de Educación y Desarrollo*, *15*(9), 8024–8043. https://doi.org/10.55905/cuadv15n9-004

García Aretio, L. (2019). Necesidad de una educación digital en un mundo digital. *RIED. Revista Iberoamericana de Educación a Distancia*, *22*(2), 9. https://doi.org/10.5944/ried.22.2.23911

Gomes, G. F., & Souza, R. A. C. de. (2022). Transformação Digital na Educação para fomentar Competências Digitais. *Anais Estendidos Do XI Congresso Brasileiro de Informática Na Educação* , 62–73. https://doi.org/10.5753/cbie_estendido.2022.226361

Hoernig, A. M. (2021). Diário de bordo Desenvolvendo habilidade de atenção e percepção. *Didácticas Específicas*, *25*, 101–127. https://doi.org/10.15366/didacticas2021.25.006

Jackman, J. A., Gentile, D. A., Cho, N.-J., & Park, Y. (2021). Addressing the digital skills gap for future education. *Nature Human Behaviour*, *5*(5), 542–545. https://doi.org/10.1038/s41562-021-01074-z

Júnior, A. P. de C. (2020). Competências digitais de professores: análise e comparação de matrizes do CIEB e da Comissão Europeia. In *Educação como (re)Existência: mudanças, conscentização e conhecimentos* (pp. 1–12).

Júnior, R. R. (2021). Segurança digital e a educação do século XXI. In *MUST UNIVERSITY* (pp. 1–13).

Leaning, M. (2019). An Approach to Digital Literacy through the Integration of Media and Information Literacy. *Media and Communication*, *7*(2), 4–13. https://doi.org/10.17645/mac.v7i2.1931

Lewrick, M., Link, P., & Leifer, L. (2020). Tools Quickfinder Matrix. In *Wiley* (pp. 1–316).

Limnéll, J., & Lindroth, M. (2024). Competências do Cibercidadão e o seu Desenvolvimento na União Europeia. In *cyber-citizen.eu*.

Loureiro, J. L. de A., Silva, T. C., & Ulysses, P. D. A. (2021). Observação Participante e Diário de Campo: quando utilizar e como analisar? *Métodos de Pesquisa Qualitativa Para Etnobiologia*, 95–112. https://www.researchgate.net/publication/351492815

Machado, J. C., Polizello, Â. A. de A., Silva, J. A. da, Moura, M. A. A. de, & Saraiva, N. S. (2023). Cidadania digital: o uso das tecnologias no ambiente escolar e os riscos do mundo digital. *Revista Amor Mundi*, *4*(11), 59–65. https://doi.org/10.46550/amormundi.v4i11.374

Malecki, W. P., Kowal, M., Dobrowolska, M., & Sorokowski, P. (2021). Defining Online Hating and Online Haters. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.744614

Martins, G. d´Oliveira, Gomes, C. A. S., Brocardo, J. M. L., Pedroso, J. V., Carrillo, J. L. A., Silva, L. M. U., Encarnação, M. M. G. A. de, Horta, M. J. do V. C., Calçada, M. T. C. S., Nery, R. F. V., & Rodrigues, S. M. C. V. (2017). Perfil dos Alunos À Saída da Escolaridade Obrigatória. *Ministério Da Educação*, 1–30.

Mattar, J., Piovezan, M. B., Souza, S., Santos, C. C., & Santos, A. I. dos. (2020). Apresentação crítica do Quadro Europeu de Competência Digital (DigComp) e modelos relacionados. *Research, Society and Development*, *9*(4), e172943062. https://doi.org/10.33448/rsd-v9i4.3062

Medon, F. (2022). (Over) Shareting: a superexposição da imagem e dos dados pessoais de crianças e adolescentes a partir de casos concretos. *Revista Brasileira de Direito Civil*, *32*(02). https://doi.org/10.33242/rbdc.2022.02.009

Meirinhos, M., & Osório, A. (2015). Práticas educativas com TIC: uma proposta de ação. *Revista de Estudios e Investigación En Psicología y Educación*, 120–124. https://doi.org/10.17979/reipe.2015.0.13.452

Melo, J. de F. R. de, & Vieira, N. M. C. (2020). O paradigma da investigação qualitativa e a forma de garantir a validade e a fidelidade nos estudos científicos de natureza qualitativa / The paradigm of qualitative research and the way to guarantee validity and fidelity in qualitative scientific studies. *ID on Line REVISTA DE PSICOLOGIA*, *14*(52), 549–557. https://doi.org/10.14295/idonline.v14i52.2730

Mesquita, S. S. de A., Pischetola, M., Vilaça, M. L. C., & Gonçalves, L. A. C. (2022). *Os sentidos da escola na cultura digital: possibilidades de mutações* (M. L. C. Vilaça, Ed.). Editora Pontocom. https://www.researchgate.net/publication/361560217

Moro, I. B. P. (2021). Clube de segurança: uma abordagem para a educação em segurança da informação. In *Anais do IV Congresso Internacional Uma Nova Pedagogia para a Sociedade Futura* (pp. 690–693). Anais IV Congresso Internacional Uma Nova Pedagogia para a Sociedade Futura. http://www.recantomaestro.com.br

Nascimento, J. L. do, & Feitosa, R. A. (2020). Metodologias ativas, com foco nos processos de ensino e aprendizagem. *Research, Society and Development*, *9*(9), e622997551. https://doi.org/10.33448/rsd-v9i9.7551

Neumann, D. M. C., & Missel, R. J. (2019). Família Digital: A Influência da Tecnologia nas Relações Entre Pais e Filhos Adolescentes. In *Pensando Famílias* (pp. 75–91).

Noleto, M. J., Gomes, M. R. O., & Braga, M. (2019). Manual para garantir inclusão e equidade na educação. In *Organização das Nações Unidas para a Educação, a Ciência e a Cultura*. Organização das Nações Unidas para a Educação, a Ciência e a Cultura.

Organização das Nações Unidas para a Educação, a C. e a C. (2019). Segurança online de crianças e adolescentes: minimizar o risco de violência, abuso e exploração sexual online. In *Broadband Commission for Sustainable evelopment* (pp. 1–102). Broadband Commission for Sustainable Development. www.unesco.org/open-access/

Pande, M., & Bharathi, S. V. (2020). Theoretical foundations of design thinking – A constructivism learning approach to design thinking. *Thinking Skills and Creativity*, *36*, 100637. https://doi.org/10.1016/j.tsc.2020.100637

Panke, S. (2019). Design Thinking in Education: Perspectives, Opportunities and Challenges. *Open Education Studies*, *1*(1), 281–306. https://doi.org/10.1515/edu-2019-0022

Pereira, N. X., & Oliveira, G. S. De. (2024). Observação e análise documental as suas contribuições na pesquisa científica. *Revista Multidisciplinar Humanidades e Tecnologias (FINOM)*, *46*, 1809–1628. https://doi.org/10.5281/zenodo.10565180

Pereira, S., & Moura, P. (2022). Estudo de impacto das iniciativas do Centro de Sensibilização Seguranet. *Ministério Da Educação - Direção-Geral Da Educação*, 1–213.

Picone, I., Kleut, J., Pavlíčková, T., Romic, B., Møller Hartley, J., & De Ridder, S. (2019). Small acts of engagement: Reconnecting productive audience practices with everyday agency. *New Media & Society*, *21*(9), 2010–2028. https://doi.org/10.1177/1461444819837569

Pinheiro, R. S. de O., & Silva, G. P. da. (2020). A importância do uso das TICS na educação básica: uso das TICS como instrumento facilitador da aprendizagem. *THOUGHT - World Education in Debate*, *1*(1), 217–225. https://doi.org/10.29327/227764.1.1-24

Pires, S. M. B. (2019). As TIC no currículo escolar ICT in the school curriculum. In *Eduser: Revista de educação* (Vol. 1, Issue 1, pp. 1–12). http://www.eduser.ipb.pt

Ponte, C., & Batista, S. (2019). EU Kids Online Portugal – 2018. Usos, competências, riscos e mediações da internet reportados por crianças e jovens (9-17 anos). *EU Kids Online e NOVA FCSH*.

Ponte, C., Simões, J. A., Batista, S., & Castro, T. S. (2018). Implicados, intermitentes, desengajados? Estilos de mediação de pais de crianças de 3-8 anos que usam a internet. *Sociologia, Problemas e Práticas*, *91*. https://doi.org/10.7458/SPP20199112332

Pontes, V. M. A. da S. (2023). As inovações tecnológicas na educação: o uso de tecnologia e novas metodologias. *Revista Ilustração*, *4*(2), 125–129. https://doi.org/10.46550/ilustracao.v4i2.164

Praxedes, G. F., Silva, C. K. da, Magalhães, P. S., Silva, S. da, & Santos, V. L. S. dos. (2023). Desafios éticos e oportunidades na educação digital e cidadania. *Revista Amor Mundi*, *4*(7), 87–94. https://doi.org/10.46550/amormundi.v4i7.298

Prensky, M. (2019). What the world needs from education: Eight billion unique, symbiotic human hybrids constantly adding value to their world. We can make it happen. In *Comunidade de Aprendizagem (COL)* (pp. 1–12). Comunidade de Aprendizagem (COL). http://hdl.handle.net/11599/3462

Rathee, D., & Mann, S. (2022). Detection of E-Mail Phishing Attacks-using Machine Learning and Deep Learning. In *International Journal of Computer Applications* (Vol. 183, Issue 47). https://tiny.qe/

Ribeiro, G. A. M., Cordeiro, P. I. R. V., & Fumach, D. M. (2022). O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal*, *8*(3). https://doi.org/10.22197/rbdpp.v8i3.723

Rosado, K. M. L., & Dias, C. da C. (2024). A Metodologia Design Thinking nas pesquisas científicas e a pertinência de sua apropriação pela Ciência da Informação. *Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência Da Informação*, *29*. https://doi.org/10.5007/1518-2924.2024.e96222

Rui, M., José, V., Barbas, M. P., Santos, J., Baptista, M. E., Rei, M., Valério, R., & Maurício, S. (2020). Estudo sobre os perigos da Internet: o fenómeno do catfhishing em contexto de produção multimédia em educação. *Edição Temática: Ciências Sociais e Humanas*, *8*(2), 47–56.

Sá, P., Costa, A. P., & Moreira, A. (2021). Reflexões em torno de Metodologias de Investigação: recolha de dados. In *Universidade de Aveiro* (Vol. 2, pp. 1–105).

Sales, M. V., Moreira, J. A. M., & Rangel, M. (2019). Competências digitais e as demandas da sociedade contemporânea: diagnóstico e potencial para formação de professores do Ensino Superior da Bahia. *Série-Estudos - Periódico Do Programa de Pós-Graduação Em Educação Da UCDB*, 89–120. https://doi.org/10.20435/serie-estudos.v24i51.1290

Sales, S. S., Costa, T. M. da, & Gai, M. J. P. (2021). Adolescentes na Era Digital: Impactos na Saúde Mental. *Research, Society and Development*, *10*(9), e15110917800. https://doi.org/10.33448/rsd-v10i9.17800

Sani, A. I., Vieira, A. P., & Dinis, M. A. P. (2021). Social Networks, the Internet, and risks: Portuguese parents' perception of online grooming. *Revista Avaliação Psicológica*, *20*(4). https://doi.org/10.15689/ap.2021.2004.22001.10

Santos, B. S. dos, Spagnolo, C., & Bücker, C. (2020). Metodologias criativas no processo de ensino e de aprendizagem na educação básica. *Revista Teias*, *21*(63), 410–424. https://doi.org/10.12957/teias.2020.50873

Santos, D. S. dos, Barros, A. M. R., Parreira, D. C., Costa, J. W. M., & Sales, R. S. (2023). Tecnologias, Cidadania e Educação. *Revista Amor Mundi*, *4*(7), 11–22. https://doi.org/10.46550/amormundi.v4i7.290

Santos, S. D. dos, Barros, A. M. R., Parreira, D. C., Costa, J. W. M., & Sales, R. S. (2023). Tecnologias, Cidadania e Educação: Estratégias para lidar com os riscos das práticas digitais nas instituições escolares. *Revista Amor Mundi*, *4*(7), 11–22. https://orcid.org/0009-0009-7009-1570

Sátyro, N. G. D., & D'Albuquerque, R. W. (2020). O que é um Estudo de Caso e quais as suas potencialidades? In *Sociedade e Cultura* (Vol. 23, pp. 1–33). https://doi.org/10.5216/sec.v23i.55631

Schlemmer, E., Morgado, L. C., & Moreira, J. A. M. (2020). Educação e transformação digital: o habitar do ensinar e do aprender, epistemologias reticulares e ecossistemas de inovação. *Interfaces Da Educação*, *11*(32), 764–790. https://doi.org/10.26514/inter.v11i32.4029

Silva, L. H. de L., & França, R. S. de. (2023). Educação para a Cidadania Digital: Um mapeamento sobre as práticas de ensino para promover a segurança e a privacidade de dados. *Anais Do XXXI Workshop Sobre Educação Em Computação (WEI 2023)*, 533–544. https://doi.org/10.5753/wei.2023.230839

Sobrinho, J. R. N., & Grott, S. (2022). Os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor. In *Revista Cientifica Multidisciplinar do CEAP* (Vol. 4, Issue 2, pp. 1–10).

Sølvik, R. M., & Glenna, A. E. H. (2022). Teachers' potential to promote students' deeper learning in whole-class teaching: An observation study in Norwegian classrooms. *Journal of Educational Change*, *23*(3), 343–369. https://doi.org/10.1007/s10833-021-09420-8

Souza, R. F. de. (2000). Inovação educacional no século XIX: a construção do currículo da escola primária no Brasil. *Cadernos CEDES*, *20*(51), 9–28. https://doi.org/10.1590/S0101-32622000000200002

Souza, R. de, Leonardo, de A. F., Freitas, de A. F., & Obladen, C. (2022). A construção da cibersoberania na União Europeia: a cibersegurança e a integração do ciberespaço europeu. In *Revista de Direito Internacional* (3rd ed., pp. 256–270). Revista de Direito Internacional.

Stumm, L. C., & Wagner, A. (2019). Uso da abordagem do design thinking na educação. *Boletim Técnico-Científico*, *5*(1). https://doi.org/10.26669/2359-2664.2019.213

Tavares, V. dos S., & Melo, R. B. de. (2019). Possibilidades de aprendizagem formal e informal na era digital: o que pensam os jovens nativos digitais? *Psicologia Escolar e Educacional*, *23*. https://doi.org/10.1590/2175-35392019013039

Tocantins, G. M. de O., & Wiggers, I. D. (2021). Infância e mídias digitais: histórias de crianças e adolescentes sobre seus cotidianos. *Cadernos CEDES*, *41*(113), 76–83. https://doi.org/10.1590/cc231445

Trindade, S. D., & Moreira, J. A. (2017). *Competências de aprendizagem e tecnologias digitais* (pp. 99–113). https://link.springer.com/content/pdf/10.1007%2F978-3-319-04093-6.pdf

Tristão, L. A., Iossi Silva, M. A., De Oliveira, W. A., Dos Santos, D., & Da Silva, J. L. (2022). Bullying e cyberbullying: intervenções realizadas no contexto escolar. *Revista de Psicología*, *40*(2), 1047–1073. https://doi.org/10.18800/psico.202202.015

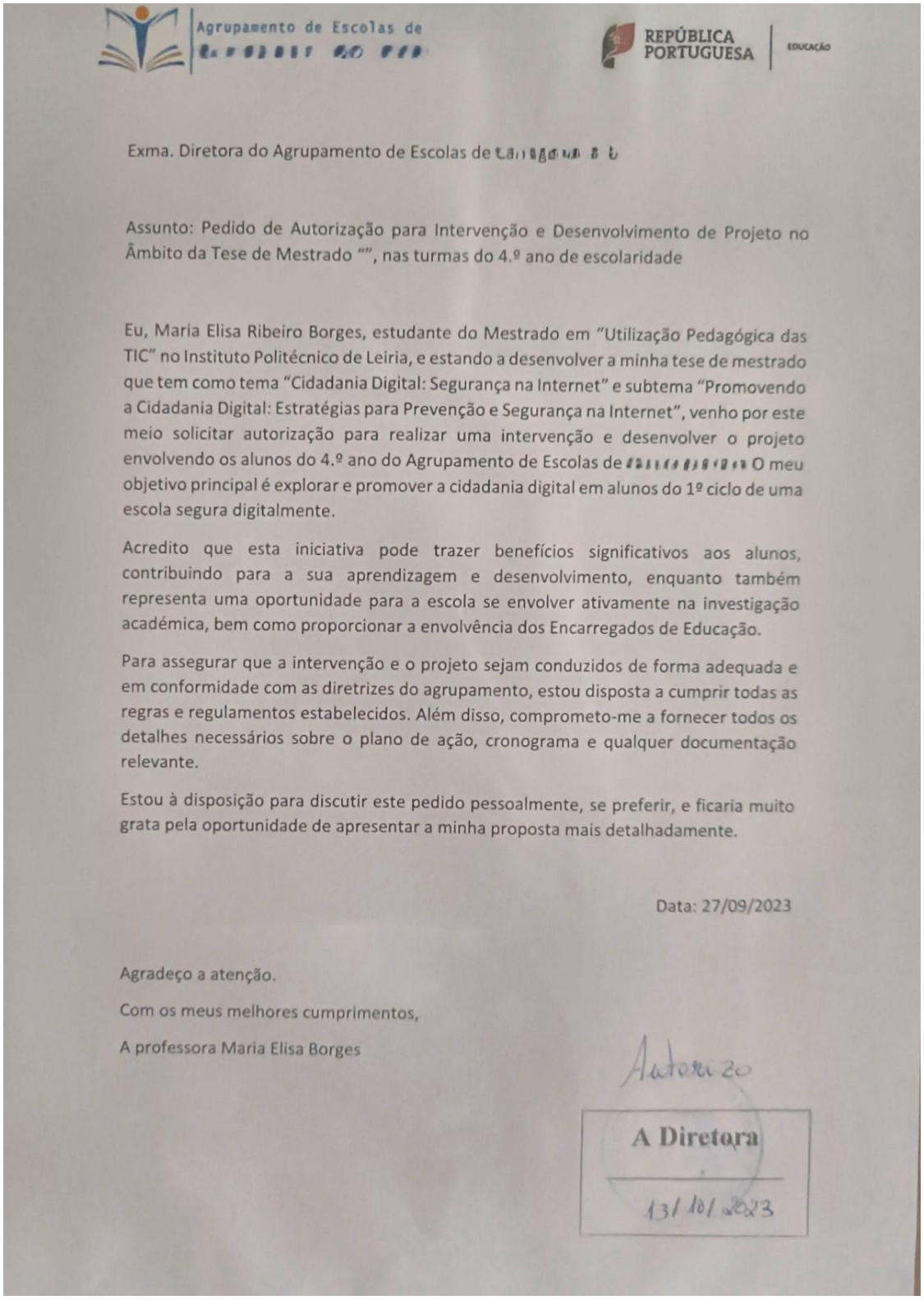
UNESCO. (2017). *Education for Sustainable Development Goals: Learning Objectives*.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." *Heliyon*, *5*(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Vilaça, M. L. C., & Araujo, E. V. F. de. (2016). *Tecnologia, Sociedade e Educação na Era Digital* (Universidade UNIGRANRIO, Ed.). Duque de Caxias.

ANEXOS

ANEXO A – AUTORIZAÇÃO DIREÇÃO AGRUPAMENTO



Agrupamento de Escolas de [redacted]

REPÚBLICA PORTUGUESA | EDUCAÇÃO

Exma. Diretora do Agrupamento de Escolas de [redacted]

Assunto: Pedido de Autorização para Intervenção e Desenvolvimento de Projeto no Âmbito da Tese de Mestrado "", nas turmas do 4.º ano de escolaridade

Eu, Maria Elisa Ribeiro Borges, estudante do Mestrado em "Utilização Pedagógica das TIC" no Instituto Politécnico de Leiria, e estando a desenvolver a minha tese de mestrado que tem como tema "Cidadania Digital: Segurança na Internet" e subtema "Promovendo a Cidadania Digital: Estratégias para Prevenção e Segurança na Internet", venho por este meio solicitar autorização para realizar uma intervenção e desenvolver o projeto envolvendo os alunos do 4.º ano do Agrupamento de Escolas de [redacted] O meu objetivo principal é explorar e promover a cidadania digital em alunos do 1º ciclo de uma escola segura digitalmente.

Acredito que esta iniciativa pode trazer benefícios significativos aos alunos, contribuindo para a sua aprendizagem e desenvolvimento, enquanto também representa uma oportunidade para a escola se envolver ativamente na investigação académica, bem como proporcionar a envolvência dos Encarregados de Educação.

Para assegurar que a intervenção e o projeto sejam conduzidos de forma adequada e em conformidade com as diretrizes do agrupamento, estou disposta a cumprir todas as regras e regulamentos estabelecidos. Além disso, comprometo-me a fornecer todos os detalhes necessários sobre o plano de ação, cronograma e qualquer documentação relevante.

Estou à disposição para discutir este pedido pessoalmente, se preferir, e ficaria muito grata pela oportunidade de apresentar a minha proposta mais detalhadamente.

Data: 27/09/2023

Agradeço a atenção.

Com os meus melhores cumprimentos,

A professora Maria Elisa Borges

Autorizo

A Diretora

13/10/2023

ANEXO B – AUTORIZAÇÃO ENCARREGADOS DE EDUCAÇÃO

Identificação do Investigador: Maria Elisa Ribeiro Borges, Professora do 1.º Ciclo do Agrupamento de [redacted]

Título do estudo: Cidadania Digital: Segurança na Internet no 1.º CEB

Enquadramento: Este estudo é conduzido no âmbito do Mestrado em Utilização Pedagógica das TIC do Instituto Politécnico de Leiria, focando-se na educação em segurança digital para alunos do 4.º ano de escolaridade do Agrupamento de Escolas de [redacted]. A orientadora do estudo é a Dr.ª Carla Freire, e a investigadora responsável é a Professora Maria Elisa Ribeiro Borges.

Explicação do estudo: O estudo Cidadania Digital: Segurança na Internet no 1.º CEB visa compreender a consciência e as práticas de segurança na internet entre alunos do 4.º ano de escolaridade do agrupamento. O foco é avaliar a familiaridade dos alunos com conceitos de segurança digital e sua habilidade em navegar de forma segura na internet.

Para atingir esse objetivo, serão utilizados os seguintes métodos de pesquisa, adaptados para serem acessíveis e apropriados para alunos do 4.º ano:

1. Discussões Guiadas em Sala de Aula: Serão realizadas sessões de discussão em grupo nas salas de aula, onde os alunos poderão compartilhar suas experiências e conhecimentos sobre o uso da internet. Estas discussões serão guiadas por perguntas simples e diretas para facilitar a participação de todos os alunos.

2. Atividades Interativas: Atividades práticas e lúdicas serão realizadas para avaliar o conhecimento dos alunos sobre segurança na internet. Isso pode incluir jogos educativos, questionários interativos e exercícios de simulação de situações online.

3. Entrevistas Breves e Informais com Alunos: Alguns alunos serão escolhidos aleatoriamente para entrevistas curtas e informais. Estas entrevistas serão conduzidas de maneira amigável e não-intrusiva para entender melhor as perceções individuais e experiências dos alunos relacionadas à segurança na internet.

4. Feedback dos Professores: Os professores das turmas envolvidas também fornecerão feedback sobre o comportamento dos alunos em relação ao uso da internet e a consciência sobre segurança digital, baseando-se em observações diárias.

O estudo ocorrerá nas salas de aula do agrupamento, proporcionando um ambiente familiar e seguro para os alunos. Este método permite uma observação natural e

interações autênticas. A duração do estudo será de aproximadamente três meses, permitindo uma análise aprofundada e contínua.

Os dados recolhidos serão tratados com a máxima confidencialidade e usados exclusivamente para os fins deste estudo. A responsável pelo cumprimento do Regulamento Geral de Proteção de Dados (RGPD) e pela condução ética do estudo é a Professora Maria Elisa Ribeiro Borges.

Estes métodos foram escolhidos por serem mais adequados para o público-alvo do estudo e por facilitarem a recolha de dados de maneira eficaz e eticamente responsável.

Confidencialidade e anonimato: Asseguramos a confidencialidade dos dados e o uso exclusivo para este estudo. Os participantes serão anonimizados e a identificação dos alunos nunca será divulgada publicamente.

Disponibilidade: Para esclarecer quaisquer dúvidas, entre em contato com a Professora Maria Elisa Ribeiro Borges pelo telefone da escola [REDACTED] ou e-mail [REDACTED].

Por favor, leia com atenção a informação. Se achar que algo está incorreto ou que não está claro, não hesite em solicitar mais informações. Se concorda com a proposta que lhe foi feita, queira assinar este documento.

Consentimento do participante

Declaro ter lido e compreendido este documento, bem como as informações verbais que me foram fornecidas pela pessoa que acima assina. Foi-me garantida a possibilidade de, em qualquer altura, recusar participar no estudo Cidadania Digital: Segurança na Internet no 1.º CEB sem qualquer tipo de consequências. Desta forma, aceito participar neste estudo e permito a utilização dos dados, que de forma voluntária forneço, confiando em que apenas serão utilizados para fins científicos e publicações que delas decorram e nas garantias de confidencialidade e anonimato que me são dadas pela investigadora.

Nome: … … ……… … … … … … …… … … … … … … … … … … … … … … … …… … … … … … …… … … … …

Assinatura: … … … … … … … … … … … … … … … …... … … … … ... … … … … … … … … …… … … … … …

Data: …… /…… /……….

SE NÃO FOR O PRÓPRIO A ASSINAR POR IDADE OU INCAPACIDADE (se o menor tiver discernimento deve também assinar em cima, se consentir)

NOME: …

BI/CC N.º: …

DATA OU VALIDADE …… /…… /……….

GRAU DE PARENTESCO OU TIPO DE REPRESENTAÇÃO: … … … … … … … … … … … … … … … … …

ASSINATURA …… … … … … … …… …

ANEXO C - PLANIFICAÇÃO DA AULA – TEMA: ATIVIDADE COM *POST-ITS*

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação
DESCRIÇÃO		
1.ª aula	**DURAÇÃO:** 50 minutos	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Segurança, Responsabilidade e respeito em ambientes digitais	Pensamento crítico e criativo	Identificação de Perigos: Alunos usam ***Post-its*** para escrever individualmente palavras-chave sobre perigos na internet, incluindo, por ex. *phishing*, *cyberbullying*, *malware*, *spyware*, vírus, *ransomware*, *hacking*, engenharia social, privacidade de dados, segurança de redes, golpes *online*, *catfishing*, invasão de privacidade, *sexting* e pornografia infantil.	15 min	***Post-its***, marcadores	Qualidade das palavras-chave escolhidas.
Investigar e Pesquisar	Informação e comunicação	Agrupamento por Temas: Alunos colocam ***Post-its*** no quadro branco, agrupando-os por temas semelhantes para identificar os tópicos mais comuns e os menos discutidos.	10 min	Quadro branco	Eficácia na organização e agrupamento das informações.
Colaborar e comunicar	Relacionamento interpessoal	Discussão em Grupo: Condução de uma discussão em grupo, onde os alunos compartilham e debatem as escolhas das palavras-chave, explorando diferentes perigos identificados.	20 min	Espaço de discussão em grupo	Participação ativa e contribuição na discussão.
Criar e inovar	Pensamento crítico e criativo	Reflexão e *Feedback*: Após a discussão, os alunos podem criar um breve resumo ou reflexão sobre o que aprenderam e como isso afeta a sua perceção de segurança na internet.	5 min	Papel, canetas	Compreensão e reflexão sobre o tema.

ANEXO C1 - GRELHA DE ANÁLISE DE CONTEÚDO - TEMA: ATIVIDADE COM *POST-ITS*

Categoria	Subcategorias	Indicadores		Unidades de Contexto
Perigos na Internet	**Identificação de Perigos**	*Phishing* *Cyberbullying* *Malware* *Spyware* Vírus *Ransomware* *Hacking* Roubo de Identidade Fraude *Online* Exposição a Conteúdo Inapropriado		Professora: Escrevam palavras-chave sobre perigos na internet que vocês conhecem. Pensem em termos como *phishing*, *cyberbullying*, *malware*, etc. Al 5: *Phishing*. Al 12: *Cyberbullying*. Al 20: *Malware*. Aluno 33: Spyware. Al 44: Vírus. Al 55: *Ransomware*. Aluno 60: *Hacking*. Al 15: Roubo de identidade. Al 25: Fraude *online*. Al 50: Exposição a conteúdo inapropriado.
		Capacidade de agrupar e identificar diferentes tipos de perigos online		Professora: Vamos agrupar os Post-its por temas semelhantes. Al 1: O meu é sobre privacidade de dados. Al 2: O meu é sobre *hacking*. Al 3: O meu é sobre *malware* e vírus. Al 40: Privacidade de dados é importante para proteger a nossa informação pessoal. Al 52: *Hacking* pode invadir os nossos computadores. Al 6: Malware e vírus podem estragar os nossos computadores.
	Agrupamento por temas	4.º A	**Privacidade *Online* (**Al 12) ***Cyberbullying*** (Al 12) **Perigos *Online*** (Al 17) **Informação Pessoal (**Al 20)	Al 12: Privacidade de dados é essencial para evitar que estranhos acedem as nossas informações pessoais. Al 12: O *cyberbullying* pode afetar a vida das pessoas de forma muito negativa, por isso é importante conhecê-lo e preveni-lo. Al 17: Devemos conhecer todos os perigos que existem *online*, como *malware* e *phishing*, para nos protegermos. Al 20: Nunca devemos partilhar informações pessoais na *internet*, pois isso pode levar ao roubo de identidade.

Categoria	Subcategorias	Indicadores		Unidades de Contexto
		4.º B	**Vírus** (Al 44) **Privacidade Online (**Al 33) **Perigos Online** (Al 33) **Comportamento Seguro Online** (Al 20)	Al 44: Os vírus podem destruir arquivos importantes e deixar o computador muito lento, por isso é crucial usar antivírus. Al 33: Privacidade *online* significa proteger as nossas informações pessoais e manter a segurança nas redes sociais. Al 33: Devemos estar sempre atentos aos perigos *online*, como fraudes e *phishing*, para evitar cair em armadilhas. Al 20: Comportamento seguro *online* inclui usar senhas fortes, verificar a segurança dos sites e não partilhar informações pessoais.
		4.º C	**Privacidade** (Al 47) **Precauções** (Al 48) **Vírus e Ataques** (Al 49)	Al 47: É importante configurar as definições de privacidade nas redes sociais para que as nossas informações não sejam expostas a estranhos. Al 48: Devemos sempre tomar precauções como usar senhas fortes e evitar clicar em *links* suspeitos para proteger as nossas contas online. Al 49: Os vírus podem infetar o computador e roubar informações pessoais, enquanto os ataques de *hackers* podem comprometer a segurança dos nossos dados.
		4.º D	- Navegação Segura (Al 70) - Proteção de Dados (Al 70) - Riscos e Comportamento *Online* (Al 72)	Al 70: Navegação segura significa estar sempre atento aos sites que visitamos e não fornecer informações pessoais sem verificar a segurança do site. Al 71: Devemos proteger os nossos dados utilizando senhas seguras e mantendo os nossos dispositivos atualizados. Al 72: Devemos ter cuidado com os riscos online, como o phishing e o *cyberbullying*, e adotar comportamentos que nos mantenham seguros.
	Importância de Conhecer os Perigos	Privacidade de dados é importante para proteger a nossa informação pessoal (Al 40) *Hacking* pode invadir os nossos computadores (Al 52)		Professora: Como proteger a privacidade *online*? Al 20: Eu nunca compartilho as minhas senhas. Al 33: Eu não posto fotos dos meus amigos sem permissão. Al 44: Eu não falo com quem não conheço *online*. Al 55: Eu verifico sempre os sites antes de clicar em algo. Professora: Como nos protegemos contra *hacking*? Al 6: Eu nunca clico em links suspeitos. Al 52: Eu mantenho o

Categoria	Subcategorias	Indicadores	Unidades de Contexto
		Malware e vírus podem estragar os nossos computadores (Al 6)	antivírus atualizado. Al 60: Eu verifico a segurança dos sites antes de aceder. Professora: Como evitar *malware* e vírus? Al 12: Eu uso um antivírus e evito baixar arquivos desconhecidos. Al 6: Eu desconfio de *links* em *e-mails*. Al 33: Eu faço *backup* dos meus arquivos regularmente para me proteger contra *ransomware*.
Privacidade Online	**Cuidados ao Compartilhar Informações**	Não Partilhar Informação Pessoal (Al 20) Não Publicar Fotos sem Autorização (Al 33) Não Falar com Estranhos (Al 44) Ter Cuidado com *Sites* Desconhecidos (Al 55)	Professora: Falem sobre o que fazem para proteger a privacidade online. Aluno 20: Eu nunca compartilho as minhas senhas. Aluno 33: Eu não posto fotos dos meus amigos sem permissão. Aluno 44: Eu não falo com quem não conheço *online*. Aluno 55: Eu verifico sempre os *sites* antes de clicar em algo.
	Publicações Online	Publicar Fotos com Cuidado (Al 5) Não Partilhar Fotos Pessoais (Al 12) Não Compartilhar Detalhes de Férias (Al 60)	Professora: Vamos discutir as melhores práticas para postar nas redes sociais. Aluno 5: Eu só publico fotos se souber que não vão causar problemas. Aluno 12: Nunca compartilho fotos pessoais. Aluno 60: Eu não conto para onde vou nas minhas férias.
Riscos Online	**Identificação e Prevenção de Riscos**	Sites Desconhecidos Podem Causar Burlas (Al 33) Hackers Podem Invadir Contas (Al 44) Proteção Contra *Ciberbullying* (Al 70)	Professora: Quais riscos que conhecem na *internet*? Como podemos evitá-los? Aluno 33: *Sites* estranhos podem ser falsos e roubar o nosso dinheiro. Aluno 44: Os *hackers* podem invadir as nossas contas se não formos cuidadosos. Aluno 70: Precisamos denunciar o *ciberbullying* quando vemos.
Comportamento Seguro Online	**Adoção de Boas Práticas**	Verificação de *Sites* (Al 5) Utilização de Senhas Fortes (Al 12) Não Aceitar Mensagens de Desconhecidos (Al 20) Usar Antivírus (Al 60)	Professora: Como se podem proteger enquanto navegam na *internet*? Aluno 5: Eu verifico sempre os *sites* que visito. Aluno 12: As minhas senhas são sempre muito fortes. Aluno 20: Nunca respondo mensagens de pessoas que não conheço. Aluno 60: Eu uso um antivírus para me proteger.

ANEXO D - PLANIFICAÇÃO DA AULA – TEMA: PESQUISA – PERIGOS NA INTERNET

IDENTIFICAÇÃO E PLANIFICAÇÃO					
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação			
DESCRIÇÃO					
1.ª aula	**DURAÇÃO:** 50 minutos			**DATA:**	
Domínios	**Áreas de Competência**	**Ações/Estratégias/Atividades**	**Duração**	**Recursos**	**Avaliação**
Cidadania Digital	Desenvolvimento Pessoal e Autonomia, Informação e Comunicação	**Consciencialização Inicial**: A professora começa a aula com uma breve introdução à segurança digital, explicando os conceitos principais com o auxílio de exemplos de ameaças como phishing, cyberbullying e *malware*. Em seguida, promove uma discussão guiada onde os alunos são encorajados a partilhar experiências pessoais. Perguntas como alguém já teve uma experiência *online* insegura? ajudam a fomentar o diálogo. Os alunos que participam ativamente têm a oportunidade de expressar seus conhecimentos prévios e aprender com as experiências dos colegas.	10 minutos	Computador, projetor, *internet*	A professora observará a participação dos alunos, avaliando sua capacidade de identificar práticas seguras e a compreensão inicial dos conceitos apresentados.
Investigação e Pesquisa	Pensamento Crítico e Criativo, Linguagens e Textos	**Pesquisa Orientada**: Após a discussão inicial, os alunos são instruídos a realizar uma pesquisa individual sobre os principais perigos *online*. Eles devem usar fontes confiáveis para identificar e compreender ameaças como *phishing*, *malware* e *cyberbullying*. Cada aluno elabora uma lista de perigos e cria um documento no *Google Docs*, onde regista	20 minutos	Computador, *internet*	A avaliação será verificada pela capacidade dos alunos na realização de pesquisas, seleção critica de informações relevantes e colaborar na criação de documentos que

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
		as palavras-chave e resumos das informações encontradas. A professora circula pela sala, oferecendo suporte e orientações sobre a escolha de fontes e a validação das informações recolhidas.			sintetizem os perigos identificados.
Comunicação e Colaboração	Relacionamento Interpessoal, Linguagens e Textos	**Apresentação dos Resultados**: Os alunos compartilham as suas descobertas sobre os perigos *online* com a turma. Cada grupo deve apresentar sua lista de perigos, explicando a importância de cada item e as fontes utilizadas. A professora modera as apresentações, incentivando os alunos a fazer perguntas e contribuir com sugestões. Esta atividade visa consolidar o entendimento dos alunos e promover a troca de conhecimentos.	15 minutos	Computador, projetor	Serão avaliadas a clareza e relevância das apresentações, bem como o envolvimento dos alunos na atividade e sua capacidade de trabalhar em grupo.
Reflexão e Discussão	Pensamento Crítico e Criativo, Desenvolvimento Pessoal e Autonomia	**Debate e Reflexão Final**: A professora finaliza a aula com um debate sobre as estratégias de segurança *online* discutidas. Os alunos são incentivados a refletir criticamente sobre as práticas digitais seguras e a importância da responsabilidade individual e coletiva na *internet*. A professora propõe questões como como podemos aplicar o que aprendemos hoje em nosso dia a dia? para estimular a reflexão. Os alunos têm a oportunidade de discutir como as novas informações adquiridas podem impactar as ações *online* e compartilhar planos de como irão adotar práticas mais seguras.	20 minutos	Computador, projetor	A avaliação focar-se-á na capacidade dos alunos de articular ideias, refletir criticamente sobre práticas seguras e participar ativamente no debate, demonstrando uma compreensão profunda dos conceitos discutidos.

ANEXO D1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: PESQUISA NA INTERNET

Categoria	Subcategorias	Indicadores	Unidades de Contexto
Perigos na *Internet*	**Identificação de Perigos**	*Phishing* (Al 5), *Cyberbullying* (Al 12), *Malware* (Al 20), *Spyware* (Al 21), Vírus (Al 22), *Ransomware* (Al 36), *Sexting* (Al 63)	Professora: Apresentação sobre a importância da segurança digital, seguida de discussão sobre experiências pessoais de navegação segura na *internet*. Al 5: *Phishing*. Al 12: *Cyberbullying*. Al 20: *Malware*. Al 21: *Spyware*. Al 22: Vírus. Al 36: *Ransomware*. Al 63: *Sexting*.
	Pesquisas sobre Perigos	*Malware* (Al 20), *Phishing* (Al 21, Al 25), Golpes *Online* (Al 57), Cyberbullying (Al 32)	Al 20: Pesquisei sobre *malware* e vírus e descobri que eles podem danificar seriamente os nossos dispositivos. Al 21: *Phishing* está em todo lugar. Al 25: *Phishing* é um grande perigo. Al 57: Golpes *online* podem roubar dinheiro ou informações.
Privacidade *Online*	**Cuidados ao Compartilhar Informações**	Privacidade de dados (Al 25), Segurança dos Dispositivos (Al 36), Invasão de Privacidade (Al 25)	Professora: Por que acham que esses temas são importantes? Al 25: Privacidade de dados é importante para proteger nossa informação pessoal. Al 25: A invasão de privacidade é quando alguém acede às nossas informações pessoais sem permissão. Al 36: *Hacking* pode invadir nossos computadores.
Reflexão Crítica	**Comportamento Seguro *Online***	Desconfiar de *links* suspeitos (Al 10), Utilização de antivírus (Al 57), Evitar sites desconhecidos (Al 32, Al 10)	Professora: Por que vocês acham que a segurança na internet é importante para todos nós? Al 5: Porque podemos evitar problemas. Al 57: Porque antivírus ajudam a proteger nossos computadores contra ameaças. Al 10: Desconfiar de links suspeitos. Al 32: Evitar sites desconhecidos.
Pesquisa e Comunicação	**Pesquisa sobre Perigos Online**	*Phishing* (Al 25), *Cyberbullying* (Al 32), *Malware* (Al 33)	Professora: Vamos pesquisar sobre os principais perigos online. Usem fontes confiáveis e façam anotações. Al 25: Phishing é um grande perigo. Al 32: Cyberbullying é sério. Al 33: *Malware* pode infetar os nossos computadores.
	Apresentação dos Resultados	Explicação de Perigos e Soluções (Al 50, Al 79), *Catfishing* (Al 79), Pornografia Infantil (Al 79)	Professora: Apresentem as vossas descobertas sobre os perigos online e digam como podemos nos proteger. Al 50: Eu descobri que *phishing* é muito comum. Al 79: *Catfishing*

Categoria	Subcategorias	Indicadores	Unidades de Contexto
			é quando alguém finge ser outra pessoa para nos enganar. Al 79: Pornografia infantil é ilegal e prejudicial.
Responsabilidade Digital	**Aplicação Prática**	Comportamentos Seguros *Online* (Al 5, Al 25), Partilha de conhecimentos com a família (Al 79, Al 25)	Professora: Como podemos usar o que aprendemos hoje para nos manter seguros *online*? Al 5: Vou ser mais cuidadoso com links desconhecidos. Al 25: Vou conversar com minha família sobre o que aprendemos, especialmente sobre privacidade de dados. Al 79: Devemos ensinar nossos amigos e família sobre os perigos.
Colaboração e Comunicação	**Colaboração em Grupos**	Listagem de Perigos (Al 50), Trabalho colaborativo em *Google Docs* (Al 32, Al 57)	Professora: Criem uma lista dos principais perigos online e partilhem no Google Docs. Al 50: Eu encontrei várias ameaças, como phishing e *malpare*. Al 32, Al 57: Participaram na colaboração de listagem de perigos.
	Discussão em Grupo	Estratégias de Proteção (Al 57, Al 79), Discussão sobre práticas seguras (Al 25, Al 36)	Professora: Vamos discutir as melhores estratégias para manter a segurança online. Como podemos ajudar os outros a ficarem seguros também? Al 57: Podemos compartilhar dicas de segurança. Al 79: Devemos ensinar nossos amigos e família sobre os perigos, como pornografia infantil. Al 25, Al 36: Contribuíram com estratégias de proteção durante a discussão.

ANEXO E- PLANIFICAÇÃO DA AULA – TEMA: JOGO DE SEGURANÇA NA INTERNET

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação
DESCRIÇÃO		
1.ª aula	**DURAÇÃO:** 50 minutos	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	**Desenvolvimento pessoal e autonomia, Informação e comunicação**	Consciencialização Inicial: - A aula começa com uma breve apresentação feita pela professora, abordando a importância da segurança digital, destacando temas como privacidade, proteção de dados e comportamento seguro na internet. - Após a apresentação, a professora conduz uma discussão guiada, onde os alunos são incentivados a compartilhar suas próprias experiências relacionadas à segurança digital. Perguntas sugeridas para guiar a discussão: - Alguém já teve uma experiência em que se sentiu inseguro na internet? - Quais são algumas medidas que você toma para se manter seguro online? - Objetivo: Estabelecer uma base de conhecimento e envolver os alunos na importância da segurança digital.	10 min	Computador, projetor, internet	Participação: Avaliar o nível de envolvimento dos alunos na discussão, observando se conseguem identificar práticas seguras e demonstrar uma compreensão inicial sobre segurança digital.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Comunicação e Colaboração	**Relacionamento interpessoal, Linguagens e textos**	**Jogo de Segurança Online**: - Descrição: Os alunos participam dos jogos https://cctic.ese.ipsantarem.pt/jogos/blog-jogar-online/ da SeguraNet, que apresenta uma série de perguntas e desafios relacionados à segurança digital. - **Atividade**: Cada aluno joga o jogo, respondendo a perguntas que abordam diferentes aspetos da segurança online, como a criação de senhas fortes, reconhecimento de phishing e navegação segura. - **Orientação**: Durante o jogo, a professora circula pela sala, oferecendo suporte e esclarecendo dúvidas. - **Objetivo**: Estimular a aprendizagem de forma lúdica, incentivando a colaboração e a aplicação prática dos conceitos discutidos.	30 min	Computador, internet, Jogo da SeguraNet	Observar o nível de envolvimento e a precisão das respostas dos alunos durante o jogo. Avaliar também a capacidade de colaboração e comunicação eficaz entre os pares ou grupos.
Reflexão e Discussão	**Pensamento crítico e criativo, Desenvolvimento pessoal e autonomia**	**Debate e Reflexão Final**: - Descrição: Após o jogo, os alunos participam de um debate guiado pela professora. Durante o debate, os alunos discutem as estratégias de segurança online que aprenderam ou reforçaram	20 min	Computador, projetor	Avaliar a capacidade dos alunos de articular ideias e refletir criticamente sobre as práticas de

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
		durante o jogo. - Atividade: A professora faz perguntas abertas para promover uma reflexão crítica, como: - Quais estratégias de segurança você acha mais importantes para aplicar no dia a dia? - Como você pode ajudar sua família e amigos a se protegerem online? - Objetivo: Incentivar os alunos a refletirem criticamente sobre as práticas seguras na internet e a importância da responsabilidade individual e coletiva.			segurança digital. Observar a participação ativa e o comprometimento dos alunos durante o debate.

ANEXO E1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: JOGOS DE SEGURANÇA NA INTERNET

Categoria	Subcategoria	Indicadores	Exemplos de Unidades de Contexto
Cidadania Digital	Consciencialização sobre Segurança Digital	Participação ativa e envolvimento na discussão inicial sobre a importância da segurança digital (Al 5). **Identificação de medidas de segurança que os alunos já utilizam** (Al 33).	**Al 5:** É importante para proteger nossos dados pessoais. **Al 6**: É ficar seguro na internet, tipo, não falar com pessoas que não se conhece ou contar as coisas pessoais. **Al 23:** Para evitar problemas de insegurança. **Al 13:** Porque manter a privacidade nos protege de hackers. **Al 33:** Para evitar problemas de segurança. **Al 35**: Para evitar que estranhos tenham acesso às nossas contas. **Al 6**: É ficar seguro na internet, tipo, não falar com pessoas que não se conhece ou contar as coisas pessoais.
	Discussão sobre Experiências Pessoais	Compartilhamento de experiências pessoais relacionadas à navegação segura na internet. (Al 20) **Relato de situações em que os alunos se sentiram inseguros online** (Al 33).	**Al 20:** Uma vez recebi um e-mail estranho e quase cliquei no link. **Al 33:** Eu sempre tento usar senhas diferentes para cada conta. **Al 44:** Eu clico em links suspeitos e depois me arrependo.
Participação no Jogo	Envolvimento no Jogo de Segurança Online	Nível de envolvimento e precisão nas respostas durante o Jogo de Segurança na Internet da SeguraNet. (Al 12)	**Al 12:** Não compartilhar senhas é a resposta correta. **Al 20:** Devemos sempre verificar a fonte antes de clicar em links. **Al 33:** É importante usar antivírus atualizado. **Al 44:** Devemos configurar as definições de privacidade nas redes sociais para proteção.
	Colaboração durante o Jogo	Capacidade de colaborar e trabalhar em equipa para responder aos desafios do jogo. (Al 20) **Discussão entre pares para acertar as respostas** (Al 55).	**Al 5:** Tenho dúvidas numa pergunta, acho que a resposta certa é evitar abrir links desconhecidos, mas não tenho certeza. **Al 55:** Concordo, é importante verificar a fonte. **Al 60:** Também devemos evitar baixar arquivos de fontes desconhecidas. **Al 70:** Devemos sempre sair das contas, fechar os e-mails, quando usamos computadores públicos…

Categoria	Subcategoria	Indicadores	Exemplos de Unidades de Contexto
Reflexão e Debate	Reflexão Crítica sobre Práticas Seguras	Reflexão sobre a importância da segurança online e estratégias de prevenção. (Al 12)	**Al 12:** Sim, eu vou ser mais cuidadoso com links desconhecidos. **Al 33:** Vou conversar mais com meus pais sobre o que aprendemos. **Al 44:** Vou usar senhas mais seguras. **Al 60:** Vou verificar as configurações de privacidade nas minhas redes sociais, acho que não muito seguras...
	Discussão sobre Estratégias de Segurança	Participação e argumentação durante o debate sobre estratégias de segurança (Al 20).	**Al 5:** Podemos compartilhar dicas de segurança. **Al 20:** Devemos ensinar os nossos amigos e família sobre os perigos. **Al 33:** Podemos criar cartazes sobre segurança online para a escola. **Al 44:** Devemos fazer atividades sobre segurança digital para os pais.

ANEXO F - PLANIFICAÇÃO DA AULA – TEMA: VISUALIZAÇÃO DE VÍDEOS

IDENTIFICAÇÃO E PLANIFICAÇÃO					
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação			
DESCRIÇÃO					
1.ª aula	**DURAÇÃO:** 50 minutos			**DATA:**	
Domínios	**Áreas de Competência**	**Ações/Estratégias/Atividades**	**Duração**	**Recursos**	**Avaliação**
Cidadania Digital	**Desenvolvimento pessoal e autonomia, Informação e comunicação**	Consciencialização Inicial: Apresentação interativa sobre a importância da segurança digital. Iniciar com um questionário para avaliar o conhecimento prévio. A professora conduz uma discussão inicial, explorando experiências pessoais sobre navegação segura, com ênfase em *cyberbullying*, sexting e proteção de dados.	15 min	Computador, projetor, internet	Participação ativa dos alunos e análise das respostas ao questionário para identificar lacunas de conhecimento e ajustar a discussão.
Comunicação e Colaboração	**Relacionamento interpessoal, Linguagens e textos**	Visualização e Discussão de Vídeos: Exibição dos vídeos da SeguraNet em: [https://www.seguranet.pt/] e [https://www.seguranet.pt/animacoes-seguranet]. Cada vídeo é seguido de atividades práticas e discussões específicas: ***Cyberbullying***: Vídeo que explora as consequências emocionais e legais do *cyberbullying*, seguido de análise de um caso fictício e debate sobre a importância de denunciar esses comportamentos. ***Sexting***: Vídeo sobre os riscos e a importância da privacidade ao compartilhar imagens íntimas, seguido de uma discussão sobre as implicações pessoais e legais e um exercício de tomada de decisão em situações hipotéticas. **Privacidade e Proteção de Dados**: Vídeo que ensina como proteger dados pessoais	40 min	Computador, projetor, vídeos da SeguraNet	Avaliação contínua durante as atividades práticas, observando a aplicação dos conceitos a situações reais e hipotéticas.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
		online, seguido de uma atividade prática onde os alunos identificam dados pessoais em perfis de redes sociais e discutem estratégias para protegê-los. ***Fake News***: Vídeo que aborda a identificação de notícias falsas, seguido de uma atividade de verificação de notícias, comparando fontes verdadeiras e falsas, e uma discussão sobre o efeito das *fake news* na sociedade. **Jogos *Online***: Vídeo que discute comportamentos seguros em jogos online, seguido de uma discussão sobre segurança e análise de cenários de risco em jogos *online*.			
Reflexão e Discussão	**Pensamento crítico e criativo, Desenvolvimento pessoal e autonomia**	**Debate e Reflexão Final**: Debate em grande grupo para discutir os temas abordados nos vídeos, focando em práticas digitais seguras e responsabilidade individual e coletiva. Cada aluno apresentará suas conclusões à turma, seguida por uma sessão de perguntas e respostas.	20 min	Computador, projetor, estudos de caso	Avaliação da clareza e profundidade das discussões em grupo, a articulação crítica dos conceitos e a capacidade de responder a perguntas com fundamentação

ANEXO F1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: VISUALIZAÇÃO DE VÍDEOS

Categorias	Subcategorias	Indicadores	Exemplos de Unidades de Contexto	Vídeo Relacionado
Consciencialização	Importância da Segurança Digital	Participação ativa e envolvimento na discussão (Al 20)	Professora: Por que é importante manter a privacidade online? Al 12: Para proteger os nossos dados pessoais. Professora: Como podemos evitar que estranhos acedem às nossas informações? Al 5: Usando senhas fortes e não compartilhando. Professora: O que acontece se não mantivermos nossas contas seguras? Al 20: Podemos ser *hackeados* e perder dados importantes.	**Como Proteger os teus Dados? (*SeguraNe*t Animações)**
Atenção	Foco durante a Visualização	Nível de atenção e interesse durante os vídeos (Al 44)	Professora: Vamos assistir aos vídeos da *SeguraNet* sobre segurança na internet. Prestem atenção nas dicas importantes. Al 55: Eu achei interessante a parte sobre não compartilhar senhas. Professora: Qual foi a dica mais importante do vídeo? Al 44: Gostei da dica sobre verificar links antes de clicar. Al 60: Devemos sempre verificar se o site é seguro antes de comprar algo.	**Reconhecer e Evitar Fraudes *Online* (*SeguraNet* Animações)**
Compreensão	Entendimento dos Conteúdos	Capacidade de identificar e compreender os conteúdos (Al 33)	Professora: O que aprenderam com os vídeos que podem usar para se manterem seguros *online*? Al 33: Ser mais cuidadoso com *links* desconhecidos.	***Fake News* (*SeguraNet* Animações)**

Categorias	Subcategorias	Indicadores	Exemplos de Unidades de Contexto	Vídeo Relacionado
			Professora: Como podemos melhorar nossa segurança nas redes sociais? Al 20: Verificando as configurações de privacidade. Professora: Por que é importante manter um antivírus atualizado? Al 12: Para proteger nossos dispositivos de vírus e *malwares*.	
Participação	Envolvimento na Discussão	Nível de participação e contribuição durante o debate (Al 5)	Professora: Quais são as melhores estratégias para manter a segurança online? Al 20: Podemos compartilhar dicas de segurança. Professora: O que podemos fazer para ajudar outros a se manterem seguros? Al 33: Criar cartazes sobre segurança online. Professora: Como podemos promover a segurança digital entre nossos amigos? Al 5: Podemos fazer apresentações na escola para conscienciализar todos.	**Desinformação em Contexto de Guerra (SeguraNet Animações)**
Avaliação Crítica	Análise de Informações	Análise da precisão e compreensão das informações (Al 44)	Professora: Quais das informações dos vídeos acharam mais importantes e porquê? Al 60: A parte sobre sexting foi muito esclarecedora. Professora: O que acham que poderiam aplicar nas suas vidas diárias? Al 55: As dicas sobre como proteger nossas contas. Professora: Como as *fake news* podem	**Sexting: O que Fazer? (SeguraNet Animações)**

Categorias	Subcategorias	Indicadores	Exemplos de Unidades de Contexto	Vídeo Relacionado
			nos prejudicar? Al 44: Podemos acabar acreditando em informações falsas e tomar decisões erradas.	
Aplicação	Uso Prático do Conhecimento	Aplicação prática dos conhecimentos adquiridos (Al 12)	Professora: Como podem aplicar o que aprenderam hoje nas atividades diárias na internet? Al 44: Verificando a fonte antes de clicar. Professora: Que outras práticas seguras vocês podem adotar? Al 60: Instalar um antivírus e mantê-lo atualizado. Professora: Como podemos garantir que nossas senhas sejam seguras? Al 12: Usando combinações de letras, números e símbolos e não reutilizando senhas.	**Jogos *Online* (*SeguraNet* Animação**

ANEXO K - PLANIFICAÇÃO DA AULA – TEMA: MENTIMETER

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ano de Escolaridade 4.º Ano	Tecnologia da Informação e Comunicação	**Tema**: Mentimeter em Açã

DESCRIÇÃO		
2.ª/ 3.ª aula	**DURAÇÃO:** 30 min + 90 min (TIC)	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	Desenvolvimento pessoal e autonomia, Informação e comunicação	**Consciencialização Inicial**: Breve apresentação sobre a importância da segurança digital. Discussão guiada pela professora sobre experiências pessoais dos alunos relacionadas a navegação segura na internet, introduzindo a pergunta principal do *Mentimeter*.	10 min	Computador, projetor, internet	Participação dos alunos na discussão, demonstrando compreensão inicial sobre segurança digital.
Investigar e Pesquisar	Pensamento crítico e pensamento criativo, Linguagens e textos	**Pesquisa Guiada**: Em pequenos grupos, os alunos pesquisam sobre os principais perigos *online*, incentivando a usar fontes confiáveis e a identificar informações verídicas. Cada grupo elabora uma lista de perigos, preparando-se para condensar suas descobertas em três palavras-chave para o *Mentimeter*.	20 min	Tablets ou computadores, acesso à internet	Capacidade de pesquisa, seleção crítica de informações relevantes e colaboração em grupo.
Comunicar e Colaborar	Relacionamento interpessoal, Linguagens e textos	**Atividade no *Mentimeter***: Utilizando o *Mentimeter*, cada grupo submete as três palavras-chave escolhidas que representam os perigos da internet identificados na pesquisa. A turma observa as respostas agregadas, facilitando a visualização das preocupações comuns entre os alunos.	15 min	Computador, projetor, *Mentimeter*	Clareza e relevância das palavras-chave escolhidas, Envolvimento na atividade do *Mentimeter*.
Criar e Inovar	Saber científico técnico e tecnológico, Sensibilidade estética e artística	**Criação de Conteúdo Digital**: Inspirados pela atividade no *Mentimeter* e pela discussão subsequente, cada grupo cria uma nuvem de palavras sobre os perigos que mais receiam o *online*, incorporando as palavras-chave e soluções para os perigos identificados.	30 min	Ferramentas de criação digital, *internet*	Criatividade na apresentação das soluções, compreensão aplicada dos conceitos de segurança digital.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Reflexão e Discussão	Pensamento crítico e pensamento criativo, Desenvolvimento pessoal e autonomia	**Debate e Reflexão Final:** Com base nas criações digitais dos grupos, organiza-se um debate sobre as estratégias de segurança *online*, promovendo uma reflexão crítica sobre as práticas digitais seguras e a importância da responsabilidade individual e coletiva na internet.	20 min	Criações digitais dos alunos, projetor	Capacidade de articulação de ideias, reflexão crítica sobre práticas seguras e participação ativa no debate.

ANEXO K1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: MENTIMETER

Categoria	Subcategorias	Indicadores	Exemplos de Unidades de Contexto
Consciencialização	Identificação de Perigos	**Palavras-chave sobre perigos *na* internet (Al 33)**	Professora: Escrevam palavras-chave sobre os principais perigos na internet que vocês conhecem. **Al: 33**: *Phishing*. **Al: 12**: *Cyberbullying*. **Al: 20**: *Malware*. Professora: Por que acham que esses perigos são importantes? **Al: 5**: Privacidade de dados é importante para proteger nossa informação pessoal. **Al: 60**: *Hacking* pode invadir nossos computadores. **Al: 44**: *Malware* e vírus podem estragar nossos computadores.
Pesquisa e Reflexão	Importância dos Perigos	**Justificação da importância dos perigos *online* (Al 60)**	Professora: Por que esses perigos são importantes? **Al: 60**: *Hacking* pode invadir nossos computadores. **Al: 5**: Privacidade de dados é importante para proteger nossa informação pessoal. **Al: 55**: *Malware* e vírus podem estragar nossos computadores. Professora: Como esses perigos afetam nossa segurança *online*? **Al: 44**: Podem roubar nossas informações pessoais.
Comunicação	Resumo de Pesquisa	**Uso do *Mentimeter* para condensar pesquisas (Al 20)**	Professora: Utilizem o *Mentimeter* para condensar as pesquisas em três palavras-chave que representem os principais perigos *online* que encontraram. **Al: 20**: *Phishing*, *malware*, privacidade. **Al: 33**: *Cyberbullying*, *hacking*, vírus. **Al: 44**: Fraudes, roubo de identidade, *spyware*.
Criação	Criação de Conteúdo	**Criação de nuvens de palavras (Al 12)**	Professora: Com base nas palavras-chave e discussões, escrevam três palavras sobre os perigos que podem encontrar na *internet*. **Al: 12**: Nuvens de palavras focado em como evitar fraudes. **Al: 60**: Apresentação sobre proteção de dados e senhas seguras. **Al: 20**: Mapa sobre os perigos do *ciberbullying* e como evitá-los.
Reflexão	Debate sobre Segurança Online	**Discussão sobre estratégias de segurança *online* (Al 5)**	Professora: Vamos debater as melhores estratégias para manter a segurança *online*. **Al: 5**: Devemos ser cuidadosos com nossas informações pessoais. **Al: 33**: Precisamos ajudar os outros a ficarem seguros *online*. **Al: 12**: Sempre verificar *links* antes de clicar.

ANEXO L - PLANIFICAÇÃO DA AULA – TEMA: CRIAÇÃO VISUAL NO CANVA

IDENTIFICAÇÃO E PLANIFICAÇÃO					
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação			
DESCRIÇÃO					
1.ª aula	**DURAÇÃO:** 50 minutos			**DATA:**	
Domínios	**Áreas de Competência**	**Ações/Estratégias/Atividades**	**Duração**	**Recursos**	**Avaliação**
Cidadania Digital	Desenvolvimento pessoal e autonomia Informação e comunicação Saber científico, técnico e tecnológico	**Consciencialização Inicial:** - Apresentação sobre a importância da segurança digital, abordando tópicos como proteção de dados pessoais e privacidade *online*. - Discussão guiada onde os alunos compartilham experiências pessoais relacionadas à navegação segura na *internet*, com foco em identificar riscos e boas práticas.	10 min	Computador, projetor, *internet*	Participação dos alunos na discussão, demonstrando compreensão inicial sobre segurança digital.
Investigação e Criação	Pensamento crítico e criativo Linguagens e textos Saber científico, técnico e tecnológico	**Pesquisa Orientada:** - Os alunos pesquisam individualmente sobre os principais perigos online, utilizando fontes confiáveis. - Elaboração de uma lista de palavras-chave relacionadas à segurança na *internet*, promovendo a habilidade de pesquisa crítica e organização das informações.	20 min	Computador, *internet*	Avaliação da capacidade de pesquisa, seleção crítica de informações relevantes e organização das ideias.
Comunicação e Colaboração	Relacionamento interpessoal Linguagens e textos Sensibilidade estética e artística	**Criação Visual no *Cana*:** - Cada aluno cria um poster digital no Canva com base nas palavras-chave e informações recolhidas. - O foco é destacar dicas e boas práticas de	30 min	Computador, projetor, *internet*, *Canva*	Criatividade e clareza na apresentação visual das informações.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
		segurança na *internet*, com uma apresentação visual clara e criativa que reflita a compreensão dos conceitos abordados.			
Reflexão e Discussão	Pensamento crítico e criativo Desenvolvimento pessoal e autonomia Saber científico, técnico e tecnológico	**Debate e Reflexão Final:** - Apresentação dos *posters* digitais criados no *Canva*, seguida de uma discussão sobre as estratégias de segurança online abordadas. - Reflexão crítica sobre as práticas digitais seguras e a importância da responsabilidade individual e coletiva na *internet*. - Encerramento com uma síntese das melhores práticas discutidas.	20 min	Computador, projetor	Capacidade de articulação de ideias e reflexão crítica sobre práticas seguras.

ANEXO L1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: CRIAÇÃO VISUAL NO CANVA

Categoria	Subcategorias	Indicadores	Exemplos de Unidades de Contexto
Perigos na Internet	Identificação de Perigos	*Phishing, Cyberbullying, Malware, Spyware,* Vírus, *Ransomware, Hacking*	Professora: Pesquisem sobre os principais perigos *online* e anotem as palavras-chave. Al 5: *Phishing*. Al 12: *Cyberbullying*. Al 20: *Malware*. Al 33: *Spyware*. Al 44: Vírus…
	Argumentos sobre a Importância de Conhecer os Perigos	*Privacidade de dados, Hacking, Malware e* Vírus	Professora: Vamos discutir por que esses perigos são importantes. Al5: Privacidade de dados é importante para proteger a nossa informação pessoal. Al 12: *Hacking* pode invadir os nossos computadores. Al 20: *Malware* e vírus podem estragar os nossos computadores…
Criação Visual	Produção de Conteúdo Digital	Posters digitais sobre boas práticas de segurança na *internet*	Professora: Criem um poster digital no *Canva* sobre segurança na *internet*. Al 5: Vou criar um *poster* sobre a importância de não compartilhar senhas. Al 12: Vou fazer sobre como evitar *ransomware*. Al 20: O meu vai mostrar como proteger a privacidade nas redes sociais. Al 33: Vou fazer um poster sobre a importância de usar antivírus atualizado…
Reflexão e Discussão	Discussão e Justificação de Estratégias	Estratégias de segurança digital, responsabilidade *online*	Professora: Vamos discutir as estratégias apresentadas nos *posters*. Al 5: Precisamos ser cuidadosos com nossas senhas. Al 12: Devemos usar diferentes senhas para diferentes contas. Al 20: Fazer *backup* regularmente é importante. Al 33: É fundamental discutir práticas seguras com a família…

ANEXO M - PLANIFICAÇÃO DA AULA – TEMA: QUIS NO NEARPOD: APLICAÇÃO DE UM QUIZ PARA CONSOLIDAR E AVALIAR A APRENDIZAGEM , COM FEEDBACK INSTANTÂNEO

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação
DESCRIÇÃO		
1.ª aula	**DURAÇÃO:** 50 minutos	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	**Desenvolvimento pessoal e autonomia, Informação e comunicação**	**Consciencialização Inicial:** - Início da aula com uma breve apresentação sobre a importância da segurança digital. A professora explica conceitos chave, como privacidade, proteção de dados, e boas práticas de navegação *online*. - Discussão guiada pela professora onde os alunos compartilham experiências pessoais. - Perguntas de apoio para a discussão: - Alguém já se sentiu inseguro na *internet*? Como lidou com isso? - Quais práticas vocês consideram seguras ao usar a *internet*? - **Objetivo:** Estimular a consciência crítica sobre a segurança digital e incentivar a partilha de boas práticas entre os alunos.	10 min	Computador, projetor, *internet*	**Avaliação Formativa:** Avaliar a participação dos alunos na discussão, observando se demonstram compreensão inicial sobre segurança digital e se conseguem identificar práticas seguras.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Tecnologias de Informação e Comunicação	**Saber científico, técnico e tecnológico; Pensamento crítico e criativo**	**Atividade Interativa:** - **Descrição:** Os alunos respondem a um questionário interativo no *Quiz* no *Nearpod* que aborda diversos cenários de segurança *online*. - **Atividade:** A professora orienta os alunos durante a atividade, incentivando-os a refletirem sobre as suas respostas e a justificarem suas escolhas. - **Objetivo:** Desenvolver a capacidade dos alunos de analisar situações de risco na internet e aplicar o pensamento crítico na tomada de decisões seguras.	15 min	Computador, internet, Quiz no ***Nearpod***	**Avaliação:** Monitorizar as respostas dos alunos, avaliando a compreensão dos conceitos abordados e a capacidade de aplicar o pensamento crítico para resolver problemas.
Comunicação e Colaboração	**Relacionamento interpessoal, Linguagens e textos**	**Discussão em Grupo:** - **Descrição:** Os alunos são divididos em grupos pequenos para discutirem as respostas ao questionário do *Quiz* no ***Nearpod***. Cada grupo é incentivado a compartilhar suas conclusões e a discutir estratégias para melhorar a segurança *online*. - **Atividade:** A professora facilita a discussão, garantindo que todos os alunos tenham a oportunidade de contribuir. - **Objetivo:** Promover a colaboração, a comunicação eficaz e o respeito pelas opiniões dos colegas.	15 min	Computador, projetor	**Avaliação:** Avaliar a clareza e a relevância das discussões em grupo, observando a capacidade dos alunos de colaborar, comunicar suas ideias e respeitar as contribuições dos outros.
Reflexão e Discussão	**Pensamento crítico e criativo, Desenvolvimento**	**Debate e Reflexão Final:** - **Descrição:** A aula termina com um debate guiado pela professora, onde os	20 min	Computador, projetor	**Avaliação Formativa:** Avaliar a capacidade dos alunos de articular ideias e

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
	pessoal e autonomia	alunos discutem as estratégias de segurança *online* que consideram mais importantes. - **Atividade:** A professora propõe perguntas abertas para promover uma reflexão crítica, como: - Como podemos aplicar as estratégias de segurança digital aprendidas na nossa vida diária? - O que podemos fazer para ajudar nossos amigos e familiares a se protegerem online? - **Objetivo:** Incentivar os alunos a refletirem criticamente sobre a segurança digital e a importância da responsabilidade individual e coletiva.			refletir criticamente sobre as práticas de segurança digital. Observar a participação ativa e o comprometimento dos alunos durante o debate

ANEXO M1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: QUIZ NO NEARPOD: APLICAÇÃO DE UM QUIZ PARA CONSOLIDAR E AVALIAR A APRENDIZAGEM , COM FEEDBACK INSTANTÂNEO

Categoria	Subcategorias	Indicadores	Exemplos de Unidades de Contexto
Consciencialização	Identificação de Perigos	**Participação na discussão inicial sobre segurança digital (Al 5)**	Professora: Alguém já se sentiu inseguro na *internet*? Como lidou com isso? **Al 12**: Uma vez recebi um e-mail suspeito e não cliquei no link. **Al 5**: Eu sempre verifico se o site é seguro antes de colocar minhas informações. **Al 33**: Nunca compartilho minhas senhas, nem com amigos. **Al 44**: Uso autenticação de dois fatores em todas as contas.
Tecnologias de Informação e Comunicação	Pensamento crítico e criativo	**Respostas no *Quiz*** no ***Nearpod*** **sobre cenários de segurança *online* (Al 20)**	Professora: Responda ao questionário no *Quiz* no ***Nearpod*** sobre como agir em diferentes cenários *online*. **Al 44**: Optei por não abrir *links* enviados por desconhecidos. **Al 55**: Escolhi não compartilhar informações pessoais em redes abertas. **Al 20**: Verifiquei as configurações de privacidade antes de postar.
Comunicação e Colaboração	Discussão em grupo	**Contribuição para a discussão em grupo sobre as respostas do** Quiz no ***Nearpod*** **(Al 33)**	Professora: Discutam suas respostas ao questionário do *Quiz* no ***Nearpod*** em grupo. Qual foi a decisão mais difícil de tomar? **Al 20**: Discutimos sobre compartilhar senhas, e concordamos que é melhor não fazer isso. **Al 33**: Falamos sobre a importância de usar um antivírus atualizado. **Al 60**: Comentamos sobre verificar *links* antes de clicar.
Reflexão e Discussão	Pensamento crítico e criativo	**Participação no debate final sobre estratégias de segurança *online* (Al 12)**	Professora: Como podemos aplicar as estratégias de segurança digital aprendidas na nossa vida diária? **Al 12**: Vou começar a usar senhas mais fortes e verificar as configurações de privacidade. **Al 5**: Vou falar com meus pais sobre instalar um antivírus no computador. **Al 33**: Vou ajudar meus amigos a entenderem melhor a importância da segurança *online*.

ANEXO M2 - PERGUNTAS FREQUENTEMENTE RESPONDIDAS INCORRETAMENTE NO *QUIZ NEARPOD*

A análise das perguntas frequentemente incorretas nos ***Quiz Nearpod***, aplicados às turmas do 4.º ano, revela alguns padrões de compreensão e lacunas no entendimento dos riscos *online*. A seguir vamos analisar as perguntas mais frequentemente erradas pelas diferentes turmas:

1. Pergunta 1 - Que tipo de atividades são realizadas na *internet*?

⇢ **4.º A**, **4.º B**, **4.º C**, **4.º D**: todas as turmas revelaram dificuldades em responder a esta pergunta, indicando que a maioria dos alunos revelou dificuldade em identificar adequadamente as atividades que realizam na *internet*. Isso pode refletir uma falha na reflexão ou na compreensão sobre a diversidade de atividades disponíveis e realizadas no ambiente *online*. O desconhecimento ou a subestimação das possibilidades da *internet* foi um ponto comum entre os alunos.

Gráfico 1 - 4.º A

Gráfico 2 - 4.º B

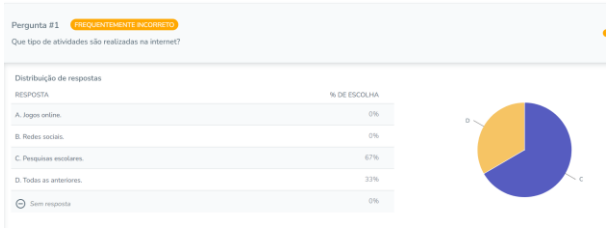
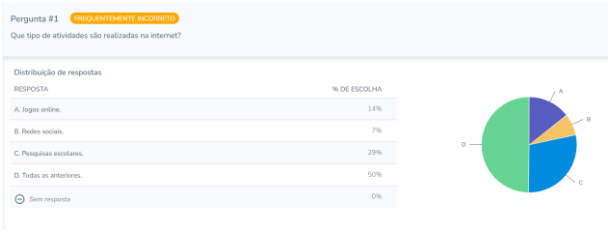


Gráfico 3 - 4.º C

Gráfico 4 - 4.º D

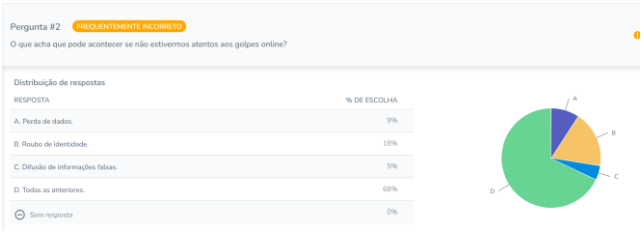


2. Pergunta 2 - O que acha que pode acontecer se não estivermos atentos aos golpes *online*?

⇢ **4.º B** e **4.º C**: a problemática desta questão também foi bastante desafiadora. Os alunos tiveram dificuldades na antecipação de potenciais riscos e consequências de não estarem atentos às fraudes virtuais, minimizando os perigos envolvidos, tais como a violação de identidade e o acesso não autorizado a dados pessoais.

Gráfico 5 - 4.º B

Gráfico 6 - 4.º C



3. Pergunta 3 - Quais são as possíveis consequências de cair num golpe na *internet*?

⇢ **4.º B**, **4.º C**, e **4.º D**: As respostas a esta pergunta indicaram que os alunos têm dificuldade em identificar as consequências mais graves de cair num golpe *online*. Houve uma tendência a minimizar os perigos ou a não reconhecer o efeito, como a perda de dinheiro, a exposição de dados sensíveis, ou o risco de danos psicológicos.

Gráfico 7 - 4.º B

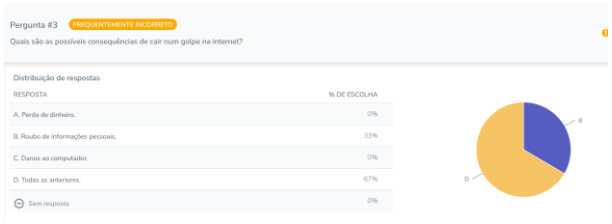
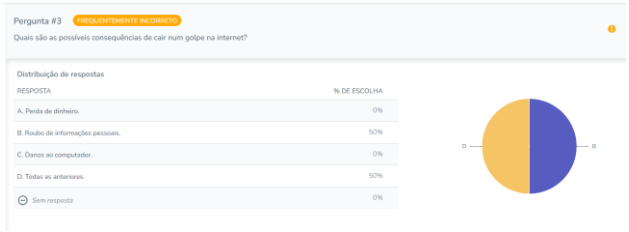


Gráfico 8 - 4.º C

Gráfico 9 - 4.º D



Análise Comparativa:

- 4.º A teve um desempenho ligeiramente melhor na compreensão das atividades realizadas na *internet*, mas ainda apresentou falhas significativas.

- 4.º B e 4.º C demonstraram dificuldades similares, especialmente em entender as consequências dos riscos *online*, sugerindo uma necessidade de reforçar a educação sobre segurança digital nestas turmas.

- 4.º D compartilhou dificuldades semelhantes com as outras turmas na compreensão das consequências dos golpes, o que sugere um padrão geral de subestimação dos riscos *online* entre os alunos.

Conclusão:

A análise aponta para a necessidade de intervenções educativas mais robustas, focadas na consciencialização dos riscos *online* e nas consequências de comportamentos inseguros na *internet*. A educação digital deve priorizar o reconhecimento dos perigos, mas também o entendimento profundo das possíveis consequências para melhorar a segurança dos alunos na *internet*.

ANEXO N - PLANIFICAÇÃO DA AULA – TEMA: DIA INTERNACIONAL DA INTERNET SEGURA (GNR)

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação
DESCRIÇÃO		
1.ª aula	**DURAÇÃO:** 50 minutos	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	**Informação e Comunicação**	**Consciencialização Inicial:** - Início da aula com uma apresentação feita por um elemento da Guarda Nacional Republicana (GNR) sobre a importância da segurança na internet. - Após a apresentação, a professora conduz uma discussão guiada, incentivando os alunos a compartilhar experiências pessoais relacionadas coma segurança digital. Exemplo de perguntas para guiar a discussão: - Alguém já teve uma experiência em que se sentiu inseguro na *internet*? - O que fazem para se proteger quando estão *online*?	15 min	Computador, projetor, internet	**Participação:** Avaliar a participação ativa dos alunos na discussão, verificando se conseguem identificar práticas seguras e demonstram compreensão inicial sobre a importância da segurança digital.
Pensamento Crítico	**Raciocínio e resolução de problemas, Pensamento crítico e criativo**	**Atividade Interativa: Simulação de Cenários de Risco Online** - **Descrição:** Os alunos trabalham em pares. Cada par recebe um cenário de risco *online* (previamente preparado pela professora). Os cenários podem incluir situações como: - Receber um e-mail suspeito pedindo	20 min	Material interativo (cenários impressos ou digitais), internet	**Envolvimento e Respostas:** Avaliar o nível de envolvimento dos alunos e a qualidade das soluções propostas para os cenários de risco. Observar a capacidade dos alunos de

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
		informações pessoais. - Encontrar um link suspeito em uma rede social. - Receber uma mensagem de um desconhecido. - **Objetivo:** Os alunos devem discutir o cenário, identificar os riscos e propor uma solução segura para a situação. Durante a atividade, a professora circula pela sala, ouvindo as discussões e oferecendo orientação quando necessário.			identificar riscos e aplicar o pensamento crítico para resolver problemas.
Colaboração e Comunicação	**Relacionamento interpessoal, Linguagens e textos**	**Debate em Pares, seguido de Discussão e Apresentação das Soluções em grande grupo:** - **Descrição:** Após a atividade interativa, cada par compartilha as suas conclusões com a turma. A professora organiza as apresentações, permitindo que todos expliquem o cenário que analisaram e a solução que propôs. - **Orientação:** A professora deve garantir que todos os alunos tenham a oportunidade de falar, incentivando uma comunicação clara e a partilha de conhecimentos. A turma pode fazer perguntas ou adicionar sugestões para enriquecer a discussão.	15 min	Computador, projetor	**Clareza e Relevância das Apresentações:** Avaliar a clareza das apresentações e a relevância das soluções propostas. Observar o nível de colaboração entre os pares e a capacidade de comunicação dos alunos.

ANEXO N1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: DIA INTERNACIONAL DA INTERNET SEGURA (GNR)

Categoria	Subcategorias	Indicadores	Unidades de Contexto
Consciencialização	Identificação de Comportamentos Seguros	**Identificação de práticas seguras online (Al 40)**	Professora: Após a apresentação dos elementos da GNR, a professora conduz uma discussão guiada sobre experiências pessoais de segurança digital. **Al 5**: Eu verifico sempre se o site é seguro antes de colocar as minhas informações. **Al 12**: Nunca compartilho as minhas senhas com ninguém. **Al 20**: Eu e minha família falamos sobre como usar a internet de forma segura. **Al 33**: Eu uso antivírus em todos os meus dispositivos. **Al 40**: Eu sempre escolho senhas que são difíceis de adivinhar. **Al 35:** que uma vez um estranho lhe mandou uma mensagem suspeita quando jogava. **Al 39:** Se algo me deixasse desconfortável, deveria contar aos meus pais ou professores.
Reflexão Crítica	Compreensão de Comportamentos Seguros	**Reconhecimento de comportamentos seguros e inseguros (Al 33)**	Professora: Quais os comportamentos seguros que vocês conhecem? **Al 33**: Nunca clico em links de e-mails suspeitos. **Al 44**: Eu às vezes esqueço de verificar a segurança dos sites. **Al 55**: Eu não sabia que atualizar o software era importante para segurança. **Aluno 60**: Eu não tinha certeza se o site era seguro. **Aluno 25**: Eu saio sempre das minhas contas quando termino de usar um computador. **Al 70**: Eu, é quando alguém tenta enganar-nos para conseguir informações nossas. **Al 41**: que ele nunca o daria e iria dizer imediatamente isso aos pais. **Al 61**: nunca enviaria fotos de si mesma online, especialmente para estranhos.
Pensamento Crítico	Resolução de Problemas	**Solução de cenários de risco online (Al 38)**	Professora: Cada par recebe um cenário de risco online para discutir e resolver. **Aluno 5**: Se receber um e-mail suspeito, vou ignorá-lo e avisar os meus pais. **Al 12**: Vou verificar o remetente antes de clicar em qualquer link. **Al 44**: Eu tive dificuldade em saber o que fazer quando recebi uma mensagem de um desconhecido. **Al 70**: Eu não

Categoria	Subcategorias	Indicadores	Unidades de Contexto
			sabia como reconhecer um link suspeito. **Al 38**: Eu acho que podemos pesquisar na internet sobre a confiabilidade de um site antes de aceder. **Al 44:** que nunca se deve responder e deve-se informar um adulto imediatamente. **Al 42:** Sempre deveríamos usar uma senha forte e nunca compartilhar as informações.
Colaboração e Comunicação	Discussão e Apresentação de Soluções	**Apresentação de soluções para os cenários de risco (Al 20)**	Professora: Cada par ou aluno compartilha as suas soluções para os cenários de risco online. **Al 20**: Podemos usar a autenticação para garantir mais segurança. **Al 33**: É importante ensinar os nossos amigos e familiares sobre os riscos online. **Al 60**: Eu percebi que preciso de ajuda para entender os riscos de instalar novos aplicativos. **Al 55**: Eu acho que posso melhorar em como identificar links seguros. **Al 47**: Eu sugiro que, antes de instalar alguma coisa, devemos sempre perguntar aos nossos pais. **Al 53**: que não se devem rir dos outros, salientando que 'devemos tratar toda a gente, como gostaríamos de ser tratados.

ANEXO O - PLANIFICAÇÃO DA AULA – TEMA: DIREITOS DIGITAIS: A VOZ DAS CRIANÇAS NA INTERNET

IDENTIFICAÇÃO E PLANIFICAÇÃO		
Ana de Escolaridade:	4.º Ano	Tecnologias de Informação e Comunicação
DESCRIÇÃO		
1.ª aula	**DURAÇÃO:** 50 minutos	**DATA:**

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	Desenvolvimento pessoal e autonomia, Informação e comunicação	**Consciencialização Inicial:** Breve apresentação sobre a importância dos direitos digitais. Discussão guiada pela professora sobre as experiências pessoais dos alunos relacionadas aos direitos digitais.	10 min	Computador, projetor, *internet*	Participação dos alunos na discussão, demonstrando compreensão inicial sobre direitos digitais.
Investigação e Pesquisa	Pensamento crítico e criativo, Linguagens e textos	**Pesquisa Orientada:** Individualmente, os alunos pesquisam sobre os principais direitos digitais das crianças, incentivando o uso de fontes confiáveis e identificação de informações verídicas. **Gravação dos direitos**: Cada aluno elabora uma lista de direitos e grava um direito com o software indicado *Voki* (https://www.voki.com/) ou Adobe Express em (**https://new.express.adobe.com/tools/animate-from-audio**), fornecido pela professora. Após a gravação coloca no *Google Classroom*.	20 min	Computador, *internet*	Capacidade de pesquisa, seleção crítica de informações relevantes e colaboração em grupo.
Comunicação e Colaboração	Relacionamento interpessoal, Linguagens e textos	**Apresentação dos Resultados:** Cada aluno apresenta as suas descobertas sobre os direitos digitais, explicando os seus direitos e as fontes utilizadas.	15 min	Computador, projetor	Clareza e relevância das apresentações, envolvimento na atividade.

Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Reflexão e Discussão	Pensamento crítico e criativo, Desenvolvimento pessoal e autonomia	**Debate e Reflexão Final:** Discussão sobre a importância dos direitos digitais, promovendo uma reflexão crítica sobre como garantir e respeitar esses direitos na *internet*.	20 min	Computador, projetor	Capacidade de articulação de ideias, reflexão crítica sobre práticas seguras e participação ativa no debate.

ANEXO O1 - GRELHA DE ANÁLISE DE CONTEÚDO – TEMA: DIREITOS DIGITAIS: A VOZ DAS CRIANÇAS NA INTERNET

Categoria	Subcategorias	Indicadores	Exemplos de Unidades de Contexto
Cidadania Digital	Identificação de Direitos Digitais	**Conhecimento dos direitos digitais (Al 20)**	Professora: Escrevam palavras-chave sobre os direitos digitais que vocês conhecem. Pensem em termos como privacidade online, segurança de dados, etc. **Al 5**: Privacidade online. **Al 12**: Segurança de dados. **Al 20**: Acesso à informação. **Al 33**: Proteção contra assédio online. **Al 44**: Direito à expressão digital. **Al 55**: Direito à segurança digital. **Al 60**: Direito à educação digital. **Al 70**: Acesso a recursos educativos.
Investigação e Pesquisa	Importância dos Direitos Digitais	**Justificação da importância dos direitos digitais (Al 33)**	Professora: Por que acham que esses direitos são importantes? **Al 12**: Privacidade de dados é essencial para proteger nossas informações pessoais. **Al 20**: A segurança de dados nos ajuda a manter as nossas contas seguras. **Al 33**: A proteção contra assédio online deve ser uma prioridade.
Criação e Expressão	Elaboração e Gravação dos Direitos Digitais	**Criação de conteúdos sobre direitos digitais (Al 12)**	Professora: Vamos criar e gravar conteúdos sobre os direitos digitais que vocês pesquisaram. **Al 5**: Eu vou gravar sobre o direito à privacidade online. **Al 12**: Eu vou gravar sobre o direito à segurança de dados. **Al 20**: Vou gravar sobre a importância da proteção contra assédio online. **Al 33**: Vou gravar sobre o direito à educação digital. **Al 55**: É importante proteger as pessoas contra assédio online, porque eu vi amigos passarem por isso.
Reflexão e Discussão	Discussão sobre a Implementação dos Direitos Digitais	**Reflexão sobre como aplicar os direitos digitais no dia a dia (Al 5)**	Professora: Como podemos aplicar o que aprendemos sobre direitos digitais no nosso uso diário da internet? **Al 5**: Vou verificar se os sites são seguros antes de usar. **Al 12**: Vou discutir com minha família sobre a importância da privacidade online. **Al 41**: Recebi uma mensagem suspeita enquanto jogava online e avisei meus pais. **Al 33**Eu não sabia que compartilhar minha localização poderia ser perigoso, agora vou verificar as configurações de privacidade.

ANEXO P - PLANIFICAÇÃO DA AULA – TEMA: FORMULÁRIO: AVALIAÇÃO DA EFICÁCIA DAS ATIVIDADES

IDENTIFICAÇÃO E PLANIFICAÇÃO					
Ana de Escolaridade:	4.º Ano		Tecnologias de Informação e Comunicação		
DESCRIÇÃO					
1.ª aula	**DURAÇÃO:** 50 minutos		**DATA:**		
Domínios	Áreas de Competência	Ações/Estratégias/Atividades	Duração	Recursos	Avaliação
Cidadania Digital	Desenvolvimento pessoal e autonomia, Informação e comunicação	**Consciencialização Inicial:** Breve apresentação sobre a importância da segurança na internet. Discussão guiada pela professora sobre as experiências pessoais dos alunos relacionadas à segurança na internet.	10 min	Computador, projetor, *internet*	Participação dos alunos na discussão, demonstrando compreensão inicial sobre segurança digital.
Investigação e Pesquisa	Pensamento crítico e criativo, Linguagens e textos	**Pesquisa Orientada:** Individualmente, os alunos respondem a um formulário *Google Forms* sobre segurança na *internet*, respondendo perguntas relacionadas com os conhecimentos obtidos sobre comportamentos seguros *online*.	20 min	Computador, *internet*	Capacidade de resposta às perguntas do formulário, compreensão dos conceitos de segurança digital.
Comunicação e Colaboração	Relacionamento interpessoal, Linguagens e textos	**Discussão dos Resultados:** Após responderem ao formulário, os alunos discutem em grupos as respostas obtidas, refletindo sobre os resultados e a importância de cada comportamento seguro mencionado.	15 min	Computador, projetor	Clareza e relevância das discussões, envolvimento na atividade.
Reflexão e Discussão	Pensamento crítico e criativo, Desenvolvimento pessoal e autonomia	**Debate e Reflexão Final:** Discussão sobre as estratégias de segurança *online*, promovendo uma reflexão crítica sobre como melhorar a segurança digital nas suas vidas diárias.	20 min	Computador, projetor	Capacidade de articulação de ideias, reflexão crítica sobre práticas seguras e participação ativa no debate.

ANEXO P1 – ANÁLISE DESCRITIVA – TEMA: FORMULÁRIO: AVALIAÇÃO DA EFICÁCIA DAS ATIVIDADES

Categoria	Subcategorias	Indicadores	Exemplos de Unidades de Contexto
Cidadania Digital	Importância da Segurança na Internet	**Avaliação da importância das atividades sobre segurança na internet (Al 5)**	Professora: Analisem como vocês avaliam a importância das atividades sobre segurança na internet. Análise com base nos gráficos do ANEXO P3 Gráfico 1: 65% dos alunos consideram a atividade. Muito importante. Gráfico 2 (4.º B): 73,7% dos alunos consideram a atividade. Extremamente importante. **Al 5**: Acho que aprender sobre segurança na internet é muito importante porque usamos a internet todos os dias. **Al 12**: Estas aulas são essenciais para nos protegermos online. **Al 33**: Precisamos saber como nos manter seguros na internet. **Al 70**: A segurança digital é importante para toda a família.
Investigação e Pesquisa	Comportamentos Seguros na Internet	**Identificação de comportamentos seguros online (Al 12)**	Professora: Escrevam comportamentos seguros que vocês acham importantes na internet. **Al 5**: Não compartilhar senhas. **Al 12**: Verificar a segurança de sites. **Al 20**: Não clicar em links suspeitos. **Al 33**: Manter o antivírus atualizado. **Al 44**: Teve dificuldade em identificar comportamentos seguros em redes sociais. **Al 55**: Demonstrou compreensão ao responder sobre a importância de atualizações de software.
Comunicação e Colaboração	Discussão dos Resultados	**Reflexão sobre os resultados do formulário (Al 60)**	Professora: Vamos discutir os resultados do formulário. **Al 5**: Percebi que muitos colegas ainda compartilham senhas. **Al 12**: Fiquei surpreso que poucos verificam a segurança dos sites antes de aceder. **Al 60**: Acho que precisamos melhorar nossa atenção ao clicar em links. **Al 70**: A segurança digital é importante e precisamos praticar mais.
Reflexão e Discussão	Melhoria da Segurança na Internet	**Sugestões para melhorar a segurança digital (Al 33)**	Professora: Como podemos melhorar nossa segurança na internet? **Al 33**: Podemos usar autenticação em dois fatores. **Al 44**: Devemos ter mais cuidado ao instalar aplicativos. **Al 55**: Precisamos educar nossos amigos e familiares sobre os riscos online. **Al 70**: Devemos manter sempre o antivírus atualizado.

ANEXO P2– FORMULÁRIO: AVALIAÇÃO DA EFICÁCIA DAS ATIVIDADES

1. **Como avalias a importância das atividades relacionadas à segurança na *internet* realizadas durante as aulas?**
    - a) Extremamente importante.
    - b) Muito importante.
    - c) Importante.
    - d) Pouco importante.
2. **O que mais te atraiu nas atividades sobre segurança na *internet*?**
    - a) Aprendizagem sobre senhas seguras.
    - b) Identificação de conteúdo seguro e perigoso.
    - c) Aprendizagem sobre privacidade online.
    - d) Reconhecimento de possíveis golpes na internet.
3. **Sentiste que as atividades ajudaram a compreender melhor os riscos associados ao uso da *internet*?**
    - a) Sim, completamente.
    - b) Sim, em certa medida.
    - c) Não tenho certeza.
    - d) Não, não ajudaram.
4. **Qual foi a parte mais interessante das atividades sobre segurança na *internet* para ti?**
    - a) Jogos educativos.
    - b) Vídeos informativos.
    - c) Discussões em grupo.
    - d) Exemplos de situações reais.
5. **Sentes-te mais confiante para lidar com problemas de segurança na *internet* após as atividades?**
    - a) Sim, muito mais confiante.
    - b) Sim, um pouco mais confiante.
    - c) Não tenho certeza.
    - d) Não, não me sinto mais confiante.
6. **Recordaste de alguma dica ou conselho específico que aprendeste durante as atividades sobre segurança na internet?**
    - a) Sim, recordo-me de algumas.
    - b) Não, não me lembro de nenhuma.
    - c) Não participei nas atividades.

- d) Preferia não responder.

7. **Achas que as atividades poderiam ser melhoradas de alguma forma?**
    - a) Sim, acho que poderiam ser melhoradas.
    - b) Não, acho que estavam bem como estavam.
    - c) Não sei, não pensei nisso.
    - d) Não participei nas atividades.
8. **Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?**
    - a) Sim, com muitos deles.
    - b) Sim, com alguns deles.
    - c) Não, não partilhei com ninguém.
    - d) Não, preferi manter o que aprendi para mim.
9. **Achas que a escola deveria oferecer mais atividades sobre segurança na internet no futuro?**
    - a) Sim, definitivamente.
    - b) Talvez.
    - c) Não tenho opinião.
    - d) Não, já é suficiente.
10. **Consideras que as atividades sobre segurança na internet foram adequadas à tua idade e compreensão?**
    - a) Sim, completamente.
    - b) Sim, em certa medida.
    - c) Não tenho certeza.
    - d) Não, acho que foram muito avançadas ou muito básicas.

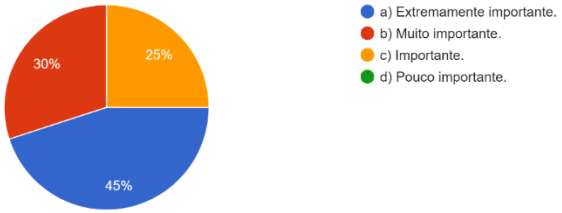
ANEXO P3 – RESULTADOS OBTIDOS

Turma	Extremamente importante (%)	Muito importante (%)	Importante (%)	Pouco importante (%)	Total de Respostas
4.º A	45	30	25	0	20
4.º B	73,7	21,1	5,2	0	19
4.º C	59,1	31,8	9,1	0	22
4.º D	46,7	40	13,3	0	15

4.º A

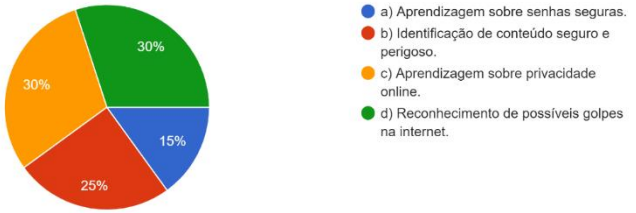
1. Como avalias a importância das atividades relacionadas à segurança na internet realizadas durante as aulas?

20 respostas

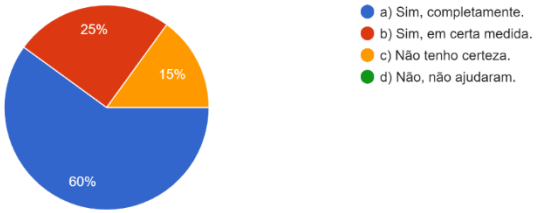


2. O que mais te atraiu nas atividades sobre segurança na internet?

20 respostas

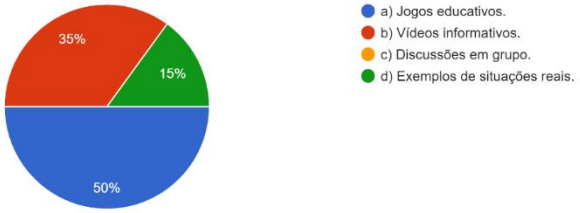


20 respostas



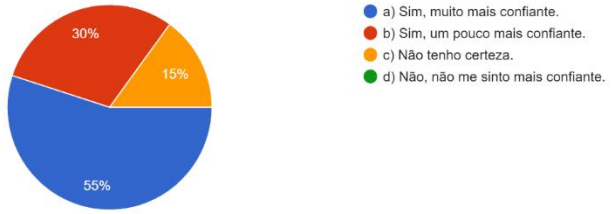
4. Qual foi a parte mais interessante das atividades sobre segurança na internet para ti?

20 respostas



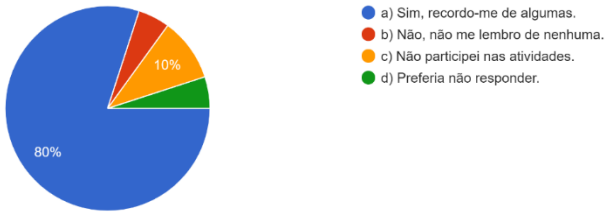
5. Sentes-te mais confiante para lidar com problemas de segurança na internet após as atividades?

20 respostas



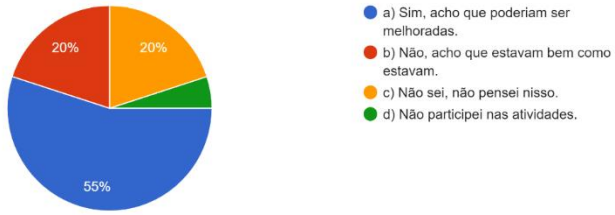
6. Recordaste de alguma dica ou conselho específico que aprendeste durante as atividades sobre segurança na internet?

20 respostas



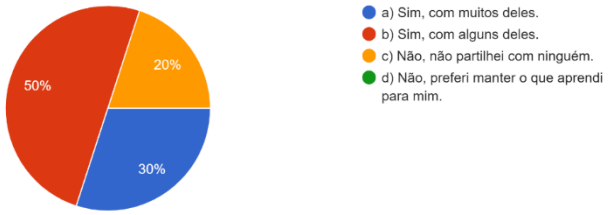
7. Achas que as atividades poderiam ser melhoradas de alguma forma?

20 respostas



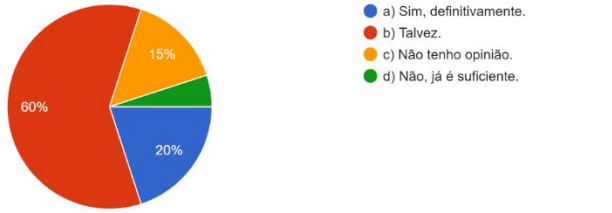
8. Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?

20 respostas



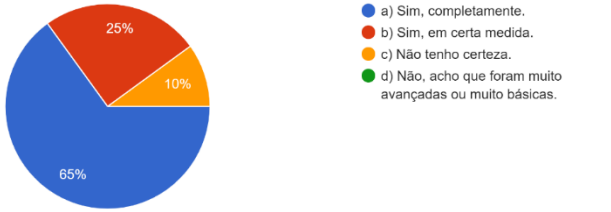
9. Achas que a escola deveria oferecer mais atividades sobre segurança na internet no futuro?

20 respostas



10. Consideras que as atividades sobre segurança na internet foram adequadas à tua idade e compreensão?

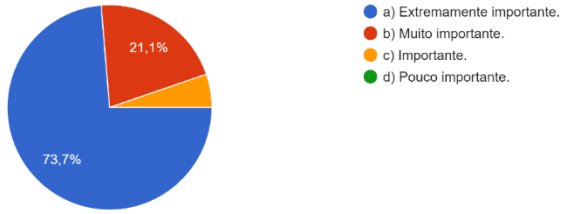
20 respostas



4.º B

1. Como avalias a importância das atividades relacionadas à segurança na internet realizadas durante as aulas?

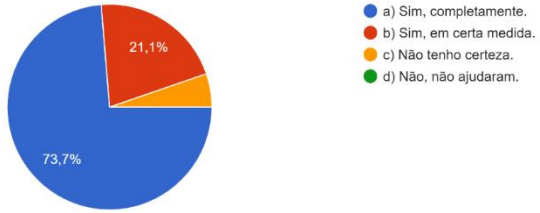
19 respostas



2. O que mais te atraiu nas atividades sobre segurança na internet?

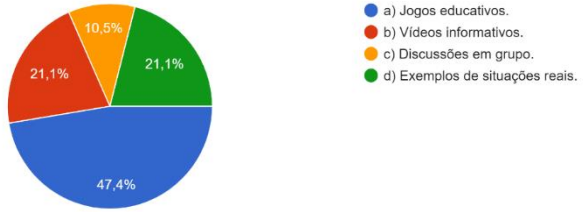
19 respostas

19 respostas



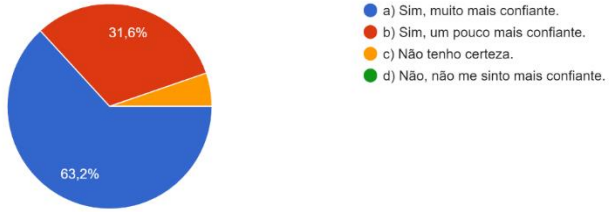
4. Qual foi a parte mais interessante das atividades sobre segurança na internet para ti?

19 respostas



5. Sentes-te mais confiante para lidar com problemas de segurança na internet após as atividades?

19 respostas



6. Recordaste de alguma dica ou conselho específico que aprendeste durante as atividades sobre segurança na internet?

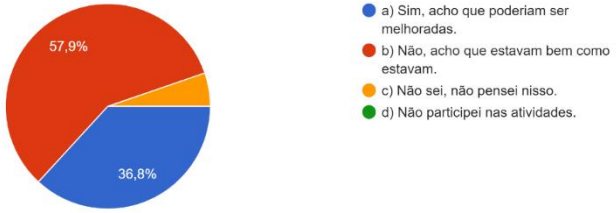
19 respostas

8. Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?

19 respostas

7. Achas que as atividades poderiam ser melhoradas de alguma forma?

19 respostas

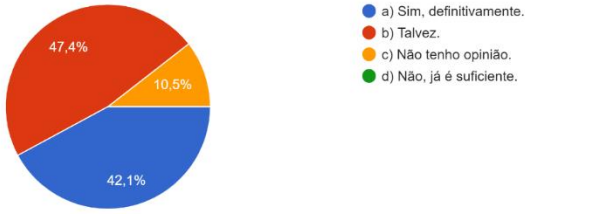


8. Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?

19 respostas

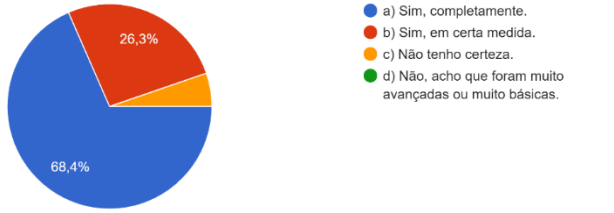
9. Achas que a escola deveria oferecer mais atividades sobre segurança na internet no futuro?

19 respostas



10. Consideras que as atividades sobre segurança na internet foram adequadas à tua idade e compreensão?

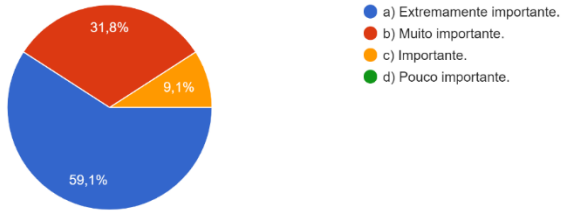
19 respostas



4.º C

1. Como avalias a importância das atividades relacionadas à segurança na internet realizadas durante as aulas?

22 respostas

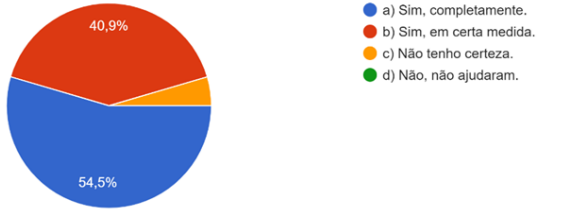


2. O que mais te atraiu nas atividades sobre segurança na internet?

22 respostas

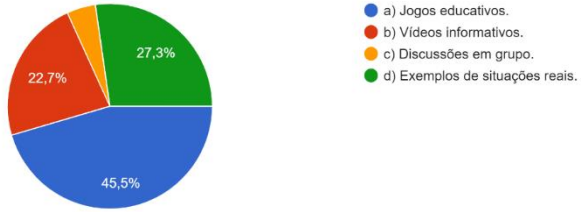
3. Sentiste que as atividades ajudaram a compreender melhor os riscos associados ao uso da internet?

22 respostas



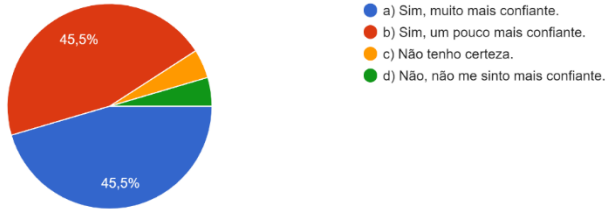
4. Qual foi a parte mais interessante das atividades sobre segurança na internet para ti?

22 respostas



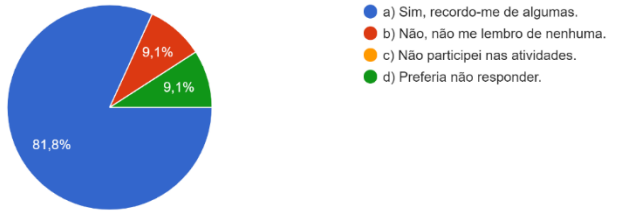
5. Sentes-te mais confiante para lidar com problemas de segurança na internet após as atividades?

22 respostas



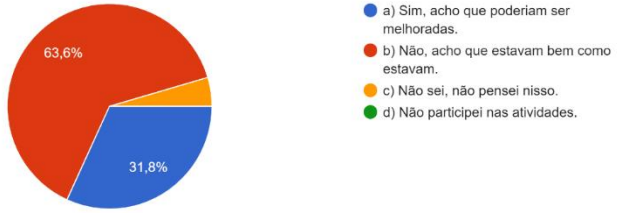
6. Recordaste de alguma dica ou conselho específico que aprendeste durante as atividades sobre segurança na internet?

22 respostas



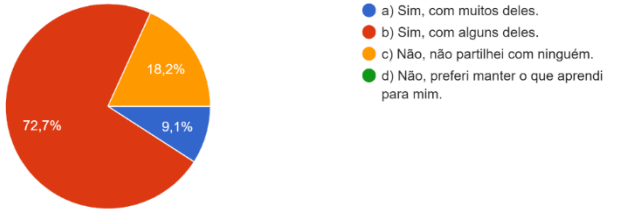
7. Achas que as atividades poderiam ser melhoradas de alguma forma?

22 respostas



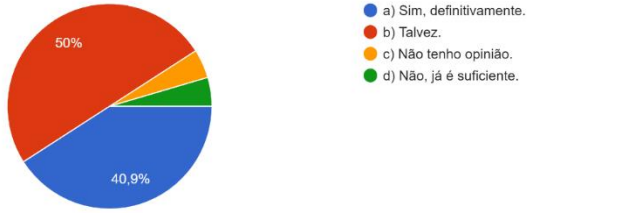
8. Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?

22 respostas



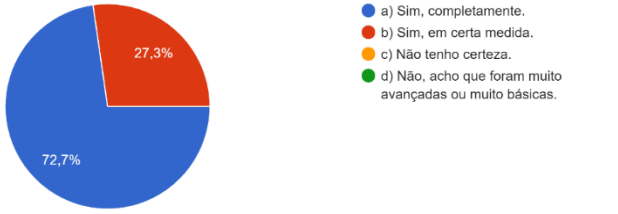
9. Achas que a escola deveria oferecer mais atividades sobre segurança na internet no futuro?

22 respostas



10. Consideras que as atividades sobre segurança na internet foram adequadas à tua idade e compreensão?

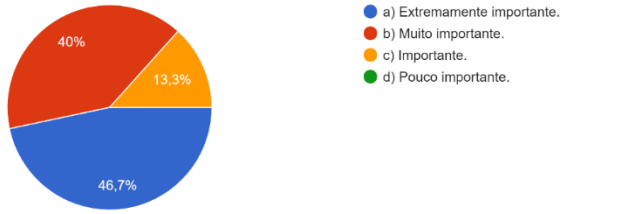
22 respostas



4.º D

1. Como avalias a importância das atividades relacionadas à segurança na internet realizadas durante as aulas?

15 respostas

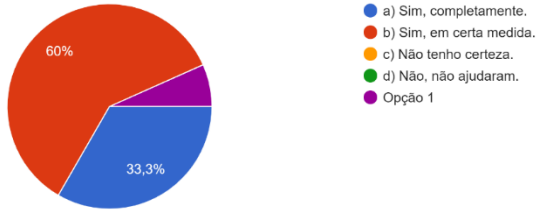


2. O que mais te atraiu nas atividades sobre segurança na internet?

15 respostas

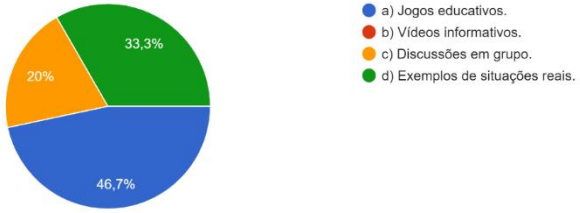
3. Sentiste que as atividades ajudaram a compreender melhor os riscos associados ao uso da internet?

15 respostas



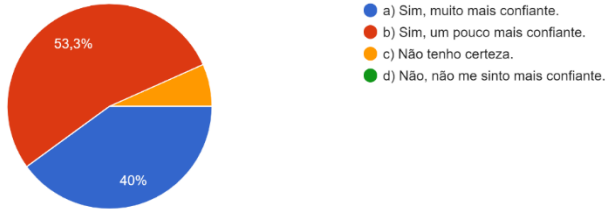
4. Qual foi a parte mais interessante das atividades sobre segurança na internet para ti?

15 respostas



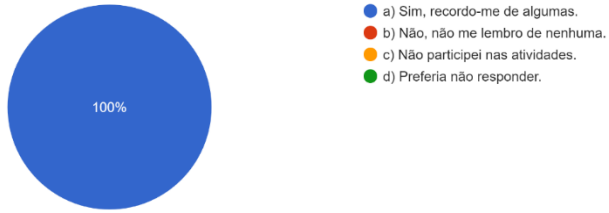
5. Sentes-te mais confiante para lidar com problemas de segurança na internet após as atividades?

15 respostas



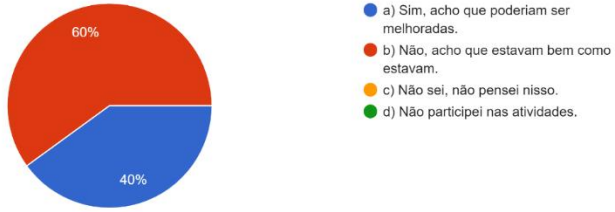
6. Recordaste de alguma dica ou conselho específico que aprendeste durante as atividades sobre segurança na internet?

15 respostas



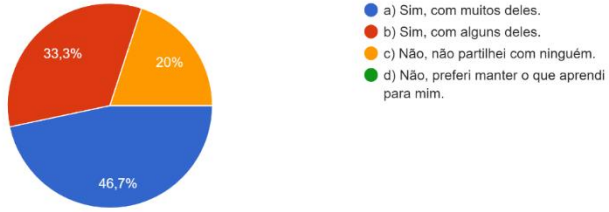
7. Achas que as atividades poderiam ser melhoradas de alguma forma?

15 respostas



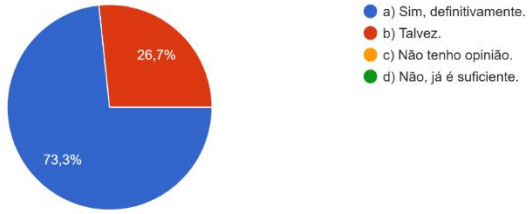
8. Partilhaste o que aprendeste sobre segurança na internet com os teus amigos ou familiares?

15 respostas



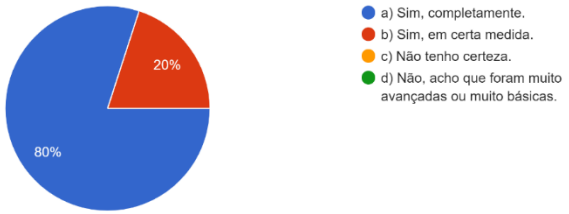
9. Achas que a escola deveria oferecer mais atividades sobre segurança na internet no futuro?

15 respostas



10. Consideras que as atividades sobre segurança na internet foram adequadas à tua idade e compreensão?

15 respostas



ANEXO Q – QUESTIONÁRIO – TABELA DE CORRESPONDÊNCIA DE RESPOSTAS DOS ALUNOS SOBRE PRÁTICAS DE SEGURANÇA DIGITAL

Pergunta	Resposta 1	Resposta 2	Resposta 3	Resposta 4
O que deves fazer se receberes uma mensagem de um desconhecido a pedir as tuas informações pessoais?	**Al 5**: Eu devo ignorar a mensagem e contar aos meus pais.	**Al 12**: Não devo responder e avisar um adulto.	**Al 33**: Devo bloquear a pessoa que enviou a mensagem.	**Al 44**: Devo apagar a mensagem e não clicar em nada.
Qual é a melhor prática para criar uma senha segura?	**Al 33**: Devo usar letras, números e símbolos.	**Al 5**: A minha senha deve ser longa e difícil de adivinhar.	**Al 20**: Devo mudar a minha senha regularmente.	**Al 70**: Nunca devo usar informações pessoais como senha.
Como podes saber se um *site* é seguro para navegar?	**Al 20**: Verificar se tem um cadeado na barra de endereço.	**Al 12**: O site deve começar com '*https*'.	**Al 33**: Pesquisar sobre o site antes de usar.	**Al 60**: Verificar a *URL* e certificar que é a oficial.
O que é *malware* e como pode afetar o teu computador?	**Al 55**: É um *software* mau que pode danificar o meu computador.	**Al 60**: Pode roubar as minhas informações e deixar o meu computador lento.	**Al 44**: Pode fazer o meu computador travar.	**Al 70**: Pode instalar programas maus sem eu saber.
Por que é importante não partilhar a tua senha com ninguém?	**Al 5**: Para que ninguém possa aceder às minhas contas sem permissão.	**Al 12**: Porque outras pessoas podem fazer coisas más com a minha conta.	**Al 33**: Para ninguém roubar as minhas coisas.	**Al 20**: Porque as senhas são pessoais e privadas.
O que deves fazer se encontrares um *link* suspeito?	**Al 70**: Eu não devo clicar no *link* e avisar um adulto.	**Al 12**: Devo ignorar o *link* e dizer a um professor.	**Al 60**: Devo apagar o *link*.	**Al 55**: Devo sair do site e não clicar em nada.
Como podes proteger as tuas informações pessoais nas redes sociais?	**Al 20**: Não devo partilhar a minha localização.	**Al 5**: Devo tornar o meu perfil privado.	**Al 33**: Não devo aceitar pedidos de amizade de estranhos.	**Al 70**: Devo pensar antes de postar qualquer coisa.

Pergunta	Resposta 1	Resposta 2	Resposta 3	Resposta 4
O que deves fazer se alguém te fizer sentir mal *online*?	**AI 12**: Contar a um adulto de confiança.	**AI 33**: Bloquear a pessoa que me fez sentir mal.	**AI 20**: Guardar provas e denunciar.	**AI 44**: Não responder e falar com os meus pais.
Como deves agir ao receber um email de um remetente desconhecido?	**AI 5**: Devo apagá-lo sem abrir.	**AI 20**: Devo marcar como spam.	**AI 33**: Não devo clicar em links nem abrir anexos.	**AI 12**: Devo contar a um adulto.
Por que é importante ter um antivírus instalado no computador?	**AI 12**: Para proteger contra vírus e *malware*.	**AI 70**: Para manter o meu computador seguro.	**AI 33**: Para evitar que hackers acedam ao meu computador.	**AI 55**: Para detetar e remover ameaças.
O que é phishing e como te podes proteger dele?	**AI 20**: É quando alguém tenta enganar-te para roubar informações pessoais.	**AI 12**: Nunca clicar em links suspeitos.	**AI 5**: Verificar o remetente do email.	**AI 33**: Contar aos meus pais ou professores.
Como deves agir quando usas um computador público?	**AI 60**: Nunca guardar as minhas senhas.	**AI 33**: Sair das minhas contas antes de sair.	**AI 70**: Não fazer compras *online*.	**AI 44**: Apagar o histórico de navegação.
O que deves fazer se um estranho te abordar online?	**AI 33**: Dizer aos meus pais.	**AI 12**: Bloquear e denunciar a pessoa.	**AI 20**: Não responder e sair da conversa.	**AI 5**: Contar a um adulto de confiança.
Por que não deves partilhar fotos pessoais online?	**AI 12**: Porque estranhos podem vê-las.	**AI 33**: Porque pode ser perigoso.	**AI 20**: Para proteger a minha privacidade.	**AI 70**: Porque não sei quem vai ver.
Como podes saber se uma app é segura para instalar?	**AI 55**: Ler as avaliações.	**AI 20**: Verificar a classificação.	**AI 33**: Perguntar aos meus pais.	**AI 60**: Ver se é de uma fonte confiável.
O que deves fazer antes de descarregar um ficheiro da *internet*?	**AI 12**: Verificar se o *site* é seguro.	**AI 33**: Perguntar a um adulto.	**AI 70**: Ver se tem vírus.	**AI 20**: Certificar que é um site confiável.
Por que é importante não conversar *com* estranhos *online*?	**AI 33**: Porque podem ser perigosos.	**AI 20**: Porque não sei quem são.	**AI 12**: Porque podem querer enganar-me.	**AI 5**: Para estar seguro.
Como deves proteger o teu dispositivo móvel?	**AI 70**: Colocar uma senha.	**AI 55**: Não partilhar o meu dispositivo.	**AI 33**: Instalar um antivírus.	**AI 12**: Fazer *backups* regulares.

Pergunta	Resposta 1	Resposta 2	Resposta 3	Resposta 4
O que deves fazer se receberes um pedido de amizade de alguém que não conheces?	**AI 20**: Não aceitar e contar aos meus pais.	**AI 33**: Ignorar o pedido.	**AI 44**: Bloquear a pessoa.	**AI 12**: Verificar quem é primeiro.
Como deves agir se encontrares conteúdo inapropriado *online*?	**AI 5**: Dizer a um adulto.	**AI 33**: Fechar a página imediatamente.	**AI 70**: Denunciar o conteúdo.	**AI 55**: Não continuar a ver.
Por que é importante ler os termos e condições antes de usar um serviço online?	**AI 60**: Para saber o que estou a aceitar.	**AI 33**: Para entender as regras.	**AI 20**: Para proteger a minha privacidade.	**AI 12**: Para saber se é seguro.
O que é uma *firewall* e como ela ajuda a proteger o teu computador?	**AI 33**: É um *software* que bloqueia ameaças.	**AI 60**: Ajuda a manter os *hackers* afastados.	**AI 70**: Protege contra ataques *online*.	**AI 55**: Controla o tráfego na **internet**.

ANEXO R – QUESTIONÁRIO – TABELA DE ATIVIDADES, TÉCNICAS, INSTRUMENTOS E ANÁLISE DE DADOS

Atividade	Técnica	Instrumento	Análise de Dados	Categorias de Análise	ANEXO
Atividade com *Post-its*	Observação	Grelha de Observação	Análise de conteúdo	- Identificação de Perigos - Importância de Conhecer os Perigos	ANEXO C1 - Grelha de Análise de Conteúdo - Tema: Atividade com ***Post-its***
Pesquisa na *Internet*	Inquérito, Observação	Questionário, Grelha de Observação	Análise de conteúdo	- Perigos na *Internet* - Privacidade *Online* - Reflexão Crítica - Colaboração e Comunicação	ANEXO D1 - Grelha de Análise de Conteúdo - Tema: Pesquisa na *Internet*
Jogos de Segurança na *Internet*	Observação, *Focus Group*	Grelha de Observação, Discussão em Grupo	Análise de conteúdo	- Consciencialização sobre Segurança Digital - Participação no Jogo - Reflexão e Debate	ANEXO E1 - Grelha de Análise de Conteúdo - Tema: Jogos de Segurança na *Internet*
Criação Visual no *Canva*	Análise Documental, Observação	Produção de Conteúdo Digital (*Posters*)	Análise de conteúdo	- Identificação de Perigos - Criação Visual - Reflexão e Discussão	ANEXO L1 - Grelha de Análise de Conteúdo - Tema: Criação Visual no *Canva*
Visualização de Vídeos	Observação, *Focus Group*	Exibição de vídeos, Grelha de Observação	Análise de conteúdo	- Consciencialização - Atenção - Compreensão - Participação - Avaliação Crítica - Aplicação	ANEXO F1 - Grelha de Análise de Conteúdo - Tema: Visualização de Vídeos
Mentimeter	Observação, *Focus Group*	Ferramenta *Mentimeter*, Grelha de Observação	Análise de conteúdo	- Consciencialização - Pesquisa e Reflexão - Comunicação	ANEXO K1 - Grelha de Análise de Conteúdo - Tema: *Mentimeter*

Atividade	Técnica	Instrumento	Análise de Dados	Categorias de Análise	ANEXO
				- Criação - Reflexão	
Dia Internacional da *Internet* Segura (GNR)	Observação, *Focus Group*	Discussão guiada, Grelha de Observação	Análise de conteúdo	- Identificação de Comportamentos Seguros - Reflexão Crítica - Pensamento Crítico - Colaboração e Comunicação	ANEXO N1 - Grelha de Análise de Conteúdo - Tema: Dia Internacional da *Internet* Segura (GNR)
Explorando a Segurança Digital: Comprovando Conhecimentos na Prática	Inquérito, *Focus Group*	Formulário de avaliação, Discussão em grupo	Análise de conteúdo	- Importância da Segurança na *Internet* - Comportamentos Seguros na *Internet* - Discussão dos Resultados - Melhoria da Segurança na *Internet*	ANEXO D1 - Grelha de Análise de Conteúdo - Tema: Explorando a Segurança Digital
Pesquisa sobre Perigos *Online* (*Google Docs*)	Inquérito, Análise Documental	Pesquisa online, *Google Docs*	Análise de conteúdo	- Pesquisa sobre Perigos *Online* - Privacidade Online - Responsabilidade Digital - Colaboração em Grupos	ANEXO D1 - Grelha de Análise de Conteúdo - Tema: Pesquisa na *Internet*
Discussão de Estratégias de Segurança	Observação, *Focus Group*	Grelha de Observação, Discussão em grupo	Análise de conteúdo	- Discussão sobre Estratégias de Segurança - Reflexão Crítica sobre Práticas Seguras	ANEXO E1 - Grelha de Análise de Conteúdo - Tema: Jogos de Segurança na Internet

Atividade	Técnica	Instrumento	Análise de Dados	Categorias de Análise	ANEXO
Discussão sobre Direitos Digitais: A Voz das Crianças na Internet	*Focus Group*, Observação	Grelha de Observação, Discussão guiada	Análise de conteúdo	- Identificação de Direitos Digitais - Importância dos Direitos Digitais - Criação e Expressão - Reflexão e Discussão	ANEXO O1 - Grelha de Análise de Conteúdo - Tema: Direitos Digitais: A Voz das Crianças na *Internet*
Criação de Nuvens de Palavras no *Mentimeter*	Observação, *Focus Group*	Ferramenta *Mentimeter*, Discussão em Grupo	Análise de conteúdo	- Identificação de Perigos - Comunicação - Criação de Conteúdo - Reflexão	ANEXO K1 - Grelha de Análise de Conteúdo - Tema: *Mentimeter*
Discussão de Soluções para Riscos *Online*	Observação, *Focus Group*	Grelha de Observação, Discussão em grupo	Análise de conteúdo	- Resolução de Problemas - Colaboração e Comunicação - Reflexão Crítica	ANEXO N1 - Grelha de Análise de Conteúdo - Tema: Dia Internacional da *Internet* Segura (GNR)
Discussão sobre Comportamentos Seguros nas Redes Sociais	Observação, *Focus Group*	Grelha de Observação, Discussão em grupo	Análise de conteúdo	- Identificação de Comportamentos Seguros - Reflexão Crítica sobre Práticas Seguras	ANEXO N1 - Grelha de Análise de Conteúdo - Tema: Dia Internacional da *Internet* Segura (GNR)