

WEB GUARDIANS

NAVEGANDO COM SEGURANÇA NA INTERNET

**GUARDIÕES DA PRIVACIDADE:
PROTEGENDO SEUS DADOS**



Cláudia Regina Costa Braga
Mirelle Pereira da Silva

3

VOLUME 3

**GUARDIÕES DA
PRIVACIDADE:
PROTEGENDO
SEUS DADOS**

Universidade Estadual de Montes Claros - Unimontes

Wagner de Paulo Santiago
Reitor

Dalton Caldeira Rocha
Vice-Reitor

Ivana Ferrante Rebello
Pró-Reitora de Ensino

Marlon Cristian Toledo Pereira
Pró-Reitor de Pós-Graduação

Maria das Dores Magalhães Veloso
Pró-Reitora de Pesquisa

Cláudia Luciana Tolentino Santos
Pró-Reitora de Planejamento, Gestão e Finanças

Rogério Othon Teixeira Alves
Pró-Reitor de Extensão

©Editora Unimontes

Maria Clara Maciel de Araújo Ribeiro
Editora Chefe

Conselho Editorial

Maria Clara Maciel de Araújo Ribeiro
Gustavo Henrique Cepolini Ferreira
Ivana Ferrante Rebello
Leandro Luciano Silva Ravnjak
Luiz Henrique Carvalho Penido
Patrícia Takaki Neves
Tânia Marta Maia Fialho
Vanessa de Andrade Royo

Apoio:



Cláudia Regina Costa Braga
Mirelle Pereira da Silva

VOLUME 3

GUARDIÕES DA PRIVACIDADE: PROTEGENDO SEUS DADOS


EDITORA
Unimontes

Coordenadores da Coleção
Fábia Magali Santos Vieira
Alcino Franco de Moura Júnior
Christine Martins de Matos
Lérica Maria Mendes Veloso
Vanderson Gonçalves da Silva

Laura Silveira Fahel
Projeto gráfico, capa e diagramação

Antônio Durães de Oliveira Neto
Maria da Penha Brandim de Lima
Revisão linguística

Maria Clara Maciel de Araújo Ribeiro
Maria Gabriela de Souza
Luana Pereira Santos
Equipe Editorial

Este livro foi selecionado por edital e submetido a parecer duplo cego.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Silva, Mirelle Pereira da Guardiões da privacidade: [livro eletrônico]:
protegendo seus dados / Mirelle Pereira da Silva, Cláudia Regina
Costa Braga; coordenadores Fábila Magali Santos Vieira... [et al.].
-- 1. ed. -- Montes Claros, MG : Editora Unimontes, 2025. -- (Web
guardians: navegando com segurança na internet; volume 3)
PDF

Outros coordenadores: Alcino Franco de Moura Júnior, Christine
Martins de Matos, Lérica Maria Mendes Veloso, Vanderson Gonçalves
da Silva

ISBN 978-85-7739-764-8

1. Educação 2. Cibernética - Medidas de segurança 3. Crianças e
adolescentes 4. Cultura digital 5. Internet - Medidas de segurança
6. Proteção de dados I. Braga, Cláudia Regina Costa. II. Vieira, Fábila
Magali Santos. III. Moura Junior, Alcino Franco de. IV. Matos, Christine
Martins de. V. Veloso, Lérica Maria Mendes. VI. Silva, Vanderson
Gonçalves da. VII. Título VIII. Série.

25-304182.0

CDD-005.8

Índices para catálogo sistemático:

1. Internet : Medidas de segurança : Ciência da computação 005.8
Maria Alice Ferreira - Bibliotecária - CRB-8/7964

©Editora Unimontes

Campus Universitário Professor Darcy Ribeiro
Montes Claros - Minas Gerais - Brasil, CEP 39401-089 - Caixa Postal 126.
www.editora.unimontes.br | editora@unimontes.br

Filiada à



VOLUMES DA COLEÇÃO WEBGUARDIANS

VOLUME 1

Antes de clicar: conhecer, prevenir, proteger

VOLUME 2

Explorando a internet

VOLUME 3

Guardiões da privacidade: protegendo seus dados

VOLUME 4

Aventuras na navegação: reconhecendo e evitando perigos na internet

VOLUME 5

Derrotando vilões: o *cyberbullying*

VOLUME 6

Identidade digital: construindo uma presença virtual segura e consciente na cultura digital

VOLUME 7

Entre Likes e Laços: construindo relações saudáveis na internet

VOLUME 8

Universo Gamer Consciente: diversão com limites e valores

VOLUME 9

Direitos Digitais: navegar com consciência e responsabilidade

SUMÁRIO



Apresentação da Coleção WebGuardians 09

Apresentação do Volume 3 12

1 Introdução 16

2 Conteúdos 19

3 Objetivos 20

4 Navegando juntos 21

5 Planejando o ensino 34

6 Mãos à obra 37

7 Integração do tema com outras disciplinas 62

8 Conectando saberes 66

9 Mais informações 68

10 Para explorar mais 70

Referências 71

APRESENTAÇÃO DA COLEÇÃO WEBGUARDIANS

Prezados(as) educadores(as), pais, mães e responsáveis,

Vivemos em uma era em que a presença digital é parte inseparável da vida cotidiana de crianças e adolescentes. A internet oferece inúmeras possibilidades de aprendizagem, comunicação e entretenimento, mas também expõe esse público a riscos que nem sempre compreendem plenamente, nem estão preparados para enfrentar sozinhos. Nesse cenário, torna-se essencial compreender como crianças e adolescentes reagem aos riscos presentes na internet e de que forma estratégias educativas e a mediação parental podem promover práticas de navegação segura e cidadania digital crítica.

Foi com esse propósito que nasceu o projeto de ensino da Universidade Estadual de Montes Claros, Unimontes, *WebGuardians: Navegando com Segurança na Internet*, aprovado e financiado pela FAPEMIG, em desenvolvimento na Escola Estadual João Miguel Teixeira de Jesus, em Montes Claros/MG. A iniciativa tem como objetivo orientar pais e professores para preparem as crianças e adolescentes da Educação Básica para o uso crítico, seguro e consciente da internet, com base em práticas educativas integradas à mediação familiar e escolar.

A presente coleção didática é fruto das ações do Grupo de Pesquisa HUB de Educação Digital, da Universidade

Estadual de Montes Claros – Unimontes. Ela foi cuidadosamente elaborada para auxiliar educadores, responsáveis e estudantes na compreensão dos desafios e possibilidades do ambiente digital, oferecendo abordagens lúdicas e educativas para uma convivência online ética e segura.

SOBRE A COLEÇÃO

Cada volume da coleção aborda um tema essencial da segurança digital, como a proteção de dados, o enfrentamento ao *cyberbullying*, a construção da identidade digital e o equilíbrio no uso das tecnologias. Veja abaixo a estrutura da série:

Volumes	Título
1	Antes de clicar: conhecer, prevenir, proteger
2	Explorando a internet
3	Guardiões da privacidade: protegendo seus dados
4	Aventuras na navegação: reconhecendo e evitando perigos na internet
5	Derrotando vilões: o <i>cyberbullying</i>
6	Identidade digital: construindo uma presença virtual segura e consciente na cultura digital
7	Entre Likes e Laços: construindo relações saudáveis na internet
8	Universo Gamer Consciente: diversão com limites e valores
9	Direitos Digitais: navegar com consciência e responsabilidade

Além de trazer materiais acessíveis e adaptados à realidade dos estudantes da Educação Básica, cada volume conta com seções dedicadas a educadores e familiares, incluindo orientações, propostas de atividades, sugestões de leitura e recomendações para mediação e diálogo com os jovens.

POR QUE WEBGUARDIANS?

Porque acreditamos que proteger não é isolar, e sim formar. A formação de jovens cidadãos digitais exige uma rede de apoio – entre escola, família e comunidade – que promova o uso consciente das tecnologias, a empatia nas interações e a responsabilidade no ambiente virtual.

Convidamos você a fazer parte desta rede. A coleção *WebGuardians* está à disposição para apoiar seu trabalho em sala de aula ou em casa, promovendo reflexões, ações preventivas e práticas educativas inovadoras.

• Em caso de dúvidas, sugestões ou interesse em parceria, acesse nossa plataforma WebGuardians para dialogar com a equipe, compartilhar experiências e acessar materiais complementares.

SEJAM BEM-VINDOS À NOSSA MISSÃO.

Junte-se aos WebGuardians. Vamos juntos construir uma internet mais segura e cidadã para todos.



APRESENTAÇÃO DO VOLUME 3

Prezados(as) Professores(as),

Em meio a avalanche de informações e inovações tecnológicas, vocês já sabem quem de fato está no controle?

Somos nós os usuários que consumimos produtos ou somos nós mesmos os produtos que estão sendo consumidos? O fato é que, quando realizamos pesquisas na internet, deixamos rastros digitais que podem ser utilizados para criar perfis detalhados sobre nossos hábitos, gostos e até mesmo nossos medos.

Por conhecermos alguns riscos, buscamos tomar o máximo de cuidado com dados e informações que compartilhamos. As crianças e adolescentes, embora nativos digitais, estão também suscetíveis aos riscos e crimes virtuais, por isso, cabe a nós, professores, com nosso dever legal e social, protegê-los a partir de uma abordagem orientadora e educacional, ações que desenvolvam autonomia e o pensamento crítico, que possam distinguir conteúdos apropriados dos impróprios.

Desse modo, é com satisfação que apresentamos o Volume 3, *Guardiões da privacidade: protegendo seus dados*, da coleção *WebGuardians: Navegando com Segurança na Internet!*, projeto cujas atividades são desenvolvidas pelo Programa de Ensino, Pesquisa e Extensão do *Educar*:

Laboratório Multiusuário de Tecnologias Digitais na Educação, do Departamento de Métodos e Técnicas, da Universidade Estadual de Montes Claros Unimontes, vem a contribuir com a formação de professores para ensinar e orientar crianças e adolescentes da Educação Básica para o uso consciente e responsável da internet.

O objetivo principal deste volume é discutir com as crianças e os adolescentes questões de privacidade e segurança na internet, orientando-os a navegar de forma responsável e proteger suas informações pessoais.

Assim, organizamos um material que oferece um conjunto de recursos pedagógicos para o ensino da privacidade e segurança digital com referencial teórico e atividades práticas para todas as etapas do Ensino Fundamental e Ensino Médio. Este volume busca auxiliá-los no desenvolvimento de um trabalho organizado e teoricamente fundamentado. Nele, são abordados como a importância da privacidade na internet; informações pessoais: o que compartilhar e o que não compartilhar; senhas seguras e proteção de contas online e internet segura: encontrando informações confiáveis.

Além disso, o material inclui sugestões de dinâmicas, atividades reflexivas, recursos pedagógicos necessários e formas de avaliação, proporcionando aos professores o necessário para promover uma educação digital segura e interessante, alinhada com o desenvolvimento e anseios da sociedade.

Assim, convidamos os professores não apenas a incorporar *Guardiões da Privacidade: protegendo seus dados* em seu planejamento pedagógico, mas também a colaborar com o projeto, sugerindo atividades e melhorias. Juntos, podemos mostrar aos estudantes

que estamos a dois cliques de resultados positivos ou negativos, reforçando que navegar na internet requer cautela e responsabilidade.

As autoras

INTRODUÇÃO

Nos últimos anos, testemunha-se um rápido avanço tecnológico e digital, no qual a internet desempenhando um papel fundamental na disseminação de informações. Além de facilitar as diversas atividades diárias, ela desperta o fascínio e atrai a atenção da sociedade, principalmente de adolescentes e crianças.

De acordo com Prensky (2001), desde os anos 2000 até os dias atuais, crianças e adolescentes são considerados nativos na linguagem digital de computadores, videogames, bem como da internet e de outras tecnologias, o que leva o autor a classificá-los como “nativos digitais”. Essa imersão precoce na era digital tem mudado a maneira como eles interagem e se envolvem com o mundo real. Contudo, não podemos fechar os olhos para os riscos e crimes cibernéticos dos quais essas personagens podem ser vítimas ou estar envolvidos.

Nesse sentido, este volume está respaldado na Competência Geral 5 da Base Nacional Comum Curricular (BNCC), a qual prevê a formação crítica de crianças e adolescentes para que eles possam adotar uma abordagem significativa, reflexiva e ética no uso das tecnologias digitais em diversos contextos sociais, incluindo a educação (Brasil, 2018). Em outras palavras, eles devem utilizar essas tecnologias para se comunicar, acessar informações, compartilhá-las, criar conhecimento, solucionar problemas e desempenhar um papel ativo e autêntico em suas vidas pessoais e na sociedade em geral.

No ambiente educacional, os aparelhos tecnológicos, as tecnologias digitais, generativas e emergentes, as redes sociais e a constante troca de informação surgem como poderosas ferramentas para atingir os objetivos propostos pela BNCC. Discutir a importância da privacidade, da segurança online e da proteção de dados na educação prepara os nativos digitais para enfrentar os desafios tecnológicos e complexos de maneira precisa, criativa e ética.

Para facilitar, em termos de definição, as **tecnologias generativas** (genAI) são sistemas de inteligência artificial (IA) capazes de criar conteúdos, conforme orientações recebidas. Disponível em: <https://blog.crowd.br.com/ai-generativa/>.

As **tecnologias emergentes** são recursos tecnológicos inovadores, que surgem com muita rapidez. Disponível em: <https://blog.cubo.network/tecnologias-emergentes>.

Dessa forma, este volume, que faz parte do projeto *WebGuardians: navegando com segurança na internet*, discute sobre a importância da proteção de dados e da segurança na internet. Esses temas são fundamentais para a formação de crianças e adolescentes, haja vista que o uso frequente da internet ao passo que traz inúmeros benefícios, expõe a privacidade e a segurança de suas informações pessoais a uma diversidade de riscos. Diante dessa realidade, é relevante orientá-los a navegar de maneira responsável, de modo a proteger seus dados e evitar condutas que possam colocá-los em situações arriscadas.

Especificamente, este material tem o intuito de:

(i) discutir os conceitos de privacidade e segurança na internet, destacando sua importância na era digital; (ii)

debater os principais riscos e ameaças à privacidade e à segurança online, como o roubo de identidade e o *cyberbullying*; e (iii) apresentar estratégias e boas práticas para proteger informações pessoais e dados sensíveis durante o uso da internet.

Para isso, ao longo deste volume, apresentamos um referencial teórico que servirá como fundamento para que o professor compreenda os conceitos relacionados à privacidade e à segurança online. Esse referencial, além de abordar os aspectos técnicos e legais, analisa os efeitos sociais e emocionais que a exposição indevida à internet pode ter sobre crianças e adolescentes. Ademais, são discutidos os principais riscos do ambiente digital, como o roubo de identidade e o *cyberbullying*, temas que estão cada vez mais presentes na vida dos jovens.

O volume também traz seis propostas de atividades, cada uma acompanhada de orientações e sugestões detalhadas. Elas foram pensadas para atender tanto aos Anos Iniciais e Finais do Ensino Fundamental quanto ao Ensino Médio, possibilitando que os professores adaptem o conteúdo de acordo com o perfil de seus estudantes. As atividades incentivam a reflexão sobre o uso consciente da internet e, ao mesmo tempo, promovem o desenvolvimento de estratégias práticas para proteger dados e informações pessoais.

Dessa maneira, esperamos que este material contribua para a formação e proteção de crianças e adolescentes, cumprindo o dever de garantir, com prioridade absoluta, a efetivação dos direitos fundamentais desses jovens.

CONTEÚDOS

- ➡ A importância da privacidade na internet;
- ➡ Informações pessoais: o que compartilhar e o que não compartilhar;
- ➡ Senhas seguras e proteção de contas online;
- ➡ Internet segura: encontrando informações protegidas e confiáveis.

OBJETIVOS

- ➡ Discutir com crianças e adolescentes questões relacionadas à privacidade e segurança na internet, orientando-os a navegar de forma responsável e a proteger suas informações pessoais;
- ➡ Compreender os conceitos de privacidade e segurança na internet, destacando sua importância na era digital;
- ➡ Debater os principais riscos e ameaças à privacidade e segurança online, como o roubo de identidade e o *cyberbullying*;
- ➡ Apresentar estratégias e boas práticas para proteger informações pessoais e dados sensíveis enquanto navegam na internet.

NAVEGANDO JUNTOS

As tecnologias digitais, o uso das redes sociais e o compartilhamento do nosso cotidiano se tornaram ações habituais, trazendo mudanças profundas na maneira como nos relacionamos. A busca constante por conexão é evidente, o que nos leva a compartilhar informações pessoais e dados sobre aqueles que estão ao nosso redor. Entretanto, é fundamental ter cuidado com esses detalhes, pois, muitas vezes, sem perceber, podemos revelar nossa localização geográfica, informações sobre nossas rotinas, dados familiares, nossas forças e fraquezas, e até mesmo aspectos acerca da nossa situação financeira.

As crianças e os adolescentes, ao nos tomarem como referência, tendem a imitar a maneira como nos comportamos diante desse universo virtual. Dessa forma, eles começam a acessar as redes sociais, jogos e sites, além de assistir a vídeos na internet, fazendo dessas atividades práticas diárias em suas próprias vidas. Ao navegarem pela internet, preenchem formulários e permitem que muitas informações sejam compartilhadas. No Brasil, de acordo com o texto do documento TIC Kids Online Brasil 2023¹ (Nic.br, 2023), 95% das crianças e adolescentes de 9 a 17 anos – aproximadamente 25 milhões – já acessaram

1 Pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br do Núcleo de Informação e Coordenação do Ponto.br - NIC.br. NIC.BR - Núcleo de Informação e Coordenação do Ponto.br. *TIC Kids Online Brasil 2023*: principais resultados. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://cetic.br/pt/pesquisa/kids-online/>. Acesso em: 29 set. 2024.

a internet, principalmente para atividades educativas e informativas, como trabalhos escolares, curiosidades e acesso a notícias. Além disso, eles utilizam a internet para procurar mapas, informações sobre saúde, oportunidades de emprego ou cursos e eventos em suas comunidades.

A partir das inovações tecnológicas, muitos aspectos da vida das crianças e dos adolescentes têm passado por mudanças. As tecnologias digitais apresentam um potencial expressivo para o desenvolvimento desse público, mas também trazem riscos que podem comprometer tanto a sua privacidade quanto a segurança. Segundo Sårts (2021):

[...] crianças e jovens são um dos grupos mais vulneráveis. Muitos deles são nativos digitais desde quando começam a andar (às vezes até antes disso). Um dos efeitos é a riqueza que os seus dados podem ter ao longo das suas vidas. Em termos de privacidade, isso significa que empresas e IAs não só podem chegar a um retrato completo de quem você é, o que você faz e como você age nesse momento, como também podem acompanhar esses dados ao longo de vários anos, potencialmente oferecendo percepções muito profundas sobre a personalidade e seus fatores determinantes (Sårts, 2021, p. 128).

Os nativos digitais, indivíduos que nasceram após os anos 2000 e que estão envolvidos com a linguagem digital de computadores, videogames e internet (Prensky, 2001), estão sob vigilância e coleta de dados pessoais por empresas e inteligências artificiais (IA), conforme Sårts (2021). Este sugere que, a partir da quantidade de informações disponíveis sobre os nativos digitais, as empresas têm o poder de delinear um perfil detalhado e saber quem a pessoa é, suas ações e seus comportamentos cotidianos. Além disso, ao coletar e analisar esses dados por longos períodos, essas empresas podem moldar a

maneira de pensar e o comportamento dessas crianças e adolescentes ao longo do tempo.

Isso ocasiona preocupações sobre a invasão de privacidade e o potencial uso dessas informações para manipulação ou controle. O ambiente virtual pode exercer uma profunda influência na forma como as crianças e os adolescentes se veem e percebem os outros, o que pode interferir na sua interação com o mundo real. Segundo Angeli *et al.* (2021):

No caso de crianças e adolescentes, o uso de dados pessoais é ainda mais preocupante, pois permite conhecer preferências, perfis de consumo, interesses, estado de saúde e outras tantas informações que podem ser danosas para esses seres em início da vida, uma vez que os dados podem ser utilizados de forma a prejudicá-los ou para influenciar e manipular o seu comportamento e conduta (Angeli *et al.*, 2021, p. 19).

Nesse sentido, entendemos a relevância em assegurar a privacidade e a segurança de crianças e adolescentes. O Estatuto da Criança e do Adolescente (ECA), instituído pela Lei n.º 8.069/1990, reconhece-os como sujeitos de direitos, com garantia de proteção integral. O Art. 4º do ECA enfatiza a responsabilidade compartilhada entre o Estado, a família e a sociedade em garantir, com prioridade absoluta, a efetivação dos direitos fundamentais à vida, saúde, educação, lazer e dignidade, além da proteção contra todas as formas de negligência, discriminação, exploração, violência e opressão (Brasil, 1990).

Diante do aumento expressivo do uso da internet por crianças e adolescentes, é importante que pais, responsáveis, educadores e o Estado trabalhem em conjunto, a fim de garantir sua segurança no ambiente digital. A vulnerabilidade característica dessa faixa etária

exige cuidados especiais, como o combate e a prevenção do *cyberbullying*; a restrição ao acesso a conteúdos indevidos; e a proteção de dados pessoais. É indispensável o investimento em educação digital, orientando crianças e adolescentes sobre os riscos e benefícios da internet, com o intuito de garantir a segurança e a privacidade desses jovens no mundo virtual.



Para saber mais, acesse:

Privacidade é uma ilusão?
- Nerdologia.



PRIVACIDADE E SEGURANÇA DIGITAL

No contexto legal, a privacidade trata do direito fundamental da pessoa em preservar suas informações pessoais, atividades e seus pensamentos protegidos da exposição ou acesso não autorizado por outras pessoas ou instituições. Ou seja, é a capacidade de controlar quais informações são compartilhadas, com quem são compartilhadas e de que maneira são utilizadas (Brasil, 2018).

Para facilitar, em termos de definição, o dicionário Houaiss da Língua Portuguesa (2001), apresenta a **privacidade**, como sendo aquilo que está relacionado à vida particular, algo privado e íntimo.

No ambiente virtual, a privacidade tornou-se uma preocupação crescente, devido à facilidade com

que as informações pessoais podem ser coletadas, compartilhadas e exploradas por terceiros, muitas vezes sem o conhecimento ou consentimento daqueles que estão envolvidos. Essa apreensão maneira é ainda mais intensa no caso de crianças e adolescentes, que se tornaram usuários vulneráveis a diversos perigos e crimes (Angeli *et al.* 2021).



Para saber mais, acesse:

Privacidade na Internet -
Nerdologia Tech.



No Brasil, atualmente, existem leis que estabelecem princípios, garantias, direitos e deveres para o uso da internet, como o Marco Civil da Internet, por meio da Lei n.º 12.965/2014 (Brasil, 2014), além de regulamentações que se preocupam com a proteção da privacidade dos dados dos usuários, como a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709, de 14 de agosto de 2018 (Brasil, 2018). Ambas as legislações contemplam dispositivos específicos para a proteção de crianças e adolescentes, com o intuito de garantir que possam acessar o ambiente digital com segurança.

Em relação ao Marco Civil da Internet, essa legislação aborda a proteção e o controle do conteúdo acessado por menores, além de promover a inclusão digital, com base nos princípios estabelecidos pela lei e pelo ECA, nos termos da seguinte legislação:

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores,

desde que respeitados os princípios desta Lei e da Lei n.º 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente (Brasil, 1990).

Esse documento discorre sobre o controle parental, que, conforme o Manual de Segurança Digital da Secretaria de Segurança da Informação e Cibernética (Brasil, 2014), refere-se às ferramentas que delimitam o acesso de crianças e adolescentes ao utilizarem dispositivos digitais. Esses programas têm o objetivo de bloquear conteúdos considerados inadequados para esses indivíduos. De acordo com a lei, a escolha desses aplicativos fica a critério dos responsáveis.

O manual mencionado define a mediação parental, que acreditamos ser uma medida colaborativa na proteção de crianças e adolescentes em relação à internet e ao acesso às tecnologias digitais de maneira orientada. A mediação parental está pautada em uma abordagem orientadora e educacional, que visa, por meio do diálogo, o desenvolvimento crítico, de modo que crianças e adolescentes sejam capazes de distinguir, por conta própria, os conteúdos apropriados dos impróprios.

A privacidade de crianças e adolescentes é um direito garantido também pelo Art. 14 da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709, de 14 de agosto de 2018 (Brasil, 2018). Esse artigo ressalta que o tratamento de dados de crianças e adolescentes deve sempre considerar o seu melhor interesse. Assim, em um contexto em que crianças e adolescentes estão cada vez mais conectados, a LGPD se alinha perfeitamente ao ECA, à Constituição Federal do Brasil e a outros

dispositivos legais que buscam assegurar os seus direitos, de modo a garantir que o tratamento de dados dessa faixa etária priorize sempre seu bem-estar, equilibrando-o com outras necessidades.



Para saber mais, acesse:

Crianças e Adolescentes na LGPD - Luana Piovani tinha razão? - Marcia Moreira.



Somos uma sociedade de acesso, conexão e compartilhamentos, e é perceptível a facilidade e a naturalidade com que crianças e adolescentes lidam e navegam pela internet. Quando discutimos segurança relacionada à internet, é importante pensá-las sob duas vertentes. A primeira está relacionada à segurança da informação, que, de acordo com Galegale, Fontes e Galegale (2017), refere-se à proteção dos dados, com o intuito de manter suas características fundamentais, como confidencialidade, integridade, disponibilidade e autenticidade.

A segunda vertente refere-se à segurança física, social, psicológica e emocional de crianças e adolescentes. Ao abordarmos essa questão, é preciso refletir sobre os motivos que justificam a existência dessa preocupação. Nesse caso, ela está associada aos problemas e riscos aos quais estão expostos a

[...] diversas formas de acessos a conteúdos inadequados, como pornográficos, discriminatórios e de ódio, os contatos potencialmente nocivos, como casos de aliciamento ou assédio, e a conduta problemática, como casos de cyberbullying e de invasão de privacidade (Dias *et al.* 2019, p. 2).

Segundo Laterça *et al.* (2021, p. 75), a interação precoce com as tecnologias – e, acrescentamos, com as

redes sociais – constrói “um rastro de dados, um mapa sobre si mesmas que poderá acompanhá-las por muito tempo”. A fragilidade na proteção da privacidade e na segurança de crianças e adolescentes expõe seus comportamentos e modos de pensar, muitas vezes levando à manipulação por terceiros.

Essa vulnerabilidade pode resultar em consequências graves, uma vez que os jovens são expostos a influências externas que podem moldar suas identidades e ações. Para Dias *et al.* (2019, p. 12), “experiências virtuais têm implicações subjetivas”. Dessa forma, torna-se fundamental acompanhar os usos que os adolescentes fazem do ambiente virtual.



Para saber mais, acesse:

Cartilha de Segurança para a Internet - CERT.



O ambiente digital oferece inúmeros benefícios, mas também traz consigo riscos que podem afetar não apenas o mundo virtual, mas também a realidade (CERT, 2012)².

INFORMAÇÕES PESSOAIS: O QUE COMPARTILHAR E O QUE NÃO COMPARTILHAR

A mídia tem evidenciado os casos de superexposição a que crianças e adolescentes estão sujeitos, dando

² CERT - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. *Cartilha de Segurança para Internet*, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 17 ago. 2023.

destaque para inúmeras ameaças resultantes da conexão com as redes sociais, como: pedofilia, roubo de dados, *bullying* e interações indesejadas. Muitos pais e responsáveis buscam por soluções que possam proteger crianças e adolescentes desses perigos da internet. No entanto, acreditamos que proibir o uso das tecnologias e da internet seria isolá-los do que acontece no mundo atual, uma vez que esses ambientes oferecem informações valiosas, que contribuem para o desenvolvimento acadêmico, social e cultural. Por isso, é fundamental protegê-los e mantê-los em segurança nesse meio digital.

Pedro e Chacon (2016) apresentam algumas orientações importantes para crianças e adolescentes, como: conversar com os pais e/ou professores caso sejam vítimas de *cyberbullying*; ter cuidado com o compartilhamento de fotos íntimas nos aplicativos e nas redes sociais, pensando bem antes de compartilhá-las; permitir que apenas amigos e familiares tenham acesso às suas postagens; ter cautela ao divulgar informações pessoais.

Além disso, Pedro e Chacon (2016, p. 18) orientam para “não acessar qualquer site ou *link*, principalmente aqueles que apresentem e ofereçam produtos com condições e ofertas que fujam da realidade”. Quando isso acontecer, pedir a orientação de um adulto; ter cuidado ao fazer “*downloads* e instalar programas nos computadores”. Por fim, os autores orientam também a “não aceitar qualquer pessoa como amigo, evitar sites e navegadores não confiáveis, evitar a superexposição nas redes sociais e aplicativos como *WhatsApp* e *Snapchat* e ter cuidado com o que compartilha” (Pedro; Chacon, 2016, p. 19).

Neste volume, apresentaremos as atividades a serem desenvolvidas com os estudantes para debate, discussão e construção de conhecimento a respeito da temática. Aconselhamos que, ao desenvolver a unidade, as referências citadas sejam consultadas.



Para saber mais, acesse:

Café Filosófico | Bullying e CyberBullying: Qual o papel da escola? - Café Filosófico.



SENHAS SEGURAS E PROTEÇÃO DE CONTAS ONLINE

Ao longo do tempo, podemos acumular inúmeras contas online, como e-mails, perfis no Instagram e no Facebook, entre outros exemplos. De acordo com o CERT (2012, p. 75), uma conta de usuário pode ser definida como a “identificação exclusiva de um indivíduo em um sistema computacional ou serviço”. Embora seja de conhecimento geral, o ideal é que o acesso a essas contas seja restrito ao usuário ou a alguém que tenha a permissão para acessá-las. Para garantir essa proteção, existe um mecanismo chamado *senha*, que permite a sua autenticação.

Segundo o CERT (2012, p. 75), a senha “serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão”. Ao criar senhas, precisamos considerar que elas serão utilizadas para acessar algumas

contas importantes para o desenvolvimento de nossas atividades cotidianas. Portanto, é essencial que essas senhas sejam fáceis de memorizar para nós, ao mesmo tempo que não sejam óbvias o suficiente a ponto de serem descobertas e exploradas por outras pessoas.

Mitnick e Simon (2003, p. 255) recomendam que as senhas “contenham pelo menos um número, um símbolo (tal como \$, -, !, &), uma letra minúscula e uma letra maiúscula (enquanto tais variáveis sejam suportadas pelo sistema operacional)”. Os autores ainda orientam para o que não utilizar na construção das senhas:

[...] palavras de um dicionário de qualquer idioma; qualquer palavra que esteja relacionada com família, hobbies, veículo, trabalho, placas do veículo, número de seguro social, endereço, telefone, nome do bichinho de estimação do empregado ou frases contendo essas palavras. [...] Não sejam a variação de uma senha usada anteriormente (Mitnick; Simon, 2003, p. 256).

Dessa forma, ao criar senhas, é importante sempre lembrar que elas nos protegem contra invasões e crimes cibernéticos. Por isso, para que cumpram essa função, é necessário considerar as dicas mencionadas acima.

INTERNET SEGURA: ENCONTRANDO INFORMAÇÕES CONFIÁVEIS

Estamos a dois passos de um clique! O universo em que vivemos é marcado pelo avanço da ciência, dos meios de comunicação e das tecnologias digitais. Para a maioria dos nativos digitais, não há como desvencilhar a internet do cotidiano. É até possível controlar o tempo de uso, mas ficar sem utilizá-la por um longo período é praticamente impossível.

Isso se deve ao fato de que inúmeras atividades, como pagar contas, estudar, produzir textos, realizar pesquisas, participar de aulas online, trabalhar remotamente, fazer inscrições em cursos, interagir com familiares e amigos por meio de redes sociais, ou até mesmo aproveitar momentos de lazer assistindo a filmes e ouvindo música, são facilitadas e, em muitos casos, dependem da conectividade.

Todavia, além dos benefícios evidentes que a internet oferece, ela também traz consigo uma série de desafios e riscos. Com o imenso volume de informações que circula pela rede, é importante lembrar que, enquanto consumimos conteúdos, estamos constantemente compartilhando dados sobre nós mesmos. Muitas vezes, isso inclui dados sensíveis, que podem ser alvo de roubo ou de uso indevido.

Estudos como o realizado pelo CERT (2012), destacam os riscos associados à navegação online, como o acesso a conteúdos inadequados; o contato com indivíduos mal-intencionados; a invasão de privacidade; e o roubo de identidade. Um dos erros mais comuns é acreditar que nossos dispositivos – seja computador, *smartphone* ou *tablet* – estão sempre protegidos contra ameaças virtuais, quando, na realidade, essa falsa sensação de segurança pode nos tornar ainda mais vulneráveis.

Em particular, as crianças e os adolescentes estão expostos a uma grande quantidade de informações, que podem ser úteis ou perigosas. Por isso, é fundamental que pais, responsáveis, professores e os próprios jovens estejam preparados para identificar desinformação e conteúdos prejudiciais que circulam na rede.

Ferrari, Machado e Ochs (2020) reforçam a importância de ensinar uma leitura crítica das informações

online, incentivando crianças e adolescentes a irem além do consumo passivo de conteúdo. É necessário desenvolver o pensamento crítico para que eles aprendam a questionar a origem e a veracidade do que encontram, com perguntas como: quem produziu essa informação? Quais evidências são apresentadas? Qual o propósito por trás da mensagem? Esse tipo de abordagem promove uma postura mais ativa e reflexiva no uso da internet.

Da mesma forma, a questão da confiabilidade das informações em ambientes digitais é fundamental. Dutra e Barbosa (2017) apontam alguns critérios que ajudam a avaliar a qualidade de uma informação, incluindo precisão, atualidade, fonte confiável e relevância. Esses princípios auxiliam os usuários a discernir entre informações úteis e conteúdos duvidosos.

Diante do apelo que a internet exerce sobre crianças e adolescentes, cabe aos pais, responsáveis e educadores adotar estratégias que, além de incentivar o pensamento crítico, também ensinem a navegar de forma segura no ambiente digital, de modo a combater a desinformação e promover uma experiência mais segura, responsável, autônoma e consciente.

PLANEJANDO O ENSINO

Ao refletirmos sobre este Volume 3, planejamos o ensino de forma a proporcionar às crianças e aos adolescentes – imersos na cultura digital – uma experiência de aprendizado mais dinâmica e relevante. O objetivo é que eles possam desenvolver suas próprias reflexões sobre a importância de conhecer e se resguardar dos perigos da internet, garantindo a segurança de seus dados e, conseqüentemente, sua proteção pessoal.

Conforme Almeida (2018), crianças e adolescentes de hoje possuem expectativas e necessidades bastante diferentes das gerações passadas, aguardando abordagens de ensino que integrem teoria e prática de maneira envolvente. Para atender a essas demandas, é essencial que os professores desenvolvam novas práticas pedagógicas e adotem estratégias metodológicas inovadoras.

Segundo a autora, a metodologia ativa não é uma novidade trazida pelas tecnologias digitais, mas sim um tema debatido há bastante tempo. Nas palavras de Almeida (2018, p. 17), essa metodologia “se caracteriza pela inter-relação entre educação, cultura, sociedade, política e escola, sendo desenvolvida por meio de métodos ativos e criativos, centrados na atividade do aluno com a intenção de propiciar a aprendizagem”.

Com base em Bacich e Moran (2018), desenvolvemos propostas de atividades fundamentadas em três abordagens de aprendizagem: ativa, compartilhada e tutorada. A aprendizagem ativa, segundo Bacich e

Moran (2018), é um processo contínuo e dinâmico. Neste volume, pensamos em atividades nas quais crianças e adolescentes se envolvem em experiências práticas, reflexivas e interessantes para sua realidade, relacionadas aos cuidados necessários para preservar sua privacidade ao utilizar a internet.

Com foco na experimentação, pesquisa e criação, este volume propõe tarefas que estimulam o engajamento direto dos estudantes na construção do conhecimento. Essas atividades são projetadas para enfrentar desafios concretos e complexos, permitindo que os alunos adquiram saberes relevantes em contextos pessoais, sociais e profissionais, especialmente no que se refere ao uso seguro da internet.

Ainda de acordo com Bacich e Moran (2018), a aprendizagem compartilhada valoriza a interação entre as pessoas, o que promove a troca de conhecimentos, experiências e perspectivas. Esse processo pode acontecer tanto em ambientes formais quanto informais, presencialmente ou por meio de tecnologias digitais, explorando os benefícios das redes sociais e da cooperação em grupo. Durante o desenvolvimento das atividades, cabe aos professores criarem oportunidades para a elaboração conjunta de soluções, produtos e ideias. Essa abordagem destaca a importância do trabalho em equipe, da cocriação e da empatia, favorecendo o desenvolvimento da participação na sociedade e fortalecendo a conexão com os desafios do mundo real.

Por fim, Bacich e Moran (2018) destaca que a aprendizagem por tutoria ocorre em um contexto de orientação personalizada e suporte direto de profissionais mais experientes. Esses profissionais

desempenham o papel de guias do conhecimento, auxiliando os estudantes a alcançar níveis mais elevados de compreensão e desenvolvimento. Nesse sentido, apresentamos estratégias que podem ser adaptadas, incentivam questionamentos e ampliam a visão de mundo, conectando aprendizagens individuais e colaborativas de maneira integrada e eficiente. Essas três abordagens, interligadas, têm o intuito de proporcionar uma experiência de aprendizagem rica, reflexiva e transformadora para crianças e adolescentes, principalmente no âmbito da educação digital.

MÃOS À OBRA

PROPOSTAS DE ATIVIDADES PARA NAVEGAÇÃO SEGURA NA WEB

A seguir, apresentamos algumas atividades que visam abordar com crianças e adolescentes questões relacionadas à privacidade e segurança na internet, orientando-os a navegar de forma responsável e proteger suas informações pessoais. Vale dizer ainda que algumas atividades podem atender a mais de uma faixa etária, pois tudo depende do nível de conhecimento do estudante, cabendo ao professor avaliar se é adequado à sua turma ou não.

1. Atividade envolvendo a importância da privacidade na internet

Objetivos	• Discutir a importância da privacidade e segurança na internet, por meio da análise crítica de situações cotidianas de exposição online; • Identificar os riscos associados à exposição de informações pessoais, aprendendo boas práticas para proteger os próprios dados; • Refletir, por meio de discussões, vídeos e dinâmicas interativas, sobre a segurança no uso de redes sociais e outras plataformas digitais, estimulando a construção de uma postura consciente e responsável no ambiente virtual.
Habilidades da BNCC	(EF12LP09), (EF35LP03) e (EF05LP15)
Níveis de ensino	Ensino Fundamental I e II
Materiais	Quebra-cabeça; laboratório de informática; projetor e computador para apresentação; pen drive.

Esta atividade tem como objetivo principal promover uma reflexão crítica sobre os riscos da exposição na internet, incentivando comportamentos mais seguros e conscientes no ambiente virtual.

Orientações/instruções para a realização da atividade

➡ **Passo 1: Agendamento e orientações**

Agende um horário no laboratório de informática, pois, para garantir o sucesso da atividade, é fundamental agendar o uso do laboratório com antecedência e preparar os estudantes a respeito das normas de conduta durante a aula. A seguir, estão algumas orientações elencadas como necessárias para a realização desta atividade.

Orientações:

- 1. Alimentos e bebidas:** é proibido levar água e lanches para o laboratório;
- 2. Equipamentos e fiação:** não é permitido mexer na fiação ou nos equipamentos;
- 3. Comportamento:** os alunos devem manter uma postura adequada, evitando correr, gritar ou agir de forma indisciplinada no laboratório;
- 4. Navegação:** é estritamente proibido acessar sites que não sejam relacionados à atividade proposta.

➡ **Passo 2: Motivação da aula**

Ao final das orientações, a aula poderá ser iniciada com um convite aos estudantes para participarem da discussão. Abaixo, seguem algumas sugestões para motivá-los à participação em sala.

Sugestões de perguntas para estimular a discussão:

1. O que vocês acham sobre postar fotos nas redes sociais?
2. Vocês sabiam que existe uma idade mínima para acessar as redes sociais?
3. Sabendo disso agora, o que vocês pensam sobre essa delimitação etária?
4. Será que é perigoso nossos pais ou responsáveis postarem nossas fotos em uma rede social?



Para saber mais, acesse:

Lei que proíbe o uso de redes sociais por menores de idade - RIC Notícias.



Após os questionamentos sobre uso de redes sociais, explique aos estudantes que a turma desenvolverá atividades relacionadas ao tema *privacidade e segurança na internet*. Para seguir a

lógica da motivação da participação nas aulas, pergunte a eles: “O que vocês sabem sobre privacidade e segurança na internet?”. “Vocês se sentem seguros ao navegar na internet? Por quê?”.

➡ Passo 3: Exibição de vídeo

Professor(a), os estudantes assistirão a um vídeo sobre privacidade online e, para que isso aconteça, preparamos algumas orientações. Veja:

Orientações:

1. Certifique-se de que a conexão com a internet esteja funcionando adequadamente e, sempre que possível, faça o *download* prévio do vídeo para evitar imprevistos.
2. Realize o *download* de forma segura, tomando as devidas precauções.
3. Antes de assistir ao vídeo, apresente a ficha técnica aos estudantes: quem produziu e onde foi disponibilizado. No decorrer do vídeo, algumas dicas de privacidade e segurança online são repassadas, conforme o próprio canal apresenta.
4. Peça a eles que assistam ao vídeo para compreenderem por que é importante prestar atenção naquilo que publicamos online e por qual motivo o ato de compartilhar informações envolve responsabilidade.
5. Abrir espaço para discussão, ouvindo as hipóteses dos estudantes.

A Figura 1, a seguir, mostra a capa do vídeo *Privacidade online para crianças - Proteção e segurança na internet para crianças*, produzido pelo canal *Smile and Learn - Português*.

**Para saber mais, acesse:**

Privacidade online para crianças - proteção e segurança na internet para crianças - Smile and Learn - Português.



Figura 1: Privacidade online

Fonte: Smile and Learn – Português (2023).

Após a exibição do vídeo, estimule a participação dos estudantes por meio dos questionamentos disponibilizados abaixo.

Sugestões de perguntas para estimular a discussão:

1. Qual é o conteúdo abordado no vídeo?
2. Davi estava em situação de risco? Se sim, por quê?
3. Quais são as lições que vocês puderam extrair do vídeo?

➡ Passo 4: Quebra-Cabeça Stop Online

Explique aos estudantes que eles participarão de um jogo chamado *Quebra-Cabeça Stop Online*. O objetivo do jogo é montar o quebra-cabeça o mais rápido possível e identificar a orientação correta da imagem para dizer “Stop”. Esse jogo serve para avaliar como os estudantes internalizaram o conteúdo da aula. Observe as instruções abaixo:

Atenção: Caso a escola não tenha internet, sugerimos a reprodução colorida dos quebra-cabeças, disponíveis no material WebGuardians. Recorte o material para que os estudantes possam montá-lo. Seguem, abaixo, os três links para acesso ao referido material.

Preparação:

Divida a turma em cinco grupos, garantindo que cada grupo tenha acesso a um quebra-cabeça online idêntico. Antes de iniciar a atividade, certifique-se de que todos os grupos tenham acesso ao mesmo quebra-cabeça para montar. Em seguida, solicite que eles cliquem em um dos links para ter acesso ao quebra-cabeça online:

Link 1: <https://www.jigsawplanet.com/?rc=play&pid=29084548674a>

Link 2: <https://www.jigsawplanet.com/?rc=play&pid=062e31d3bedc>

Link 3: <https://www.jigsawplanet.com/?rc=play&pid=2153365c0613>

A Figura 2, a seguir, mostra uma montagem bem sucedida do *Quebra-Cabeça Stop Online*, feita pelo link 1 fornecido anteriormente.

Figura 2: Montagem do Quebra-Cabeça Stop Online



**NÃO COMPARTILHE IMAGEM QUE REVELE O
ENDEREÇO DE SUA RESIDÊNCIA**



Fonte: WebGuardians (2023).

Partida:

Quando a partida começar, os grupos deverão montar seus quebra-cabeças online. À medida que as

peças forem encaixadas, os estudantes deverão ficar atentos à imagem que está se formando. Assim que um grupo achar que montou o quebra-cabeça corretamente e identificar a orientação correta da imagem, um membro do grupo deve falar “Stop” e parar de tocar no quebra-cabeça.

Verificação:

Quando um grupo falar “Stop”, todos os grupos devem interromper a montagem. O professor verificará o quebra-cabeça e a orientação da imagem do grupo que falou “Stop”. Se estiver correto, esse grupo ganha pontos.

Pontuação:

Cada grupo recebe pontos com base na precisão de sua montagem e orientação correta da imagem, ficando estabelecido o ranking de 1º, 2º, 3º e 4º lugares. O grupo com mais pontos finais é o vencedor.

O professor pode finalizar a atividade pedindo para que os estudantes façam uma avaliação da aula.

Passo 5: Avaliação

A avaliação será formativa e se fundamentará nos seguintes aspectos: comprometimento, participação e responsabilidade com os estudos da disciplina; cumprimento das atividades propostas; domínio dos conteúdos abordados; coerência e coesão nas argumentações; e discussões acerca do conteúdo estudado.

Procedimentos de avaliação: participação na discussão e na montagem do quebra-cabeça.

2. Atividade envolvendo senhas seguras e proteção de contas online

Objetivos	• Discutir a importância de criar senhas seguras e proteger contas online, refletindo sobre os critérios utilizados na elaboração de senhas e a necessidade de mantê-las protegidas; • Adotar boas práticas de segurança digital para prevenir acessos não autorizados e proteger suas informações pessoais em ambientes virtuais.
Habilidades da BNCC	(EF01LP16)
Níveis de ensino	Ensino Fundamental I
Materiais	Tinta guache; papéis ou cartões para a escrita das senhas criadas; uma sala de aula; uma caixa fechada com um cadeado.

Você, professor, pode iniciar a aula com a exposição de uma caixinha trancada por um cadeado. Dentro dela, haverá algumas adivinhações da literatura popular e brincadeiras folclóricas, porém, os estudantes não saberão o que há dentro da caixinha e, para descobrir, precisarão abrir o cadeado utilizando um chaveiro que tem diversas chaves.

Orientações/instruções para a realização da atividade

➡ **Passo 1: Jogo de adivinhação**

O professor explicará às crianças que, dentro da caixa, há seis adivinhações, e o grupo que mais acertar será o vencedor da brincadeira. Em seguida, ele pedirá que um representante de cada grupo retire um papel da caixa, leia a adivinhação para a turma e tente dar a

resposta. Caso não consiga, poderá passar a vez para os colegas do seu grupo. Se ninguém souber a resposta, qualquer outro grupo poderá responder e ganhar a pontuação correspondente.

Adivinhas:

O que é, o que é: posso ser pequeno, posso ser grande, mas sou essencial. Posso ter letras e números. Se outros souberem, sua vida virará um vendaval?

O que é, o que é: para muitos sou invisível, mas se clicar nos três pontinhos da tela do computador, verás o meu rastro. Quem sou eu?

O que é, o que é: às vezes posso estar vermelho, às vezes azul. Se não me possuírem, terão pesadelo?

O que é, o que é: posso ser o amigo que te guia por toda a rede, mas cuidado! Eu posso ver o que você não quer que ninguém veja. Quem sou eu?

Atenção: O professor poderá escolher outras adivinhações.

Passo 2: Contextualização da aula

Após a introdução situada no passo 1 desta proposta de atividade, o professor poderá prosseguir para a explicação das abordagens do dia: o estudo de senhas seguras e a proteção de contas online. Ele pode começar perguntando aos estudantes se sabem o que é uma senha e se já criaram alguma. Caso a resposta seja positiva, pode-se questionar o modo como os estudantes as criaram e por meio de quais critérios de criação.



Para saber mais, acesse:

Senhas: como proteger suas contas - Descomplicando a Tecnologia Online.



Autenticação de 2 fatores: como ativar - Descomplicando a Tecnologia Online.



Passo 3: Atividade Fortaleza de Senha

Neste momento, será desenvolvida a atividade *Fortaleza de Senha*. Ela envolve trabalho em equipe, pensamento estratégico e comunicação. O objetivo é promover a colaboração em grupo, a comunicação e a resolução de problemas. Seguem as orientações para realização da atividade mencionada.



Orientações:

1. Divida a sala de aula em três grupos. Cada grupo deve escolher um membro para ser o *Guardião da Senha* a cada rodada. O estudante escolhido como guardião será o único a ter as mãos e os pés sujos de tinta guache.
2. Forneça a cada grupo uma folha de papel ou cartão em branco para que escrevam a senha. A senha pode ser uma palavra, uma frase ou um código, dependendo do nível de dificuldade desejado.
3. O Guardião da Senha do primeiro grupo esconderá a senha escrita pelo grupo utilizando as mãos e os pés sujos de tinta guache. Ele deve escolher um local na sala de aula para esconder o papel com a senha, sem revelar a localização para os outros membros do grupo.
4. Após o primeiro grupo esconder sua senha, os outros dois grupos são autorizados a entrar na sala e começar a procurar. Eles podem usar observações, pistas deixadas acidentalmente pelo Guardião (manchas de tinta, pegadas etc.) e qualquer outro método para tentar encontrar a senha.
5. Cada grupo terá um tempo limite para encontrar a senha do primeiro grupo.
6. Quando o tempo acabar, o primeiro grupo revelará a localização da senha.
7. Após a revelação do local, os grupos trocarão de papel: o segundo grupo escolherá seu Guardião da Senha, esconderá sua senha e assim por diante. O processo será repetido até que cada grupo tenha escondido e procurado a senha.

Ao final, você pode contar quantas senhas cada grupo conseguiu encontrar com sucesso e finalizar a atividade pedindo para que os estudantes façam uma avaliação da aula.

➡ Passo 4: Avaliação

A avaliação será formativa e se fundamentará nos seguintes aspectos: comprometimento, participação e responsabilidade com os estudos da disciplina; cumprimento das atividades; domínio dos conteúdos abordados; coerência e coesão nas argumentações; e discussões acerca do conteúdo estudado.

Procedimentos de avaliação: será considerada a participação nas brincadeiras, as estratégias que os estudantes utilizaram para solucionar o problema e a avaliação que eles fizerem da aula.

3. Atividade sobre a privacidade e segurança online

Objetivos	Introduzir os conceitos de privacidade, segurança e proteção de dados, incentivando os estudantes a refletirem sobre a importância de proteger suas informações pessoais no ambiente digital.
Habilidades da BNCC	(EF02LP18), (EF35LP18) e (EF69LP38)
Níveis de ensino	Ensino Fundamental I e II
Materiais	Folha de rascunho; cartolina; pinceis; lápis de cor.

Esta atividade propõe discussões acerca da importância da privacidade e da segurança online. Para isso, o professor poderá explicar aos estudantes os riscos associados à divulgação de informações pessoais na internet e os métodos para proteger seus dados.

Orientações/instruções para a realização da atividade

Passo 1: Formação dos grupos

Divida a turma em grupos e atribua a cada grupo um dos tópicos abaixo:

1. Privacidade e segurança online;
2. Senhas seguras e proteção de contas online;
3. Internet segura: encontrando informações confiáveis;
3. Configurações de privacidade.

Neste momento, peça aos grupos que pesquisem informações confiáveis sobre seus tópicos. Escolha, junto aos estudantes, três turmas para as quais eles apresentarão o trabalho desenvolvido. Solicite que se preparem para apresentar a temática de forma clara e informativa para as turmas escolhidas.

Atenção: Caso a escola não tenha acesso à internet, solicite com antecedência que os estudantes realizem a pesquisa em casa e apresentem na aula seguinte.

Passo 2: Produção dos cartazes

Distribua o material para os grupos e peça que criem um rascunho antes de produzir os cartazes definitivos. Avalie os rascunhos, faça as considerações necessárias e autorize a confecção dos cartazes. Os cartazes devem conter dicas práticas e textos claros. Após a finalização, organize uma revisão para garantir que todas as informações estejam corretas e sejam relevantes.

➡ **Passo 3: Apresentação das produções**

Peça a cada grupo que apresente seu cartaz às turmas selecionadas anteriormente, explicando as informações e dicas contidas no material. Após as apresentações, os cartazes podem ser fixados no mural da escola, em um local de destaque, para que outros estudantes, professores e funcionários também tenham acesso às informações.

➡ **Passo 4: Avaliação**

A avaliação será formativa e se fundamentará nos seguintes aspectos: comprometimento, participação e responsabilidade com os estudos da disciplina; cumprimento das atividades; domínio dos conteúdos abordados; coerência e coesão nas argumentações; e discussões acerca do conteúdo estudado.

Procedimentos de avaliação: serão avaliadas as produções dos cartazes e a apresentação realizada por cada equipe.

4. Atividade envolvendo o impacto das tecnologias digitais na privacidade, segurança e identidade

Objetivos	Introduzir os conceitos de privacidade, segurança e proteção de dados, incentivando os estudantes a refletirem sobre a importância de proteger suas informações pessoais no ambiente digital.
Habilidades da BNCC	(EM13LGG702)
Níveis de ensino	Ensino Médio
Materiais	Cartolina ou folhas; canetas coloridas; quadro branco e marcadores para registrar as ideias.

Esta atividade introduz o trabalho com a temática referente à importância da privacidade, segurança e proteção de nossos dados. O professor pode começar a aula explicando que o intuito é dar início à discussão sobre os referidos temas no contexto da internet, ressaltando como são cada vez mais essenciais para o uso consciente e responsável das tecnologias digitais.

Orientações/instruções para a realização da atividade

Passo 1: Organização da sala

O professor organizará os estudantes em um semi-círculo (formato de U), criando um ambiente mais colaborativo, favorecendo o compartilhamento de ideias e experiências. Para que a participação seja estimulada, na sala de aula, o professor pode suscitar questões como: “Quem de vocês tem acesso a aparelhos celulares, computadores ou costuma navegar na internet?” e “Quantas horas por dia vocês passam usando celulares, computadores ou navegando na internet?”

Essas perguntas iniciais ajudarão a abrir espaço para a conversa e incentivarão os estudantes a compartilhar suas experiências cotidianas com o uso da tecnologia. O professor pode registrar as respostas no quadro para facilitar a visualização coletiva. Em seguida, pode-se introduzir o tema principal da aula.

Passo 2: Discussão em grupo

Pelas respostas dos estudantes, o professor pode conduzir uma discussão com a seguinte provocação (professor, fique à vontade para adaptá-la. Lembre-se que se trata apenas de uma sugestão): “Agora, pensem por um

momento: enquanto vocês navegam na internet, baixam aplicativos ou usam redes sociais, já pararam para pensar o que acontece com os dados que vocês compartilham? Será que estamos realmente seguros online?”.

O objetivo do questionamento é criar um momento de reflexão, no qual os estudantes possam pensar criticamente sobre o uso da internet. A ideia é que consigam entender que, mesmo sem perceber, ao navegar pela rede, estamos constantemente deixando informações pessoais, que podem ser usadas por terceiros de maneiras que nem sempre compreendemos ou aprovamos.

Passo 3: Atividade em grupo

Organize a turma em pequenos grupos de 3 a 5 estudantes para promover a interação e a troca de ideias. Cada grupo receberá uma cartolina ou folha grande e canetas coloridas. Os grupos terão 10 minutos para discutir e escrever suas ideias sobre “O que é privacidade digital?” e “O que é segurança digital?”. Os estudantes poderão anotar palavras-chave, frases ou até fazer desenhos que representem o que entendem sobre esses conceitos.

Sugestões de perguntas para estimular a discussão:

1. O que vocês acham que significa privacidade quando estão usando a internet?
2. Quais informações vocês acham que precisam ser mantidas em segredo ou protegidas online?
3. Vocês se sentem seguros quando navegam na internet? O que acham que é segurança digital?

4. O que pode acontecer se alguém violar sua privacidade digital?

Observação: Deixe claro que, nesta etapa, não há respostas certas ou erradas – o objetivo é que os alunos expressem suas percepções de forma livre.

➡ **Passo 4: Apresentação dos grupos**

Após os 10 minutos de discussão, cada grupo deverá apresentar suas ideias para o restante da turma. Os estudantes podem explicar o que anotaram e as razões pelas quais associaram essas ideias aos conceitos de privacidade e segurança digital.

➡ **Passo 5: Síntese coletiva**

O professor fará uma síntese das ideias apresentadas, relacionando-as aos conceitos formais de privacidade e segurança digital. Verifique tais conceitos no quadro abaixo:

Conceitos

Privacidade digital: é a capacidade de controlar o acesso às suas informações pessoais *online* e decidir o que compartilhar, quando e com quem.

Segurança digital: é a proteção dos seus dados e informações contra roubos, fraudes ou acessos não autorizados, garantindo que seus dados pessoais estejam seguros na internet.

Recado importante: Professor, sinta-se à vontade para adaptar esta atividade conforme o perfil da sua turma e as suas estratégias de ensino. A proposta é que você explore a sua criatividade e utilize os recursos que considerar mais adequados para promover o aprendizado dos estudantes. Uma possibilidade é a criação de um cartaz para ilustrar a temática e torná-la ainda mais interessante. Um visual atrativo pode despertar a curiosidade dos estudantes e facilitar tanto a compreensão quanto a participação na atividade.

Sugestões de perguntas para estimular a discussão:

1. Quando você posta uma foto nas redes sociais, quem pode vê-la? E se essa foto for compartilhada sem sua permissão?
2. Quando você aceita os termos de um aplicativo, sabe quais dados ele pode acessar?

Passo 6: Reflexão final

Para encerrar a temática abordada na aula, o professor pode perguntar aos estudantes: “Agora que discutimos esses temas, vocês acreditam que estão protegendo adequadamente a sua privacidade e a sua segurança digital? O que poderiam fazer de diferente?”.

Passo 7: Avaliação

A avaliação pode ser feita com base na participação dos estudantes nos grupos, na qualidade das discussões e nas ideias apresentadas. O professor poderá, também, solicitar que cada estudante escreva um pequeno texto individual e o traga na próxima aula,

**Material necessário:**

Atividade produção de texto.

QR Code da atividade para o professor imprimir:



respondendo à seguinte questão: “Como você pode melhorar a proteção da sua privacidade e segurança digital no dia a dia?”

O professor pode orientar os estudantes a fazerem uma pesquisa na internet ou a assistirem a vídeos no YouTube.

5. Atividade de bate-papo sobre o impacto das tecnologias digitais na privacidade, segurança e identidade

Objetivos	Discutir a importância da privacidade e da segurança na internet, abordando os riscos e desafios associados à exposição de dados pessoais, além de apresentar boas práticas que auxiliem na proteção dessas informações.
Habilidades da BNCC	(EM13LGG702)
Níveis de ensino	Ensino Fundamental I e II
Materiais	Projeto e computador para apresentação; materiais para anotações (papel, canetas); acesso à internet (opcional, se for necessário para atividades práticas).

Esta atividade consiste em um bate-papo entre os estudantes e um especialista da área de tecnologia. O especialista discutirá a importância da privacidade e da

segurança na internet, abordando os riscos e os desafios associados à exposição de dados pessoais. Além disso, ele precisa apresentar boas práticas que contribuam para a proteção dessas informações.

Orientações/instruções para a realização da atividade

Passo 1: Preparação

Professor, para enriquecer o bate-papo sobre segurança na internet para crianças e adolescentes, podemos convidar diversos profissionais com domínio na área. Algumas opções interessantes incluem:

- **Bacharel em Direito:** especialistas em proteção de dados e privacidade, com foco na legislação que protege crianças e adolescentes;
- **Conselheiro Tutelar:** profissionais com experiência em lidar com casos de violação de direitos de crianças e adolescentes no ambiente online;
- **Professor com doutorado, mestrado ou especialização:** especialistas em educação digital e segurança da informação, com disponibilidade para apresentar o conteúdo de forma clara e didática;
- **Policial:** profissionais que atuam diretamente na prevenção e no combate a crimes cibernéticos envolvendo crianças e adolescentes;

- **Promotor de justiça:** especialistas em direito da criança e do adolescente, com experiência em casos relacionados ao uso da internet.

Observação: para organizar o espaço do bate-papo com o especialista em tecnologia, o professor deve selecionar uma sala ampla, capaz de acomodar todos os estudantes, com cadeiras dispostas em formato de círculo ou semicírculo, facilitando a interação. É importante verificar a disponibilidade de recursos tecnológicos, como projetor e acesso à internet, agendando-os previamente. Além disso, o ambiente deve ser mantido livre de distrações, garantindo que os estudantes possam se concentrar na discussão. O professor também deve confirmar a presença do especialista e agendar a sala de aula com antecedência. Por fim, criar um clima acolhedor, com cartazes sobre privacidade e segurança na internet, pode estimular o interesse dos estudantes e enriquecer a experiência do bate-papo.

Passo 2: Contextualização do bate-papo

Apresentar brevemente o tema da aula e contextualizar a importância de discutir a privacidade na internet, citando exemplos práticos, como o uso de redes sociais, compras online, aplicativos de mensagens, entre outros. Em seguida, o professor apresenta o especialista convidado, mencionando sua formação e experiência na área e, por fim, passa a palavra para o especialista.

Passo 3: Explicação da temática

O especialista, ao longo de sua apresentação, pode abordar os seguintes pontos:

- O que é privacidade na internet;
- Principais riscos do uso inadequado de dados pessoais;
- Desafios enfrentados na proteção da privacidade online;
- Casos reais de violações de privacidade e suas consequências;
- Boas práticas para manter a privacidade online: senhas seguras, autenticação em duas etapas, uso consciente de redes sociais, entre outros.

Passo 4: Perguntas e Respostas

Após a fala do especialista, os estudantes terão a oportunidade de interagir com o convidado, fazendo perguntas sobre privacidade e segurança online. O professor pode mediar o diálogo, garantindo que as dúvidas mais relevantes sobre o tema sejam esclarecidas.

Passo 5: Reflexão final

O professor pode encerrar a atividade com uma reflexão sobre a importância de aplicar, no cotidiano dos alunos, as práticas discutidas, ressaltando o impacto dessas ações na segurança e na privacidade dos dados pessoais.

Passo 6: Avaliação

A avaliação será formativa e se fundamentará nos seguintes aspectos: comprometimento, participação e responsabilidade com os estudos da disciplina; cumprimento das atividades; domínio dos conteúdos abordados; coerência e coesão nas argumentações; e discussões acerca do conteúdo estudado.

6. Atividade sobre pesquisa da nossa relação com a internet

Objetivos	Discutir os hábitos e comportamentos dos estudantes em relação ao uso da internet, identificando semelhanças e diferenças entre os níveis dos alunos do Ensino Fundamental e do Ensino Médio.
Habilidades da BNCC	(EM13MAT102), (EF89LP25) e (EM13LGG704)
Níveis de ensino	Ensino Fundamental II e Ensino Médio
Materiais	Projeto e computador para apresentação; plataforma <i>Google Forms</i>; cópias com o formulário das perguntas do <i>Google Forms</i>. 

Professor, nesta atividade, os estudantes do Ensino Médio serão conduzidos ao laboratório de informática para responder a uma pesquisa sobre seus hábitos e comportamentos na internet.

Orientações/instruções para a realização da atividade

➡ Passo 1: Agendamento e orientação

Para garantir o sucesso da atividade, é fundamental agendar o uso do laboratório de informática com antecedência, além de orientar os estudantes quanto às normas

de conduta durante a aula. A seguir, você encontrará o destaque de algumas orientações a serem comunicadas.

Orientações:

Alimentos e bebidas: é proibido levar água e lanches para o laboratório;

Equipamentos e fiação: não é permitido mexer na fiação ou nos equipamentos;

Comportamento: os alunos devem manter uma postura adequada, evitando correr, gritar ou agir de forma indisciplinada no laboratório;

Navegação: é estritamente proibido acessar sites que não sejam relacionados à atividade proposta.

➡ Passo 2: Definição de amostragem

Explique aos estudantes o conceito de amostragem em uma pesquisa e como essa técnica pode ser utilizada para coletar dados de alunos do 6º ao 9º ano do Ensino Fundamental. Com base no formulário elaborado, os dados deverão ser organizados em formas de gráficos, tabelas e apresentação em slides, demonstrando e analisando os resultados entre os diferentes níveis de ensino para entender melhor como a internet é utilizada por esses estudantes.

**Para saber mais, acesse:**

População e Amostra -
Introdução à Estatística.



Passo 3: Apresentação dos resultados

De posse dos slides, o professor apresentará e discutirá os resultados com os estudantes do Ensino Médio. Em seguida, os próprios estudantes se organizarão para apresentar os resultados aos alunos do 6º ao 9º ano do Ensino Fundamental.

Passo 4: Avaliação

A avaliação será formativa e se fundamentará nos seguintes aspectos: comprometimento, participação e responsabilidade com os estudos da disciplina; cumprimento das atividades; domínio dos conteúdos abordados; coerência e coesão nas argumentações; e discussões acerca do conteúdo estudado.

Procedimentos de avaliação: preenchimento do formulário no laboratório de informática e realização de pesquisa com os estudantes dos Anos Finais do Ensino Fundamental.

INTEGRAÇÃO DO TEMA COM OUTRAS DISCIPLINAS

Professor(as), que tal aprofundar o tema deste volume e integrar a questão da segurança digital com outras disciplinas, como Língua Portuguesa, Ciências, Matemática e Educação Física, para que os alunos compreendam o assunto de maneira ampla e aplicada a diferentes contextos? Para este volume, sugerimos os temas a seguir.

PROJETO 1

Reconto: quem conta um ponto aumenta caracteres

O professor pode propor um projeto de reconto de contos de fadas ou outras histórias, incentivando os estudantes a adaptarem os enredos para o contexto contemporâneo, especialmente envolvendo e alertando para os perigos da internet. O objetivo desse projeto é possibilitar que os alunos explorem temas como segurança digital, privacidade online, *cyberbullying* e outros desafios do ambiente virtual, mediante narrativas já familiares.

Ao recontar narrativas como *Branca de Neve*, *Chapeuzinho Vermelho* ou outras fábulas, os estudantes podem recriar personagens e tramas, inserindo elementos como golpes digitais, exposição indevida de dados pessoais, *haters*, *fake news* e a exploração de vulnerabilidades nas redes sociais. por meio dessa abordagem, as histórias ganham uma nova perspectiva, conectando o

mundo fantasioso dos contos de fadas à realidade tecnológica vivida por crianças e adolescentes diariamente.

Por exemplo, um estudante pode transformar a história da Branca de Neve em um conto que aborda situações como a exposição de fotos sem permissão por parte de sua madrasta, ou o momento em que a personagem cai em um golpe ao clicar em um *link* malicioso. Dessa forma, os estudantes desenvolvem habilidades de escrita criativa enquanto refletem criticamente sobre os riscos que a internet apresenta.

Além disso, o projeto pode culminar em uma apresentação, na qual crianças e adolescentes compartilham seus recontos e promovem discussões sobre as melhores práticas para uma navegação segura na internet, promovendo o aprendizado colaborativo e a conscientização digital. Essa proposta permite ao professor abordar o tema da segurança digital de forma integrada aos componentes curriculares de Língua Portuguesa, Tecnologia e Cidadania, estimulando o desenvolvimento de habilidades como leitura crítica, produção textual e empatia.

PROJETO 2

Metaverso do tempo: deixando nossas pegadas

O projeto *Metaverso do tempo: deixando nossas pegadas* propõe que os estudantes, com o apoio do professor, construam um metaverso interativo que funcione como uma linha do tempo, destacando a evolução das tecnologias digitais, emergentes e generativas. A proposta também explora como, ao longo dos anos, as pessoas deixam pegadas digitais – dados pessoais valiosos que são utilizados por empresas e instituições.

Integrando as disciplinas de História, Ciências e Geografia, os estudantes investigarão o avanço tecnológico, desde o surgimento da internet até as tecnologias atuais, refletindo sobre a coleta e o uso de dados digitais. A linha do tempo virtual representará marcos importantes das tecnologias e mostrará como essas inovações impactaram a sociedade ao longo do tempo. Além disso, o projeto promove uma reflexão crítica sobre privacidade e segurança online, incentivando crianças e adolescentes a adotarem um uso consciente da tecnologia e a refletirem sobre o impacto de suas pegadas digitais.

PROJETO 3

Proteção digital e família: garantindo a segurança online de crianças e adolescentes

Este projeto, *Proteção digital e família: garantindo a segurança online de crianças e adolescentes*, propõe o trabalho em conjunto com a família: pais ou responsáveis. Será um momento para discutir com eles a importância da privacidade e segurança na internet, especialmente em relação aos dados pessoais de seus filhos. A oficina poderá ser desenvolvida pela escola, que convidará as famílias para participarem de uma sessão interativa, na qual serão abordados os principais riscos digitais que crianças e adolescentes enfrentam ao navegar na internet.

Além de discutir o quanto os dados dos jovens estão expostos na rede, o projeto visa ensinar os responsáveis a configurarem tanto os seus dispositivos quanto os de seus filhos, para reforçar a privacidade e evitar que os dados pessoais sejam utilizados indevidamente para fins comerciais ou outros objetivos prejudiciais.

Durante a oficina, pais e responsáveis serão orientados sobre como os dados podem ser coletados por meio de aplicativos, redes sociais e sites – muitas vezes sem que os usuários tenham plena consciência disso. Serão apresentadas estratégias simples e práticas para aumentar a segurança digital, como ativar controles de privacidade, limitar o compartilhamento de informações pessoais e evitar a exposição desnecessária de dados sensíveis. Os participantes também aprenderão a configurar as permissões dos aplicativos, criar senhas seguras, ativar a autenticação em dois fatores e utilizar ferramentas de monitoramento, com o intuito de proteger melhor as informações no ambiente online.

CONECTANDO SABERES

COMPARTILHAMENTO DE CONHECIMENTOS E BOAS PRÁTICAS

Você, professor, está convidado a participar ativamente da rede WebGuardians, colaborando com seus conhecimentos, suas experiências e boas práticas por meio do *Hub de Educação Digital* – uma plataforma criada pela Universidade Estadual de Montes Claros (Unimontes). O Hub foi desenvolvido para facilitar o intercâmbio de ideias e recursos pedagógicos entre educadores, promovendo um ambiente colaborativo que valoriza o ensino e o aprendizado digital.

No Hub, você poderá compartilhar suas práticas pedagógicas inovadoras, materiais complementares, vídeos tutoriais, jogos interativos e outras ferramentas que enriquecem suas aulas. Ao participar, além de contribuir para que outros educadores aprimorem suas metodologias, você também se beneficiará das soluções e abordagens compartilhadas por outros colegas.

Para facilitar seu acesso, disponibilizamos um QR Code, que o levarão diretamente ao *Hub de Educação Digital* da Unimontes. Lá, será possível registrar suas experiências e colaborar com uma rede de educadores que, assim como você, estão

**QR Code para acesso ao
Hub de Educação Digital**



Fonte: WebGuardians (2024).

comprometidos com o uso consciente e inovador das tecnologias digitais no ambiente educacional.

Os itens compartilhados e aprovados por uma equipe de especialistas serão disponibilizados no repositório do Hub. Essa iniciativa tem o intuito de promover uma cultura de troca de saberes, estimulando a colaboração e a inovação entre professores. Ao compartilhar suas experiências e práticas pedagógicas, você contribuirá para o desenvolvimento de uma educação digital mais inclusiva e colaborativa, alinhada às demandas do mundo contemporâneo. Junte-se à rede e ajude a transformar o aprendizado digital para seus alunos e colegas!

Professores(as), compartilhem seus conhecimentos, suas experiências e suas atividades na rede do *WebGuardians*, por meio da *Plataforma Digital WebGuardians*. Esse espaço foi criado especialmente para o compartilhamento de materiais complementares, vídeos tutoriais, jogos interativos, fórum e, principalmente, troca de experiências entre educadores. A proposta é promover formas de conexão entre educadores e divulgar práticas pedagógicas a respeito do uso consciente da internet. Compartilhem conosco suas experiências! Temos certeza de que podemos aprender muito com vocês!

MAIS INFORMAÇÕES

Esta seção apresenta uma lista de referências que permite ao professor aprofundar seus conhecimentos sobre o tema estudado. Seleccionamos materiais que enriquecem a compreensão e contribuem para o planejamento e a formação docente.

FUNDAÇÃO GETÚLIO VARGAS. *Guia de Proteção de Dados Pessoais – Crianças e Adolescentes Versão 1.0* - Outubro, 2020. E-book. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/751d0a-33-70f7-46ba-8626-625a9fb8536e/content>. Acesso em: 30 set. 2024.



NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. *Privacidade e proteção de dados pessoais 2021 [livro eletrônico]*: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 01 out. 2024.



TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. *Proteção de Dados de Crianças e Adolescentes Cenário Brasileiro e Experiências Internacionais*. Instituto de Tecnologia e Sociedade do Rio, 2021. E-book. Disponível em: <https://itsrio.org/wp-content/uploads/2021/08/Relatorio-Boas-Praticas-Crianças-e-Adolescentes.pdf>. Acesso em: 01 out. 2024.



CANAIS E VÍDEOS NO YOUTUBE QUE VOCÊ PODE ACESSAR:

Nesta parte do Volume 3, sugerimos alguns vídeos no YouTube que abordam, de forma dinâmica e acessível, temas como a importância da privacidade na internet, o que compartilhar (ou não), senhas seguras e a proteção de contas online. Esses materiais auxiliam no entendimento de conceitos complexos e na visualização de exemplos práticos.

Smile and Learn - Português. *O que é a netiqueta?* Normas de comportamento na internet para crianças Compilação. Youtube, 14 jun. 2022. Disponível em: https://www.youtube.com/watch?v=SOY-je0K_92g. Acesso em: 29 set. 2024.



Smile and Learn - Português. *O que são as fake news?* - Dicas para reconhecê-las - *Fake news* para crianças. Youtube, 14 jun. 2022. Disponível em: <https://www.youtube.com/watch?v=xRWcW0RtYjY>. Acesso em: 29 set. 2024.



PARA EXPLORAR MAIS

Desenvolvemos esta seção com sugestões de atividades complementares relacionadas à segurança e à privacidade na internet. As propostas abordam aspectos fundamentais, como a importância de proteger informações pessoais, a conscientização sobre o que deve ou não compartilhar nas redes e práticas para manter senhas seguras e contas online protegidas.

Guia Geração Digital Adolescentes Seguros na Internet é um material criado por um projeto com o objetivo de gerar e compartilhar conhecimentos sobre o uso seguro da Internet. O material pode ser acessado pelo link: https://eprofessor.com.br/pluginfile.php/87/mod_glossary/attachment/5/e-book_google%20seguran%C3%A7a%20digital%20-%20atividades.pdf

Ou pelo QR Code:



Outro material é a cartilha produzida pela Safernet Brasil, que ensina como *Brincar, estudar e... navegar com segurança na Internet!* Acesse a cartilha pelo link: https://new.safernet.org.br/sites/default/files/content_files/cartilha-saferdicas.pdf

Ou escaneie o QR Code para acessar diretamente:



REFERÊNCIAS

ALMEIDA, M. E. B. Apresentação. In: BACICH, L.; MORAN J.(Org.). *Metodologias ativas para uma educação inovadora: uma abordagem teórico-prática* [recurso eletrônico]. Porto Alegre: Penso, 2018.

ANGELINI, K.; BARBOSA, A.; SENNE, F.; DINO, L. A. Privacidade e proteção aos dados pessoais de crianças e adolescentes na Internet: marco legal e ações estratégicas para prover direitos na era digital. In: LATERÇA, P. S.; FERNANDES, E.; TEFFÉ, C. S. D.; BRANCO, S. (coords.). *Privacidade e proteção de dados de crianças e adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS); Obliq, 2021, p. 15-28.

BACICH, L.; MORAN J. (Org.). *Metodologias ativas para uma educação inovadora: uma abordagem teórico-prática* [recurso eletrônico]. Porto Alegre: Penso, 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Lei nº 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 29 set. 2024.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 set. 2024.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos. *Lei nº 12.965, de 23 de abril de 2018*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 set. 2024.

BRASIL. Ministério da Educação. Secretaria da Educação Básica. *Base nacional comum curricular*. Brasília, DF, 2018.

CERT - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. *Cartilha de Segurança para Internet*, versão 4.0 / CERT. br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 17 ago. 2023.

DIAS, V. C.; LIMA, N. L.; VIOLA, D. T. D.; KELLES, N. F.; GOMES, P. S.; SILVA, C. R. Adolescentes na Rede: Riscos ou ritos de passagem? *Psicologia: Ciência e Profissão*, 39, 1-15. 2019. Disponível em: <https://doi.org/10.1590/1982-3703003179048>. Acesso em: 14 ago 2025.

DUTRA, F. G.; BARBOSA, R. R. Modelos e critérios para avaliação da qualidade de fontes de informação: uma revisão sistemática de literatura. *Informação & Sociedade: Estudos*. João Pessoa, v. 27, n. 2, p. 19-33, maio/ago. 2017.

FERRARI, A. C.; MACHADO, D.; OCHS, M. *Guia da Educação Midiática*. 1. ed. São Paulo: Instituto Palavra Aberta, 2020. Disponível em: [https://educamidia.org.br/api/wp-content/uploads/2021/03/Guia-da-Educac%C3%A7%C3%A7o-Midia%CC%81tica-Single.pdf](https://educamidia.org.br/api/wp-content/uploads/2021/03/Guia-da-Educac%C3%A7%C3%A7%C3%A7o-Midia%CC%81tica-Single.pdf). Acesso em: 19 ago. 2023.

GALEGALE, N. V. FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. *Perspectivas em Ciência da Informação*, v. 22, n. 3, p.75-97, jul./set. 2017.

LATERÇA, P. S.; FERNANDES, E.; TEFFÉ, C. S.; BRANCO, S. (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021.

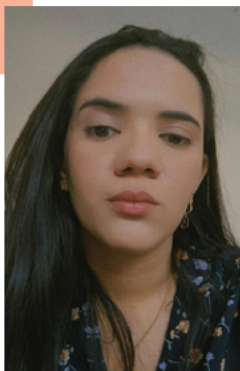
MITNICK, K. D.; SIMON, W. L. *A arte de enganar*: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.

NIC.BR. - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. *TIC Kids Online Brasil 2023*: principais resultados. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://cetic.br/pt/pesquisa/kids-online/>. Acesso em 29 set. 2024.

PEDRO, K. M.; CHACON, M. C. M. *Informativo sobre competências digitais e segurança na internet*: orientações para pais, professores e estudantes. Cartilha (informativo) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista- Unesp, 2016. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/148563/pedro_km_oe_mar.pdf?sequence=1&i-sAllowed=y. Acesso em 28 de agosto de 2023.

PRENSKY, M. Digital Native, digital immigrants. Digital Native immigrants. On the horizon, *MCB University Press*, v. 9, n. 5, 2001. Disponível em: [https://marcprensky.com/writing/Prensky%20 %20Digital%20 Natives,%20Digital%20Immigrants%20-%20Part1.pdf](https://marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf). Acesso em: 17 ago. 2023.

SÂRTS, J. Protegendo os nativos digitais! In: 5RIGHTS FOUNDATION. *O Futuro da infância no mundo digital*: ensaios sobre liberdade, segurança e privacidade. São Paulo: Instituto Alana, 2021.

**Mirelle Pereira da Silva**

<http://lattes.cnpq.br/0601959249867123>

Graduada em Pedagogia pela Universidade Estadual de Montes Claros (2018). Graduada em Licenciatura em Matemática pelo Instituto Federal do Norte de Minas Gerais Campus Januária (2022). Pós-Graduada em Educação Matemática (Especialização) e em Inspeção Escolar (Especialização). Atualmente é Analista Educacional-Inspetora Escolar na rede Estadual de Minas Gerais. Estuda formação de professores, conhecimentos dos professores que ensinam Matemática, e investiga o processo de ensino e aprendizagem em Matemática.

**Claudia Regina Costa Braga Rodrigues**

<http://lattes.cnpq.br/7140743460400503>

Bacharel em Engenharia e Licenciada em Informática, Pós-Graduada em Robótica Educacional (Especialização). Atualmente, é professora de Educação Básica no SESI, em que trabalha com alunos da rede municipal da cidade de Salinas- MG. Desenvolve e ministra oficinas e minicursos de robótica, promovendo o aprendizado prático e a inovação tecnológica no ambiente escolar. Com uma abordagem dinâmica, busca incentivar o pensamento crítico, a criatividade e o protagonismo dos estudantes por meio da robótica educacional.

WEB GUARDIANS

NAVEGANDO COM SEGURANÇA NA INTERNET

