



# CIDADÃO DIGITAL

CADERNO DE FORMAÇÃO  
PARA EDUCADORES

2021



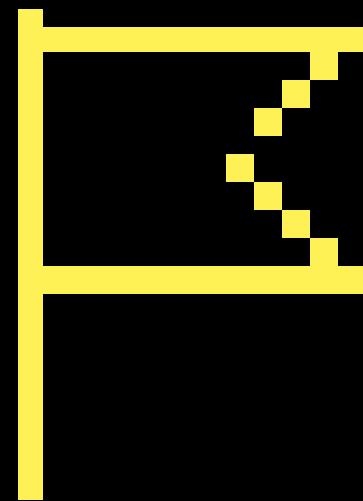
## ÍNDICE

<b>1</b>	<b>INTRODUÇÃO</b>	<b>02</b>	Criptografia Ponto a Ponto	<b>27</b>	Ferramentas	<b>57</b>		
	Carta ao Educador	<b>03</b>	Desafios Jurídicos no Brasil	<b>29</b>	Atividades sugeridas	<b>58</b>		
	Sobre o Programa Cidadão digital	<b>04</b>	Direitos Humanos e serviços essenciais	<b>30</b>	<b>6</b>	<b>EDUCAÇÃO MIDIÁTICA</b>	<b>60</b>	
	Sobre a Safernet	<b>06</b>	Como ativar a Criptografia	<b>31</b>	Contexto	<b>62</b>		
	Sobre a Formação	<b>07</b>	Sugestão de Atividades	<b>32</b>	Desordem Informacional	<b>63</b>		
	Temas	<b>08</b>	<b>4</b>	<b>COMPORTAMENTOS POSITIVOS</b>	<b>33</b>	Análise Crítica de Mídias	<b>66</b>	
	Base Nacional Comum Curricular: BNCC	<b>09</b>	Contexto	<b>35</b>	Checagem de Fatos	<b>70</b>		
	Como ler este caderno	<b>10</b>	Respeito e Empatia	<b>37</b>	Responsabilidade das Plataformas	<b>71</b>		
<b>2</b>	<b>PRIVACIDADE E REPUTAÇÃO</b>	<b>11</b>	Ferramentas	<b>43</b>	Ferramentas	<b>72</b>		
	Contexto	<b>13</b>	Sugestão de Atividades	<b>44</b>	Atividades Sugeridas	<b>74</b>		
	Privacidade, Dados Pessoais e Reputação	<b>14</b>	<b>5</b>	<b>AUTOCUIDADO ONLINE</b>	<b>48</b>	<b>7</b>	<b>AÇÕES INSPIRADORAS</b>	<b>76</b>
	Ferramentas Práticas	<b>16</b>	Contexto	<b>50</b>	Contexto	<b>78</b>		
	Sugestão de Atividades	<b>18</b>	Leis e Diretrizes	<b>53</b>	Projetos Inspiradores	<b>80</b>		
<b>3</b>	<b>CRIPTOGRAFIA</b>	<b>21</b>	Saúde Mental e Covid	<b>54</b>	Sugestão de Atividades	<b>81</b>		
	Contexto	<b>23</b>	Campanhas de Autocuidado	<b>55</b>	<b>8</b>	<b>CRÉDITOS</b>	<b>82</b>	
	Criptografia no Transporte de Dados	<b>26</b>	Campanhas sobre Autoviolência	<b>56</b>				



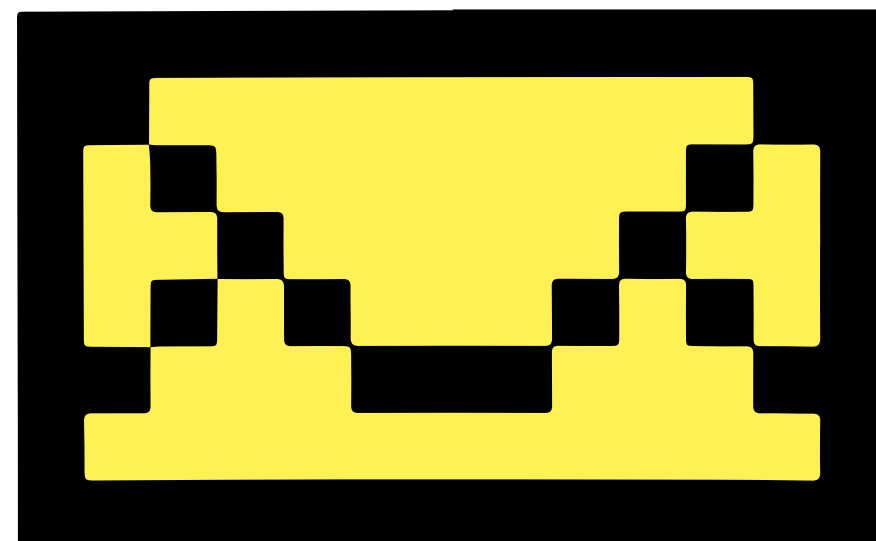
CAPÍTULO

1



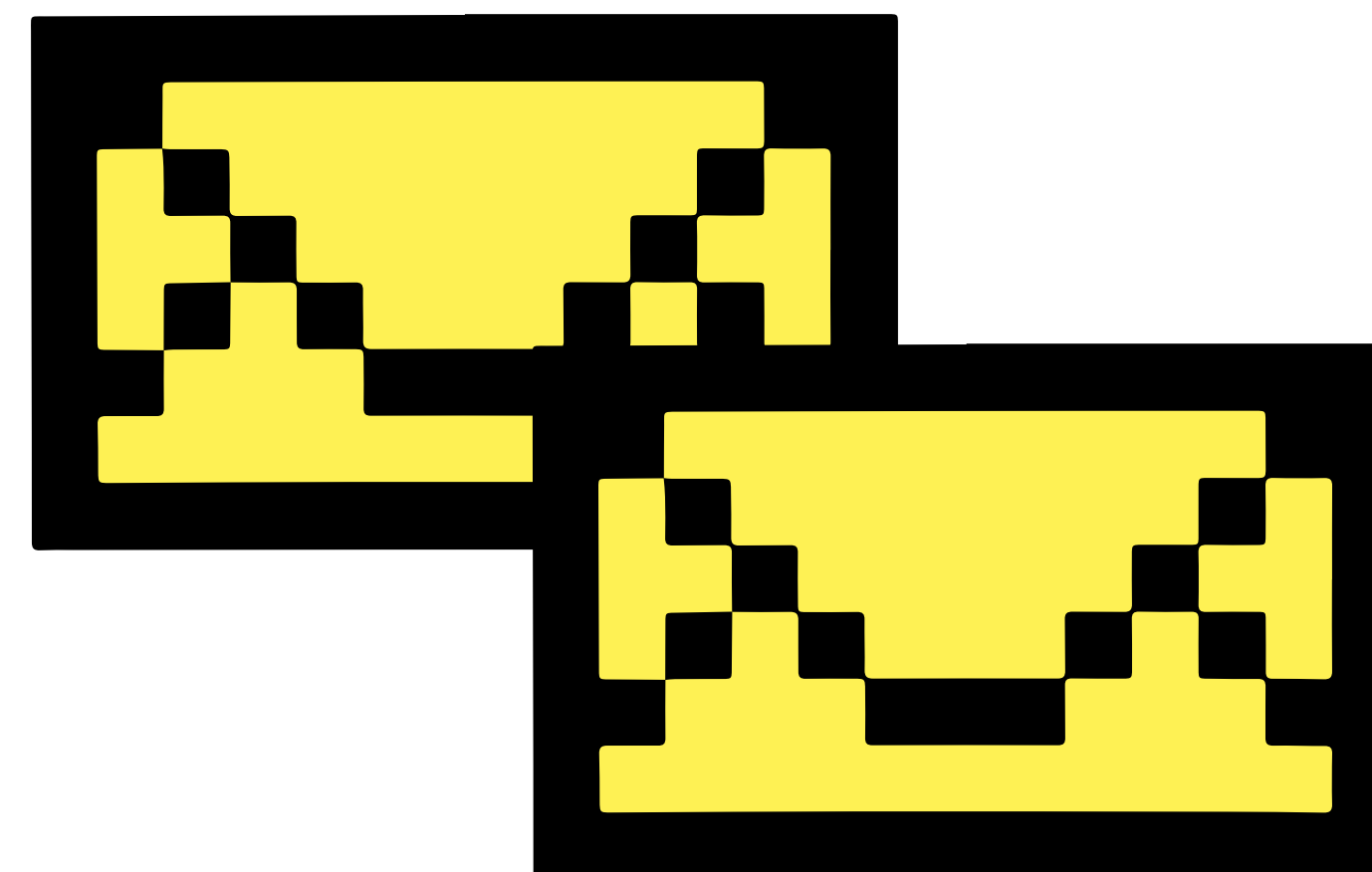
# INTRODUÇÃO

# CARTA AO EDUCADOR



Em 2020, a Safernet Brasil e o Facebook lançaram o Cidadão Digital, programa para a formação de jovens embaixadores e a promoção de ações de educação digital com foco em alunos da rede pública de todo o país.

Este caderno que você está lendo agora é uma versão adaptada e publicada em 2021 da formação online de 25 horas para educadores que lançamos no projeto, no qual trazemos conteúdos e recursos que ajudam você a ampliar seus conhecimentos sobre segurança, bem-estar e cidadania no contexto digital.



# 1.2 SOBRE O PROGRAMA

# CIDADÃO DIGITAL

É um programa gratuito de formação de jovens mobilizadoras/es em temáticas de segurança, educação midiática e cidadania digital, e também de promoção de ações educativas sobre os temas junto a educadores da rede pública de ensino e adolescentes de 13 a 17 anos de todo o país.

A iniciativa é uma parceria da SaferNet Brasil e do Facebook e impactou em sua primeira edição, em 2020, mais de:

	&	
<b>97 MIL</b>		<b>61 MIL</b>
<b>ADOLESCENTES E JOVENS</b>		<b>EDUCADORES</b>

Confira dados atualizados em [cidadaodigital.org.br](http://cidadaodigital.org.br)

VIDEO



# 1.2 PÚBLICOS

SAIBA MAIS



VOCÊ PODE CONFERIR MAIS DETALHES SOBRE OS IMPACTOS DO PROGRAMA ACESSANDO [WWW.CIDADAODIGITAL.ORG.BR](http://WWW.CIDADAODIGITAL.ORG.BR)

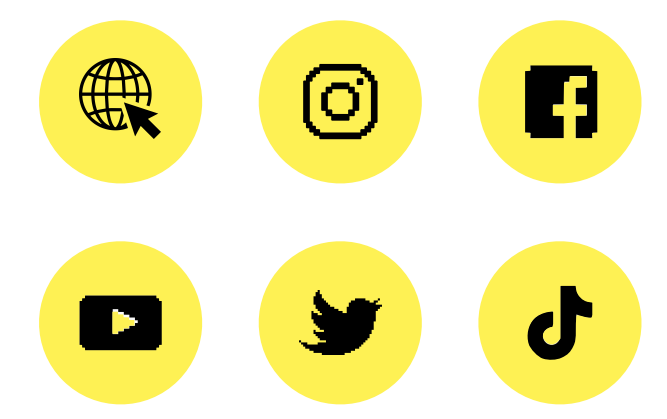
PÚBLICOS DO CIDADÃO DIGITAL	PODE PARTICIPAR DA FORMAÇÃO?	PODE SE INSCREVER PARA RECEBER ATIVIDADES?	PODE PARTICIPAR DAS ATIVIDADES?	TEM ACESSO AOS CONTEÚDOS DOS PROGRAMAS?
ADOLESCENTES DE 15-17 ANOS	NÃO, MAS TENHA CERTEZA QUE VOCÊ VAI APRENDER MUITO NAS ATIVIDADES	NÃO, MAS VOCÊ PODE PEDIR PARA QUE A SUA ESCOLA OU PROJETO SOCIAL SE INSCREVA		
JOVENS DE 19-25 ANOS		SE VOCÊ FOR LÍDER DE ALGUM PROJETO OU ONG QUE ATENDE O PÚBLICO ALVO, SIM!	VOCÊ PODE PARTICIPAR COMO FACILITADOR! MAS PRECISA SE INSCREVER PARA O CURSO DE FORMAÇÃO, OK?	
EDUCADORES				
LÍDERES DO SETOR PÚBLICO E DA SOCIEDADE CIVIL	SE VOCÊ TAMBÉM ATUAR COMO EDUCADOR, TÁ VALENDO			
DEMAIS PÚBLICOS	NÃO, MAS VOCÊ PODE BAIXAR OS CONTEÚDOS DO PROGRAMA!	NÃO, MAS VOCÊ PODE PEDIR PARA QUE A ESCOLA OU PROJETO SOCIAL QUE CONHECE SE INSCREVA		

# 1.3 SOBRE A SAFERNET

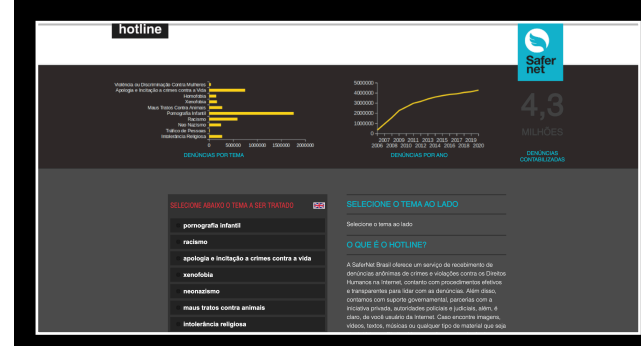
A SaferNet é a primeira ONG do Brasil a estabelecer uma abordagem multissetorial para promoção dos Direitos Humanos no ambiente digital. Criamos e coordenamos desde 2005 a Central Nacional de Denúncias de Violações contra Direitos Humanos (Hotline), o Canal Nacional de Apoio e Orientação sobre Segurança na Internet (Helpline) e desenvolvemos ações de conscientização sobre uso cidadão da Internet.

São mais de 15 anos de experiência na entrega de projetos inovadores com enorme impacto social, incluindo programas de capacitação para educadores, adolescentes, jovens e formuladores de políticas públicas no Brasil.

Recebemos mais de 4 milhões de denúncias, mais de 32 mil atendimentos a vítimas de violações na rede e 81 mil matrículas de educadores nos cursos EAD. Só em 2020, foram mais de 10 milhões de pessoas impactadas por nossas campanhas. Fazemos parte da rede Inhope/ Insafe e desde 2009, lideramos o Dia Mundial da Internet Segura no Brasil. Em 2013, fomos homenageados com o Prêmio Nacional de Direitos Humanos, concedido pela Presidência da República do Brasil



SAIBA MAIS



**CENTRAL NACIONAL DE DENÚNCIAS DE VIOLAÇÕES CONTRA OS DIREITOS HUMANOS**



**CANAL DE AJUDA**



**DIA DA INTERNET SEGURA**

**Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**

Em 15 anos, a Central de Denúncias recebeu e processou 4.291.200 denúncias anônimas envolvendo 64.401 páginas (URLs) distintas (das quais 465.249 foram removidas) escritas em 18 idiomas e hospedadas em 78.932 domínios diferentes de 208 diferentes TLDs e conectadas à internet através de 79.576 números (Países distintos, atribuídos para 100 países em 6 continentes). As denúncias foram registradas pela população através dos 3 hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos. Saiba mais sobre este projeto!

**OS INDICADORES DE DENÚNCIAS RECEBIDAS DESDE O INÍCIO DA AÇÃO, EM 2006, ESTÃO DISPONÍVEIS PARA CONSULTA. O CANAL DE DENÚNCIAS É MEMBRO DA REDE INTERNACIONAL DE COMBATE A IMAGENS DE ABUSO SEXUAL DE CRIANÇAS E ADOLESCENTES INHOPE.**

# 1.4 SOBRE A FORMAÇÃO

Queremos te dar as boas-vindas na formação do programa Cidadão Digital 2021! Neste caderno de formação on-line de 25 horas, autoinstrucional, vamos compartilhar materiais educativos e orientações para a promoção da cidadania digital, alinhados com as diretrizes da BNCC e do Marco Civil da Internet.

	<b>FORMATO</b>	AUTO- INSTRUCIONAL E REMOTO
	<b>CARGA HORÁRIA</b>	25 HORAS
	<b>UNIDADES TEMÁTICAS</b>	6

## > O QUE EU PRECISO PARA INICIAR A FORMAÇÃO?

Nada! É só iniciar os estudos a partir desse caderno.

## > TEM ALGUM CUSTO?

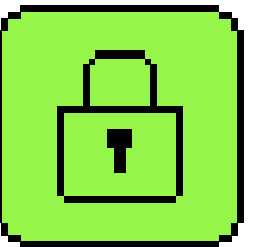
Nenhum. O itinerário formativo é totalmente gratuito.



# 1.5 TEMAS

Confira os percursos deste itinerário que é composto por 6 blocos temáticos, cada um com um vídeo de webinar com especialistas convidados e muitos materiais complementares para conectar os temas com as atividades pedagógicas:

01



**PRIVACIDADE E REPUTAÇÃO**

PANORAMA DO USO DA INTERNET POR ADOLESCENTES NO BRASIL, NOÇÕES BÁSICAS DE RASTROS DIGITAIS, DADOS PESSOAIS, CONFIGURAÇÕES DE PRIVACIDADE E SENHAS SEGURAS

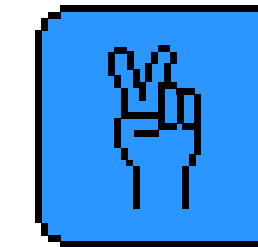
02



**CRIPTOGRAFIA**

COMO FUNCIONA A TECNOLOGIA QUE AJUDA A GARANTIR A SEGURANÇA E A PRIVACIDADE DE SUAS CONVERSAS E ARQUIVOS

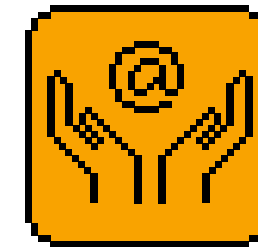
03



**COMPORTAMENTOS POSITIVOS NA REDE**

RESPEITO E EMPATIA NAS REDES; RELACIONAMENTOS SAUDÁVEIS; PREVENÇÃO E ENFRENTAMENTO DE VIOLÊNCIA ONLINE: DISCRIMINAÇÃO, CIBERBULLYING, VAZAMENTO DE IMAGENS ÍNTIMAS E SEXTORSÃO

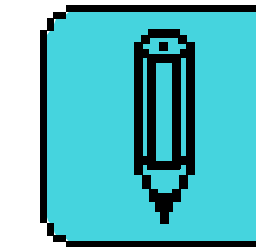
04



**AUTOCUIDADO E SAÚDE EMOCIONAL**

COMPARAÇÃO SOCIAL, USO EXCESSIVO E ROTINAS SAUDÁVEIS ONLINE PARA PROMOÇÃO DO BEM-ESTAR

05



**EDUCAÇÃO MIDIÁTICA**

"FAKE NEWS" OU DESINFORMAÇÃO, VERIFICAÇÃO DE NOTÍCIAS E LEITURA CRÍTICA

06



**AÇÕES INSPIRADORAS**

CAMPANHAS DE ENGAJAMENTO MOBILE, FERRAMENTAS DE APOIO NA EDUCAÇÃO PARA CIDADANIA DIGITAL

1.6

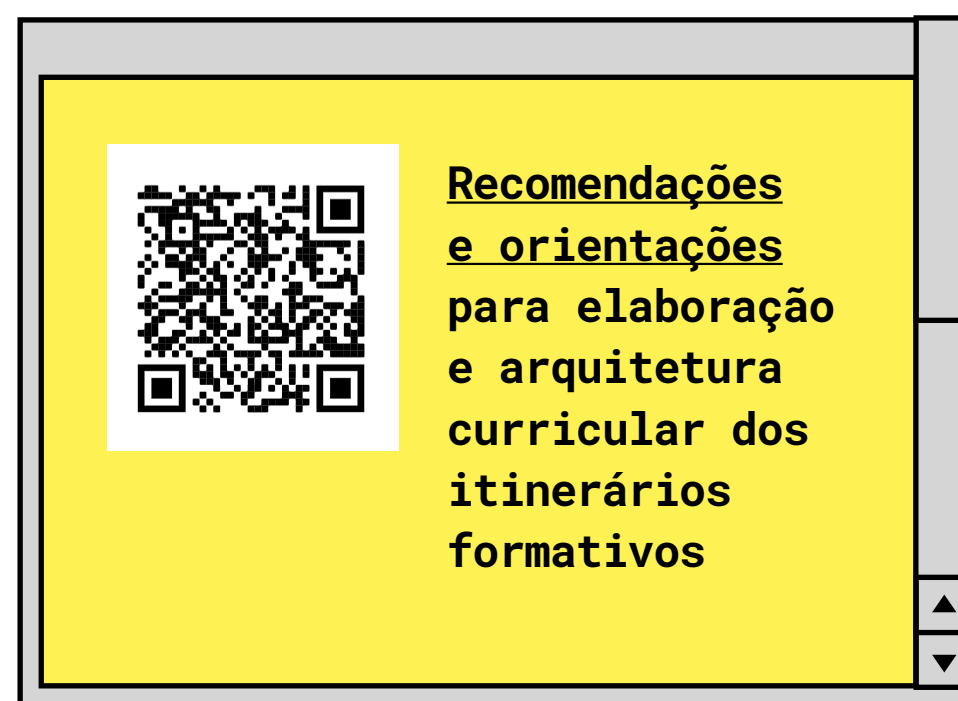
# BNCC E BNC

## RELAÇÃO COM BASE NACIONAL COMUM CURRICULAR

Este material foi criado para educadores a partir dos elementos da competência geral 5, relacionada à cultura digital, prevista pela **BNCC** (BRASIL, 2018) para a educação básica.

Os blocos temáticos são também alinhados a competências específicas e habilidades de diferentes componentes curriculares consideradas as etapas do ensino fundamental – anos finais e do ensino médio. Além disso, a formação

pode subsidiar a construção de itinerários formativos na área de “Mediação e intervenção sociocultural” (BRASIL, 2019) no novo Ensino Médio.

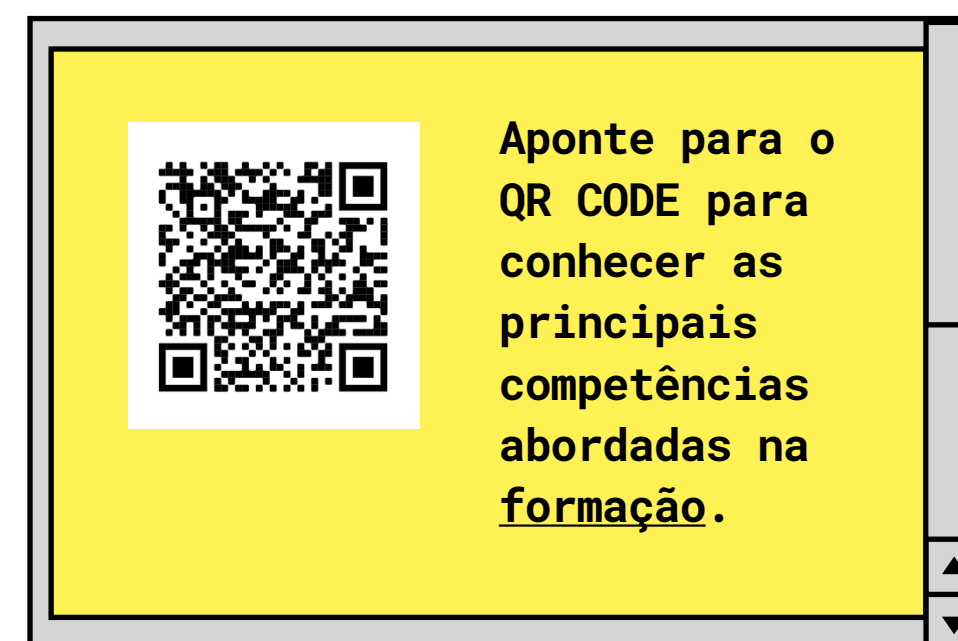


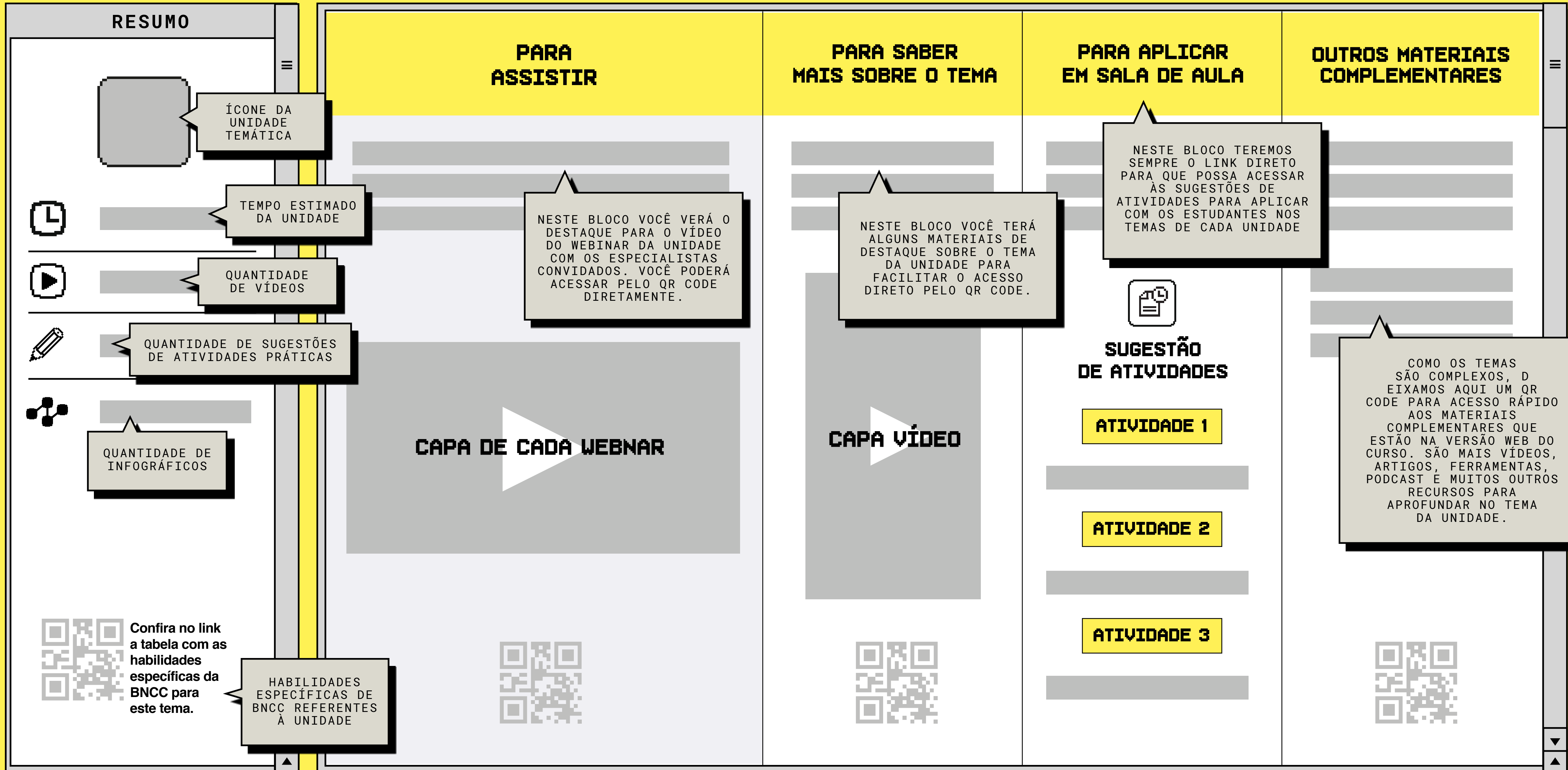
## RELAÇÃO COM BNC - FORMAÇÃO CONTINUADA

A trilha formativa também observa as Diretrizes Curriculares Nacionais para a Formação Continuada de Professores, com orientação da Base Nacional Comum para a Formação Continuada de Professores da Educação Básica – BNC-Formação Continuada (BRASIL, 2020).

A BNC-Formação Continuada tem em vista o desenvolvimento contínuo da profissão docente na busca por fortalecer dimensões que favoreçam o apoio pleno aos estudantes na construção de aprendizagens essenciais (BRASIL, 2018). Essas dimensões são

complementares e interdependentes, abrangendo, além de competências gerais, competências específicas distribuídas em: I – conhecimento profissional; II – prática profissional; e III – engajamento profissional.





RESUMO

ÍCONE DA UNIDADE TEMÁTICA

TEMPO ESTIMADO DA UNIDADE

QUANTIDADE DE VÍDEOS

QUANTIDADE DE SUGESTÕES DE ATIVIDADES PRÁTICAS

QUANTIDADE DE INFOGRÁFICOS

HABILIDADES ESPECÍFICAS DE BNCC REFERENTES À UNIDADE

Confira no link a tabela com as habilidades específicas da BNCC para este tema.

PARA ASSISTIR

NESTE BLOCO VOCÊ VERÁ O DESTAQUE PARA O VÍDEO DO WEBINAR DA UNIDADE COM OS ESPECIALISTAS CONVIDADOS. VOCÊ PODERÁ ACESSAR PELO QR CODE DIRETAMENTE.

CAPA DE CADA WEBINAR

PARA SABER MAIS SOBRE O TEMA

NESTE BLOCO VOCÊ TERÁ ALGUNS MATERIAIS DE DESTAQUE SOBRE O TEMA DA UNIDADE PARA FACILITAR O ACESSO DIRETO PELO QR CODE.

CAPA VÍDEO

PARA APLICAR EM SALA DE AULA

NESTE BLOCO TEREMOS SEMPRE O LINK DIRETO PARA QUE POSSA ACESSAR ÀS SUGESTÕES DE ATIVIDADES PARA APLICAR COM OS ESTUDANTES NOS TEMAS DE CADA UNIDADE

SUGESTÃO DE ATIVIDADES

ATIVIDADE 1

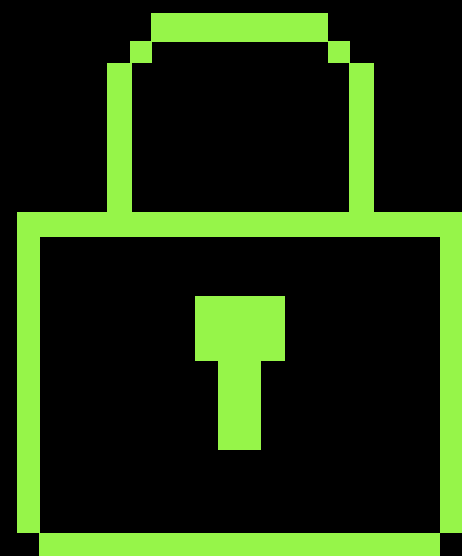
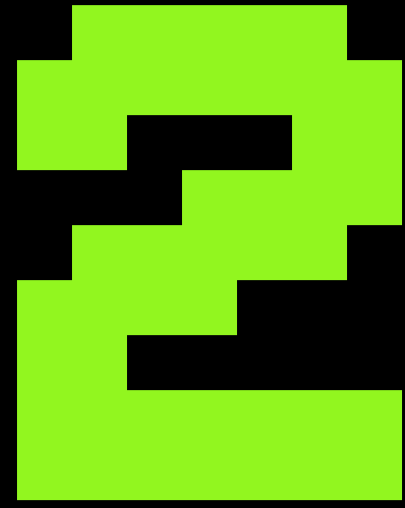
ATIVIDADE 2

ATIVIDADE 3

OUTROS MATERIAIS COMPLEMENTARES

COMO OS TEMAS SÃO COMPLEXOS, D EIXAMOS AQUI UM QR CODE PARA ACESSO RÁPIDO AOS MATERIAIS COMPLEMENTARES QUE ESTÃO NA VERSÃO WEB DO CURSO. SÃO MAIS VÍDEOS, ARTIGOS, FERRAMENTAS, PODCAST E MUITOS OUTROS RECURSOS PARA APROFUNDAR NO TEMA DA UNIDADE.

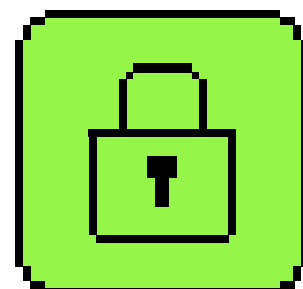
CAPÍTULO



Privacidade remete a um amplo debate. Vamos apresentar aqui alguns materiais mencionados pelos convidados e também recursos complementares, sempre pensando em sugestões que ajudem a preparar atividades remotas e presenciais com adolescentes da rede pública.

# PRIVACIDADE E REPUTAÇÃO

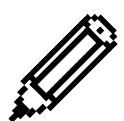
RESUMO



2 HORAS



4 VIDEOS



3 SUGESTÕES DE ATIVIDADE

O trabalho com a temática da segurança digital, da privacidade e da reputação on-line pode mobilizar competências e habilidades previstas pela BNCC (BRASIL, 2018) ao abranger desde cuidados no uso das tecnologias digitais até algoritmos de proteção de dados, passando pela observação de direitos e deveres.



Confira no link a tabela com as habilidades específicas da BNCC para este tema.

PARA ASSISTIR

Diretor de educação da Safernet, Rodrigo Nejm conversa sobre privacidade e reputação digital de adolescentes com Bruno Bioni, advogado e Diretor-fundador do Data Privacy Brasil, e Luísa Adib, coordenadora da pesquisa TIC Kids Online do CETIC.br/NIC.br.



PARA SABER MAIS SOBRE O TEMA

Dicas práticas e boas reflexões sobre privacidade nas redes digitais



PARA APLICAR EM SALA DE AULA

Recursos práticos para usar em sala de aula (remota ou presencial)



SUGESTÃO DE ATIVIDADES

ATIVIDADE 1

Mini aula animada para iniciar discussões e trabalhos em grupo

ATIVIDADE 2

Fazendo e compartilhando um passo a passo de ajustes de privacidade

ATIVIDADE 3

Conjunto de aulas para refletir sobre redes sociais e compartilhamento

OUTROS MATERIAIS COMPLEMENTARES

Confira material extra na versão online da formação para aprofundar seus conhecimentos.






2.1

# CONTEXTO

Para todas as atividades do programa Cidadão Digital, buscamos analisar o que temos de indicadores sobre o contexto de uso da Internet por crianças e adolescentes no Brasil. Uma das referências que destacamos é a pesquisa **TIC Kids Online, realizada pelo CETIC.br - NIC.br - CGI.br**. A pesquisa aponta desigualdades regio-nais e econômicas nas formas de acesso, o que se reflete na forma como as oportunidades e os riscos são experienciados.

**Vejamos um resumo que contempla outros tópicos além da Privacidade:**

Os dados específicos sobre habilidades indicam que ainda há muitas dúvidas sobre privacidade e sobre como desativar a geolocalização dos aparelhos.

HABILIDADES PARA O USO DA INTERNET				
% de crianças e adolescentes de 11 a 17 anos usuários de internet (2019)	TOTAL	11 a 12 anos	13 a 14 anos	15 a 17 anos
 MUDAR AS CONFIGURAÇÕES DE PRIVACIDADE EM REDES SOCIAIS	60	36	55	76
 DESATIVAR A FUNÇÃO DE GEOLOCALIZAÇÃO	65	44	65	77
 EXCLUIR PESSOAS DA LISTA DE CONTATOS OU AMIGOS	89	76	91	95

Muitos adolescentes usam as redes sociais com o perfil público, assim, as informações podem ser recebidas, copiadas e compartilhadas para pessoas muito distantes e não há como ter controle do alcance.

Na dúvida, é sempre bom pensar bem antes de compartilhar para reconhecer os potenciais riscos e escolher com cuidado, o que, onde e com quem compartilhar. Mas sempre rola uma brecha... 23% dos adolescentes entre 11 e 17 anos afirmam que já publicaram alguma coisa na Internet, se arrependeram e depois apagaram.

Sabemos que este “apagar” não garante que a informação não tenha sido vista, copiada e até usada sem a autorização neste intervalo.

Vale também observar a forma como a Internet é usada nas escolas públicas brasileiras com os dados da pesquisa TIC Educação. Infelizmente o tema “uso seguro e consciente” ainda não está presente no planejamento pedagógico da maior parte das escolas públicas do país. Mas o cenário vem melhorando e você pode fazer uma diferença positiva com suas ações, aplicando os materiais que receberá nesta formação ;)

PARA SABER MAIS




VOCÊ PODE CONFERIR OS DADOS DETALHADOS DAS PESQUISAS TIC KIDS ONLINE E TIC EDUCAÇÃO [AQUI](#).




2.2

# PRIVACIDADE, DADOS PESSOAIS E REPUTAÇÃO


VAMOS COMEÇAR!

 **PRIVACIDADE**


O direito individual de controlar informações, assuntos e relações pessoais, escolhendo não compartilhar ou selecionando o que, como e com quem compartilhar conteúdos pessoais.

 **REPUTAÇÃO**


A palavra reputação tem origem no latim reputatio, relacionada ao verbo reputare: pensar, refletir, calcular o valor de algo. No uso que fazemos atualmente no português, "reputação" se tornou uma avaliação sobre o valor moral de alguém.

 **DADOS PESSOAIS**

Informação relacionada a pessoa natural identificada ou identificável.

 **DADO PESSOAL SENSÍVEL**

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

 **DADO ANONIMIZADO**

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

PARA SABER MAIS



DEFINIÇÕES NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (13.709/2018)



## 2.2 CONTINUAÇÃO

Tudo o que a gente faz na internet se transforma em dado. Cada publicação, cada novo seguidor, cada conteúdo curtido ou compartilhado gera informações sobre quem é você na rede. Mesmo o uso de aplicativos no celular que não tem espaço para “publicar” gera dados sobre seus hábitos. Quantas vezes por dia você usa, quais conteúdos prefere, com quem conversa ou mesmo em quais locais você estava ao usar são exemplos de informações que ficam registradas.

Daí a importância de discutir **PRIVACIDADE e REPUTAÇÃO** no ambiente digital. O papo aqui é sobre como as ferramentas de privacidade e segurança podem ajudar a ter mais controle sobre a presença online, para que as pessoas façam escolhas mais conscientes. O que entendemos como privacidade tem mudado no mundo atual, por isso é tão importante que cada um pare para pensar, e agir, sobre a forma como se apresenta nas redes.

Como todo comportamento on-line deixa um registro, um rastro, precisamos assumir o controle para que as escolhas sejam feitas de forma consciente e crítica. Conheça mais sobre alguns tipos de rastros digitais [aqui](#).

Tudo isso pode parecer muito óbvio, ou papo chato, mas a proposta é que você possa ajudar a debater estes temas de maneira mais suave e divertida possível, conectando com os projetos de vida dos estudantes.

Cada um tem seus limites, seus objetivos e sua personalidade, fazendo com que as escolhas certas sejam diferentes, únicas. Pensar em uma carreira, em um plano de vida e nas conquistas que desejamos para nossas vidas passa também por cuidar da reputação digital. E vale lembrar que o Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tem a proteção da privacidade e dos dados pessoais como base.





2.3

# FERRAMENTAS PRÁTICAS

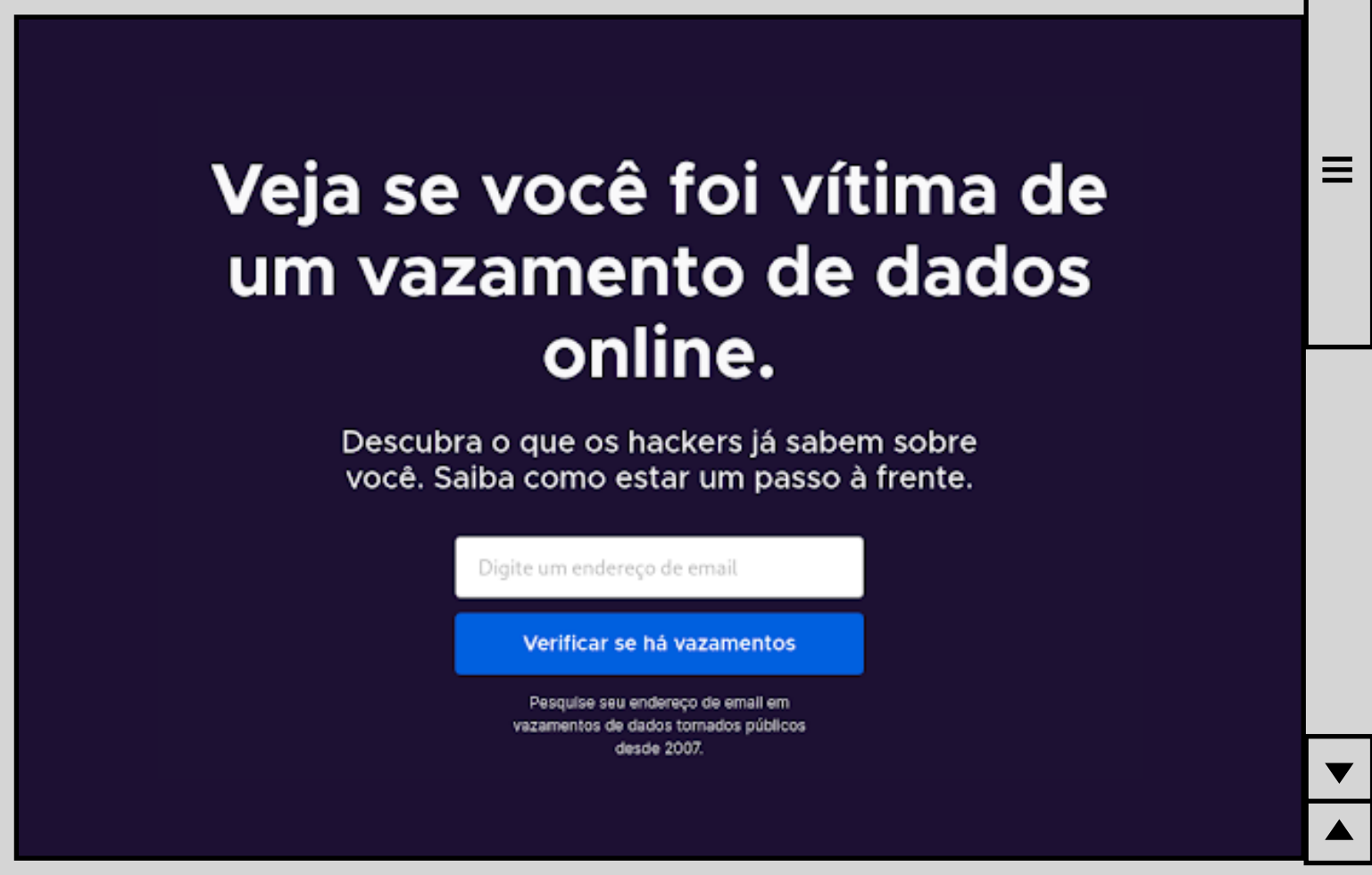
Há algumas ferramentas que ajudam a ampliar a privacidade e segurança nas redes. Nem sempre os jovens usam ou sabem que existem. Vamos listar algumas que podem ser usadas nas atividades com adolescentes e nas nossas próprias contas. É possível escolher audiências, apagar conteúdos antigos que não fazem mais sentido, proteger os aparelhos e contas ou até baixar todo conteúdo publicado antes de excluir um perfil.

## SENHAS

Começamos pelo básico: senha. Não dá para manter o “1234”, nem o “9876543210”. Parece piada, mas estas ainda estão entre as 50 senhas mais usadas no mundo. Colocar senha no celular e reforçar o tamanho das senhas nas contas é o passo 1.

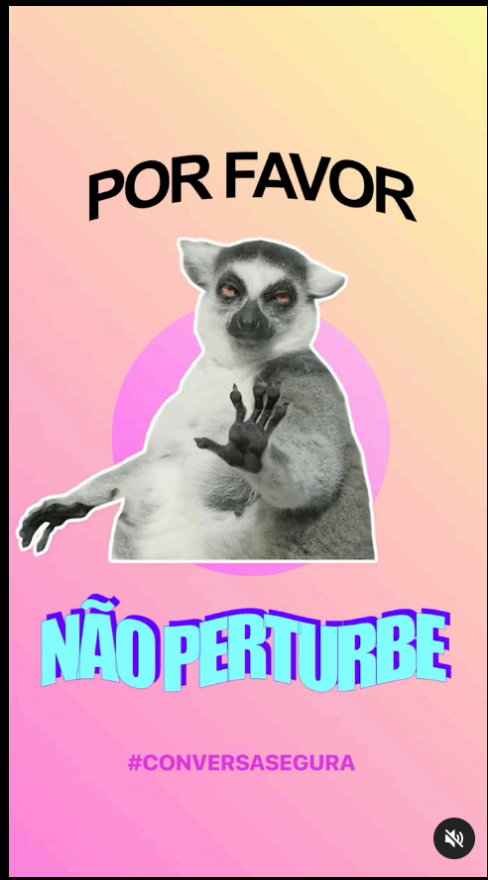
Existem alguns sites alguns sites na Internet que te permitem checar se o seu e-mail “caiu” na rede ou foi alvo de algum grande vazamento recente.

É só jogar o seu e-mail no Firefox Monitor (em português) ou no **Have I Been Pwned?** (em inglês) que ele te ajudam a localizar por onde suas informações circularam. Dica: essa ferramenta faz muito sucesso com os alunos



nas atividades e pode ser utilizada em tempo real! Além disso, ajuda a demonstrar porque gerenciadores de senha são tão importantes: afinal, se o seu email for objeto de um **grande vazamento que expõe senhas**, automaticamente todas as suas outras senhas se tornam comprometidas e você tem um trabalho muito maior para sair trocando tudo. Não precisa entrar em pânico, importante é trocar as senhas e reforçar a segurança das contas com as dicas a seguir.

VIDEO



### 2.3 CONTINUAÇÃO

#### VERIFICAÇÃO EM 2 ETAPAS

A verificação em duas etapas é uma camada extra de segurança que você pode incluir nas suas contas de aplicativos, sites, contas de email e de armazenamento. Ela pode ser chamada também:

- Verificação em 2 fatores
- Autenticação em dois passos
- Two-factor authentication
- Aprovação de login

Ao habilitar o recurso na sua conta, há opção de geração de um novo código complementar à sua senha e que dificulta o acesso não autorizado. O código pode ser enviado por SMS ou email, gerada aleatoriamente em um gerador de códigos ou ter um cartão de códigos. Há ainda a opção, em alguns serviços, de ativar a confirmação a partir

de um aparelho confiável previamente cadastrado. Dessa forma, caso sua senha tenha sido descoberta, você garante que sua conta não será invadida, já que esse segundo código é necessário toda vez que quiser acessá-la de um novo dispositivo. Em um mundo em que cada vez mais nos preocupamos com a segurança das nossas informações, a verificação em duas etapas é uma estratégia essencial. Lembre-se sempre de atualizar a sua verificação em duas etapas caso tenha trocado de celular ou de número.

Uma forma bacana de introduzir o assunto é lembrar que no mundo offline

nós também utilizamos esse tipo de estratégia. Atualmente, por exemplo, a maioria dos bancos exige, além da senha, uma autenticação biométrica (digital) para que sejam realizados saques. Ou quando você precisa, além de assinar um documento, também mostrar algum documento oficial seu, como o RG, em que consta sua foto e assinatura.

A verificação em duas etapas é para todos, de todas as idades, em todas as redes. Se não fez ainda, aproveite. Além do SMS, você pode utilizar aplicativos específicos, como **Google Authenticator**, **Microsoft Authenticator**, **Authenticator**

ou o **Authy** (em inglês). Eles geram códigos de verificação que expiram após um tempo, o que torna ainda mais difícil um acesso indevido. Bacana né?

Lembre-se: nunca informe para outra pessoa códigos de verificação que você recebe por SMS ou por um aplicativo autenticador. Isso é uma tática utilizada por golpistas para conseguir acesso ao seu celular ou a uma conta. Mas nosso desafio é estimular (e facilitar) o acesso a estas ferramentas pelos adolescentes. Mesmo sem um aplicativo específico para a verificação em 2 etapas, você pode ativar diretamente em suas contas.

**Confira os caminhos nas principais redes:**

**JÁ DEU PARA VER QUE TODAS AS REDES SOCIAIS, PLATAFORMAS DE JOGOS E MESMO OS APLICATIVOS DE VÍDEO E MÚSICA PERMITEM ALGUM CONTROLE DE SEGURANÇA E PRIVACIDADE. BASTA IR NAS CONFIGURAÇÕES DA CONTA E BUSCAR POR “SEGURANÇA” OU “PRIVACIDADE”. A VERIFICAÇÃO EM 2 ETAPAS PRECISA SER ATIVADAS EM TODAS PARA EVITAR SURPRESAS E GOLPES. VALE GASTAR UNS MINUTINHOS EM SUAS CONTAS PARA FAZER AQUELE UPGRADE EM SUA SEGURANÇA ;) MAS FICA A PERGUNTA, SERÁ QUE CONSEGUIMOS CONVENCER OS ADOLESCENTES SOBRE A IMPORTÂNCIA DISSO TUDO?**



A1

ATIVIDADE 1

Com o contexto das ações remotas, podemos usar vários formatos diferentes de ações com os alunos das escolas públicas, sempre respeitando os limites de acesso de cada localidade. Um recurso bem valioso que temos para começar o debate é o vídeo feito pela SaferNet com os embaixadores do Cidadão Digital em 2020. Como uma mini aula animada, podemos iniciar o papo e conectar com os materiais de apoio (slides, gincanas, quiz e outros recursos disponíveis).

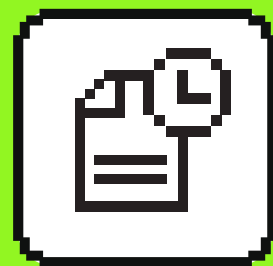
TÍTULO

**Autenticação de 2 fatores**  
*é uma camada de segurança adicional para sua conta*




TÍTULO



A2

ATIVIDADE 2

Com base na conversa com Luísa (CETIC.br) e com Bruno (Data Privacy), o desafio a ser feito aos alunos pode ser dividido em duas atividades:

1 Faça seu próprio check-up (verificação) de privacidade e segurança em suas contas em redes sociais. No material acima, você encontra links para as páginas oficiais sobre o tema nas redes mais conhecidas. Leia sobre as principais configurações, busque entender os termos e faça ajustes que você considera essenciais para manter suas contas mais seguras e privadas, lembrando sempre das dicas que foram dadas. A ideia é colocar a mão na massa e experimentar, então não é necessário enviar nenhuma comprovação do seu check-up.

2 Depois de passar por esse processo, imagine que você precisa traduzi-lo de forma acessível para adolescentes de uma comunidade que está recebendo internet pela primeira vez, orientando sobre configurações e ajustes possíveis.

Pense: o que você acha que funcionaria? Como começar a criar uma consciência crítica sobre o tema sem ser impositivo? Agora é hora de materializar essas dicas: crie um conjunto de pelo menos três

imagens contendo os ajustes que você considera principais para uma ou mais redes. Tente deixar claro o porquê desses ajustes serem importantes. A proposta é pensar essa série de conteúdos como se você fosse postá-los em suas redes sociais, campanhas na escola ou outro formato interessante para atrair a atenção dos adolescentes. Vale pensar no formato de stories, memes, gifs, banners, infográficos, etc. Vale ter texto, prints, ilustrações, o que você achar que vai criar um conteúdo acessível, informativo, divertido, que as pessoas tenham vontade de ver e conhecer mais.

Você pode usar aplicativos/sites gratuitos para ajudar a criar essas imagens. São exemplos o **Canva** (para criar posts/stories/cartazes), **Pixabay** (para baixar imagens com licença gratuita) e **Freepik** (para baixar ícones e outras ilustrações de apoio gratuitas). Procure sempre usar conteúdos de licença aberta para respeitar os direitos de autor. Solte a criatividade! Caso crie uma imagem para ser postada em uma rede social, você pode também pensar em um texto de

apoio. Organize com os alunos uma forma de receber o material produzido para uma revisão e um debate em grupo.

3 Resuma em um parágrafo o que você aprendeu com a experiência. Por quais caminhos você achou melhor iniciar a conversa sem deixá-la entediante para os adolescentes? Conte como foi o processo de fazer o seu check-up de privacidade e segurança nas redes. Foi difícil? O que acha que poderia melhorar nas configurações disponíveis?

DICA

A ATIVIDADE PODE CONTEXTUALIZAR O TRABALHO COM GÊNEROS DOS CAMPOS JORNALÍSTICO-MIDIÁTICO E DE ATUAÇÃO NA VIDA PÚBLICA AO ABORDAR ESTRATÉGIAS DE INFORMAÇÃO E PERSUAÇÃO MEDIADAS PELA ESCRITA DIGITAL.



A3

ATIVIDADE 3

Este material pode ajudar a pensar outras atividades on-line e no contexto remoto da educação, para mobilizar os adolescentes nas escolas.

Biblioteca de Alfabetização Digital

Privacidade e reputação

# Redes sociais e compartilhamento

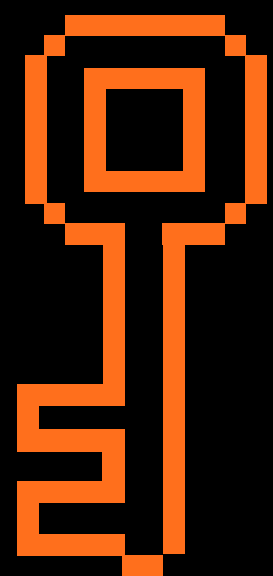
De Youth & Media

Iniciar esta lição

Baixar pacote de lições




CAPÍTULO




Vamos agora desmistificar este importante recurso de proteção das informações: a criptografia. Nunca ouviu falar? Ficou com medo de não entender? Calma, que neste bloco você vai entender mais sobre o que é, qual é a aplicação no nosso dia a dia e, principalmente, como trabalhar o tema com os estudantes.

# CRIPTOGRAFIA

### RESUMO




---



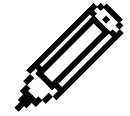
**2 HORAS**

---




**3 VIDEOS**

---




**1 SUGESTÃO DE ATIVIDADE**


O trabalho com a temática da criptografia pode mobilizar competências e habilidades previstas pela BNCC (BRASIL, 2018) ao abranger a investigação e análise sobre o funcionamento tecnologias digitais, seus princípios e implicações sociais.



### PARA ASSISTIR

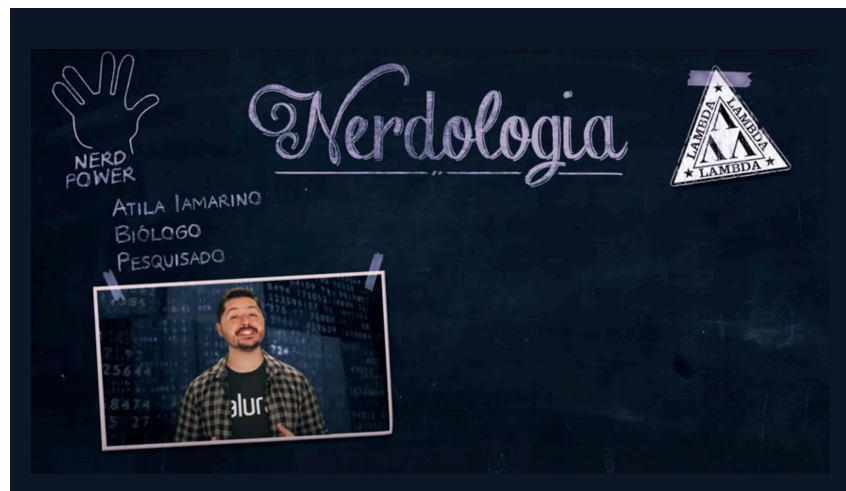
Criptografia no cotidiano e na escola. Debate com Dario Durigan, diretor de Políticas Públicas para o WhatsApp no Brasil, Ecivaldo de Souza Matos, Professor do Dep. de Ciência da Computação e do Programa de Pós-graduação em Ensino, Filosofia e História das Ciências da UFBA, e Raquel Saraiva, presidenta do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Mediação de Guilherme Alves, mestre em Tecnologia e Sociedade, coordenador de engajamento de jovens da SaferNet Brasil.






### PARA SABER MAIS SOBRE O TEMA


Criptografia proporciona segurança na comunicação ao transformar a “mensagem” em um código, que só pode ser decifrado por quem tem a chave. Há séculos já era usada, mas agora ficou muito mais popular, e avançada.





### PARA APLICAR EM SALA DE AULA

Qual a importância da criptografia no dia a dia? Quais implicações para nossa cidadania? Como funciona a informação “cifrada”?




**SUGESTÃO DE ATIVIDADES**

**ATIVIDADE 1**

Dinâmica com os estudantes utilizando o conceito de “cifrar” uma informação transformando-a em texto codificado.

### OUTROS MATERIAIS COMPLEMENTARES

[Confira material extra na versão online da formação para aprofundar seus conhecimentos.](#)



3.1

# CONTEXTO

A Internet possibilitou uma revolução comunicativa e informacional, impulsionando a comunicação a nível global pela grande capacidade de conexão entre as pessoas. Nos módulos anteriores, vimos como ferramentas de privacidade e segurança da informação podem ajudar a tornar nossa experiência online mais segura, inclusive protegendo contra ameaças e violências que podem ser desencadeadas por discriminação ou intolerância. Nesta semana, continuamos a falar de ferramentas de proteção, agora tratando especificamente sobre criptografia. Nunca ouviu falar? Ficou com medo de não entender? Calma, que neste módulo você vai entender mais sobre o que é e, principalmente, qual é a aplicação da criptografia no nosso dia a dia online.

O desenvolvimento tecnológico, para além dos benefícios sociais e científicos, constantemente desafia a garantia e a manutenção de direitos fundamentais. Sabemos que a Internet possibilitou a criação de ferramentas de comunicação instantânea que podem ser aliadas, por exemplo, do direito ao acesso à informação e à cultura.

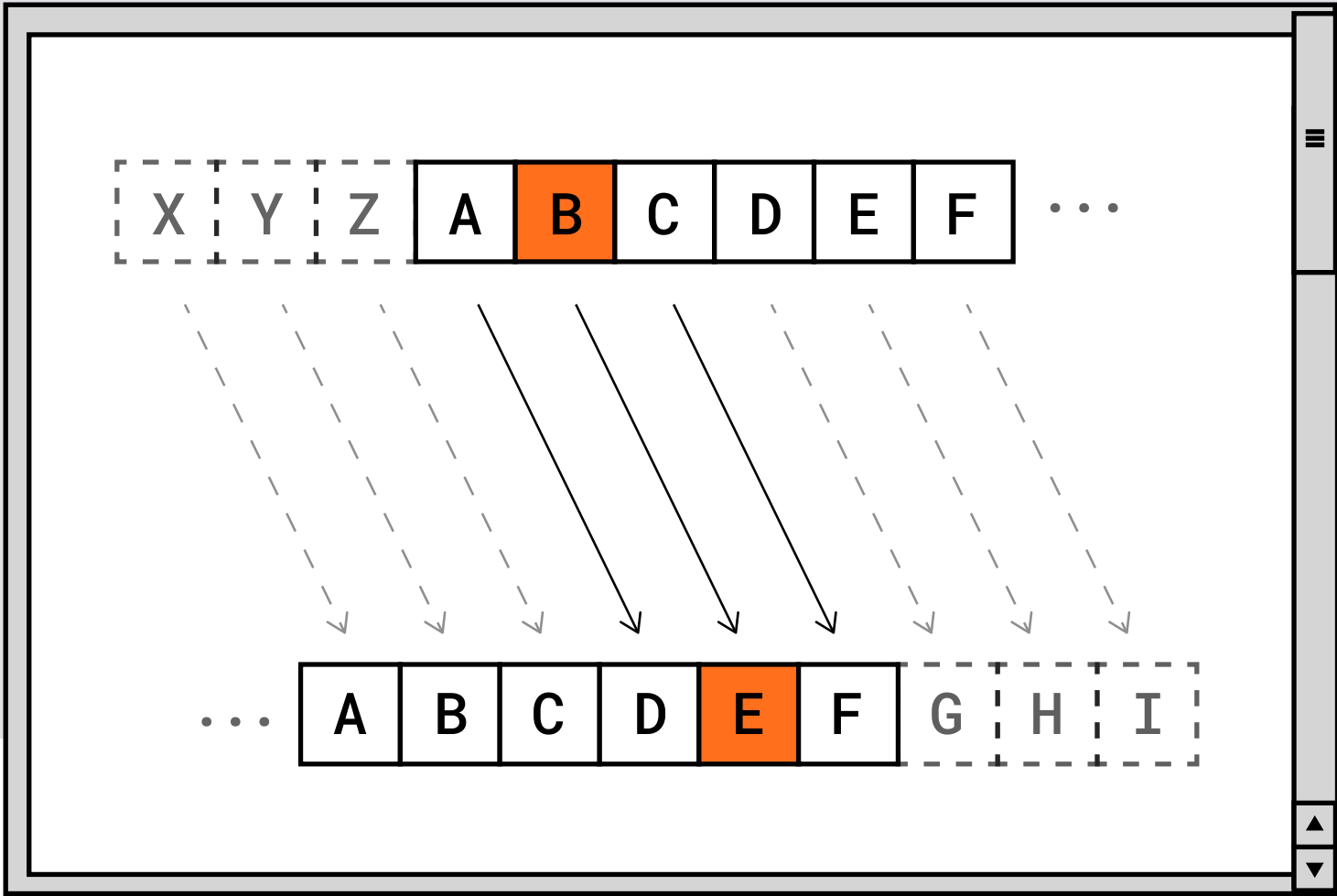
Mas como garantimos que essa comunicação será, de fato, privada? A criptografia é uma das nossas estratégias. Ela proporciona segurança nesta comunicação ao transformar a “mensagem” em um código, que só pode ser decifrado por quem tem a chave. E o melhor é que isso pode ser feito utilizando tecnologias que nós nem sabemos que existem, mas que estão

operando por trás de cada clique que damos na Internet. Garantir a privacidade de uma mensagem é garantir também a liberdade de expressão. Vamos entender melhor.

3.1.1

## ESCREVENDO OS CÓDIGOS NA HISTÓRIA

A criptografia era vista, na antiguidade, como uma arte. Sim, ela não foi inventada com os computadores. “A arte de escrever e decifrar códigos”, como



expressa o Dicionário Oxford, é uma técnica utilizada desde a antiguidade para proteger mensagens de guerra, trocas diplomáticas e comerciais, mas também mensagens de amor.

Um exemplo bem conhecido é a **Cifra de César**. O Imperador da Roma Antiga utilizava uma cifra (combinação secreta de letras) que ficou conhecida com seu nome e que era usada para proteger a comunicação com seu exército. A cifra de César era uma cifra de substituição que usava um deslocamento de 3 posições do alfabeto. Era assim: a letra “A”, por exemplo, era substituída pela “D”; a “B” pela “E”, e assim sucessivamente.



**3.1 CONTINUAÇÃO**

Quem tivesse a chave da cifra, ou seja, soubesse qual era o esquema de substituições, era capaz de decifrar a mensagem.

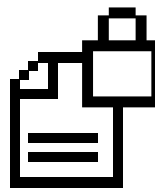
Outro exemplo histórico foi a máquina Enigma, que teve modelos usados durante a Segunda Guerra Mundial. Ela encriptava, isto é, colocava em código, mensagens do comando alemão para os exércitos, com objetivo de proteger a comuni-cação e não entregar os planos aos adversários caso a mensagem fosse interceptada. O mate-mático inglês Alan Turing foi responsável pela quebra da Enigma alemã através da “bomba eletromecânica”, uma máquina construída por ele. A decodificação das mensagens dos inimigos alemães foi muito importante para que os Aliados vencessem a guerra. Turing é considerado, por este feito, o pai da criptografia moderna. Essa história é contada no filme “O jogo da imitação” e nesta pequena aula de história da criptografia.

Turing também criou uma máquina que é considerada a precursora do que conhecemos como computadores hoje.

**3.1.2**


# CRIPTOGRAFIA NA ERA DIGITAL

Nos anos 1970, a criptografia deixou de ser utilizada apenas para a proteção ao sigilo, passando a garantir também a integridade (garantia de que a mensagem não foi alterada no caminho) e a autenticidade (quem foi o autor da mensagem) das comunicações. Surgiu, então, a noção moderna da criptografia. Vamos a este e outros **conceitos básicos**:




## CRIPTOGRAFIA

Transformação de uma informação inteligível numa forma aparentemente ilegível, a fim de ocultar a informação de pessoas não autorizadas. A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos. Hoje, entendemos a criptografia como o uso de técnicas matemáticas para assegurar informação digital, sistemas e computação distribuída contra os ataques de adversários.



## CHAVE DE CRIPTOGRAFIA

Informação usada por um sistema computacional para controlar a encriptação e a decriptação, de modo que só os detentores da chave podem decifrá-la. Funciona como uma senha, mas de forma automática e invisível para os usuários quando utilizada em sistemas computacionais. Ou seja, não precisamos decriptar a mensagem: o sistema faz isso sozinho e sem a gente perceber.



## ENCRIPTAÇÃO E DECRIPTAÇÃO

São os processos de converter uma informação inteligível para uma informação cifrada e vice-versa



## ALGORITMO CRIPTOGRÁFICO

O procedimento computacional utilizado para encriptar e decriptar informações.

### 3.1 CONTINUAÇÃO

A criptografia tem como objetivo a garantia de três propriedades das informações: a confidencialidade, a integridade e a autenticidade. Ou seja, uma informação encriptada permanece:

- **Confidencial, isto é, sigilosa**
- **Íntegra, ou seja, não alterada**
- **Autêntica, no sentido de que o remetente é realmente aquele que diz ser.**

Há dois tipos de sistemas de chaves de criptografia: os simétricos e os assimétricos. Nos **simétricos**, uma mesma chave é usada tanto para encriptar como para decriptar as informações (semelhante a como a criptografia era usada antes dos computadores, como na Cifra de César).

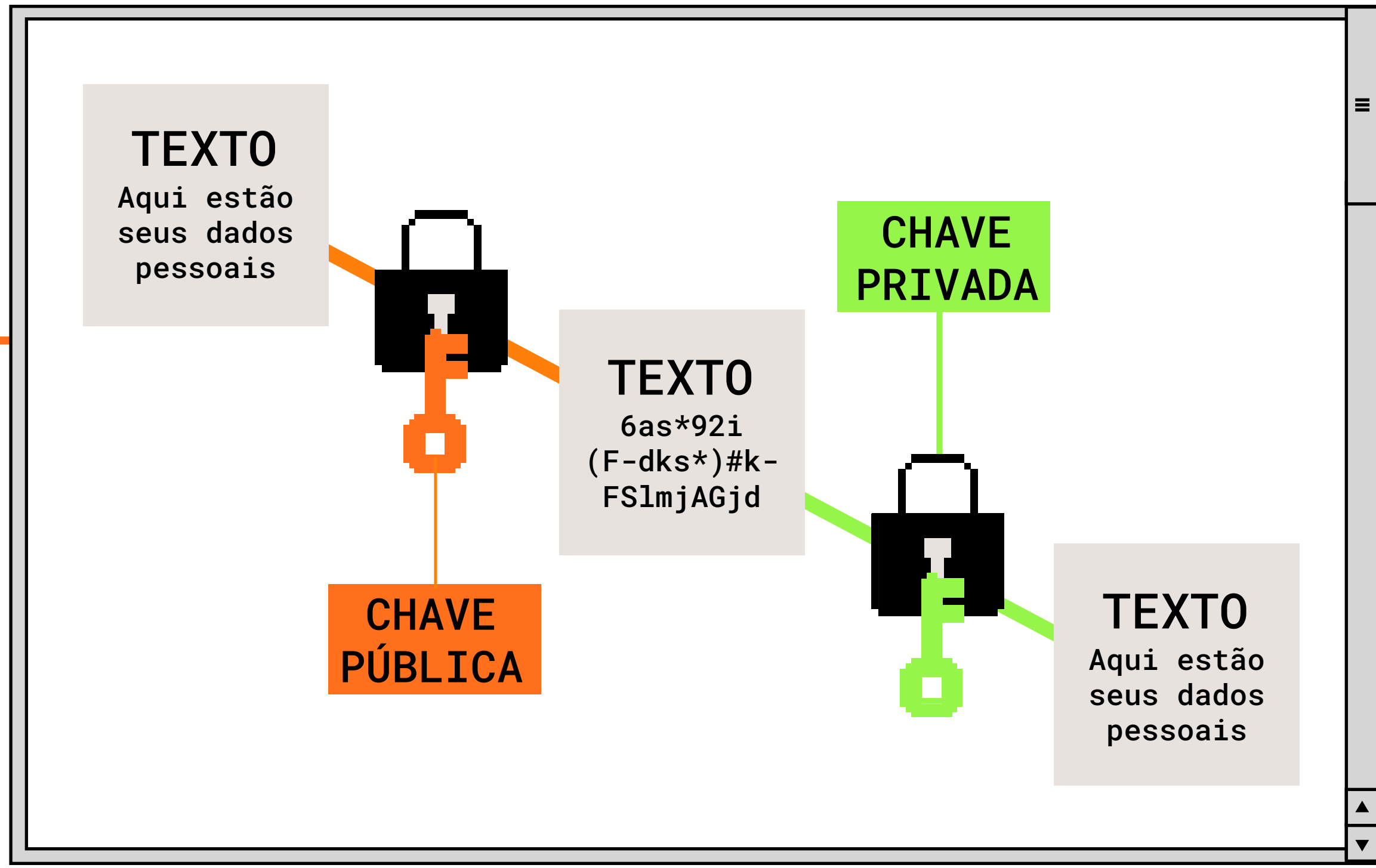
Este sistema funciona bem para quando as informações estão armazenadas localmente (como arquivos no computador ou celular), ou quando as informações estão em uso (como quando estamos escrevendo uma mensagem antes de enviá-la). Entretanto, não é um sistema usado para quando há uma troca constante de informações, porque isso levaria à necessidade de enviar, também, a chave, que poderia ser interceptada no meio do caminho (lembrando que os dados trafegam pela Internet, entre dispositivos e servidores espalhados pelo mundo).

Já nos **sistemas assimétricos**, duas chaves são usadas. Uma delas é pública (todos têm acesso), e ela é usada para encriptar a informação. A segunda delas é privada, e é usada para decriptar a informação. As duas chaves são pareadas (associadas), mas apenas o destinatário da informação tem a chave privada que pode decifrá-la.

Veremos adiante como os sistemas de chaves assimétricas funcionam em

nossos celulares e nos nossos computadores em quase todos os usos que fazemos da Internet -- mesmo sem sabermos, já que as chaves privadas ficam registradas nos códigos dos programas. As chaves assimétricas são as mais usadas ao trocarmos informações (de qualquer tipo) pela Internet. Isso tudo pode parecer muito abstrato, mas vamos ver dois exem-

plos de uso que você certamente faz da criptografia, mesmo sem bem saber. A criptografia nas comunicações pela Internet acontecem de duas principais formas: **a criptografia na camada de transporte de dados** e **a criptografia ponta a ponta**, entre dois polos de comunicação.



## 3.2

# CRIPTOGRAFIA NO TRANSPORTE DE DADOS

A criptografia na camada de transporte é aplicada na comunicação entre páginas na Internet e o navegador utilizado pelo usuário, no momento em que os dados são transferidos entre dispositivos. Toda vez que acessamos um site na Web, nosso navegador envia uma solicitação para que o servidor do site nos retorne com as informações que solicitamos. Esse processo ocorre continuamente, de forma automática, enquanto navegamos pelo site.

Para entender melhor: quando enviamos uma encomenda pelos Correios, o pacote vai lacrado e essa é nossa garantia de que ele não foi aberto. Na criptografia no transporte de dados, temos um sistema de chaves que garante o “lacre” das infor-

mações enviadas e que vão transitar entre o seu navegador e os sites que você visitar.

Por exemplo, para transações bancárias realizadas pela Internet, bem como operações de comércio eletrônico, essa segurança adicional é fundamental por ser a proteção contra fraudadores de qualquer espécie. Nesses casos, a criptografia é usada para evitar que alguém possa capturar a informação no caminho entre o seu navegador e o servidor da página da Internet e usar essa informação de forma maliciosa (por exemplo, descobrindo sua senha do banco ou número do cartão de crédito).

**Como saber se esse tipo de criptografia está ativa?** Na barra de endereço nos navegadores, antes do domínio (endere-

ço) do site, você geralmente encontra a sigla HTTP, que é o protocolo que usamos para acessar páginas na Web. Quando há um S após o HTTP, transformando-o em **HTTPS**, isso significa que os dados entre o seu navegador e o servidor do site transitam de forma criptografada e, portanto, mais segura. Esse tipo de criptografia é conhecida pelas siglas em inglês, SSL (Protocolo de Camada Segura de Soquetes, em português) e TLS (Segurança da Camada de Transporte, em português), sendo a última mais recente e mais segura.

**Todo site HTTPS é seguro?** É preciso mencionar que, infelizmente, o HTTPS não garante uma segurança total, já que alguns sites mal-intencionados também

aceitam o protocolo. Essa proteção fica no “lacre” da informação, garantindo que os dados não sejam decifrados no meio do caminho. Mas, se o site for do tipo phishing, isto é, um site falso que imita um verdadeiro, o HTTPS vai apenas garantir que sua informação não seja descoberta antes de chegar ao servidor do site e, portanto, ao golpista. Uma pessoa mal intencionada cria um site semelhante a outro já existente e com boa reputação e induz os usuários a inserirem ali seus dados, achando que estão no site verdadeiro. Esse site pode conter HTTPS, mas não é legítimo, pois não é da loja que o consumidor acredita ser. Ou seja, seus dados transitaram de forma protegida, mas o destinatário que pode receber e decifrar o conteúdo é o criminoso.



3.3

# CRIPTOGRAFIA PONTO A PONTO

A criptografia ponta a ponta (E2EE, na sigla em inglês End to End Encryption), por sua vez, assegura que a comunicação entre duas partes não pode ser lida por nenhum intermediário, seja o provedor de conexão (quem fornece o serviço de conexão à Internet), seja o provedor de aplicação (quem fornece o serviço que estamos usando para nos comunicar, como e-mail ou aplicativo de mensagem).

Ela é chamada de ponta a ponta justamente porque acontece antes mesmo de a informação ser transmitida pela Internet.

Aqui são usados os sistemas de chaves assimétricas que apresentamos acima. A informação é encriptada usando uma chave pública que está pareada com o destinatário, e permanece embaralhada até que o destinatário a receba em seu dispositivo, não havendo a possibilidade de os provedores a lerem porque eles não possuem a chave de deciptação dos dados (a chave privada).

No exemplo da encomenda dos Correios, é como se a criptografia de ponta a ponta fosse a proteção para que uma mensagem escrita e colocada dentro do pacote não pudesse ser lida por terceiros ainda que o lacre do pacote fosse violado. Isso porque apenas o destinatário possui a chave privada para poder deciptar a mensagem. Sem a chave, a informação não passa de combinações aleatórias sem qualquer sentido.



3.3 CONTINUAÇÃO

Esse é o tipo de encriptação utilizado por aplicativos de mensagem instantânea populares, como Signal e WhatsApp. Com isso, nem mesmo os próprios provedores do serviço têm acesso ao conteúdo das mensagens que são trocadas, conforme nos explicou no webinar o convidado Dario Durigan, do Whatsapp.

Isso é importante porque os dados não são utilizados para direcionamento de propaganda, por exemplo. Além disso, caso haja um vazamento nos servidores da empresa, o conteúdo das mensagens não vai ser exposto, preservando a privacidade dos usuários. Quando não há criptografia ponta a ponta e é possível instalar a conta em outro dispositivo, o invasor pode ter acesso a todas as conversas. Esse é o caso do aplicativo Telegram, que não utiliza esse tipo de criptografia por padrão, apenas em casos específicos, e armazena todas as conversas no seu próprio servidor.

**UMA DICA IMPORTANTE**

Você sabia que quando o seu contato troca de aparelho ou reinstala o Whatsapp, a chave de criptografia da conversa entre vocês também muda? Você pode configurar o aplicativo para te avisar sempre que isso acontecer (veja na seção "Como ativar a criptografia"). Essa ferramenta é importante porque serve para identificar também quando uma conta foi roubada. Sempre que você ver essa mensagem, vale confirmar a identidade da pessoa com quem você está conversando utilizando um outro canal de comunicação, como uma ligação de vídeo.

PARA SABER MAIS



ENTENDA COMO FUNCIONA A CRIPTOGRAFIA DE PONTO A PONTO NO WHATSAPP



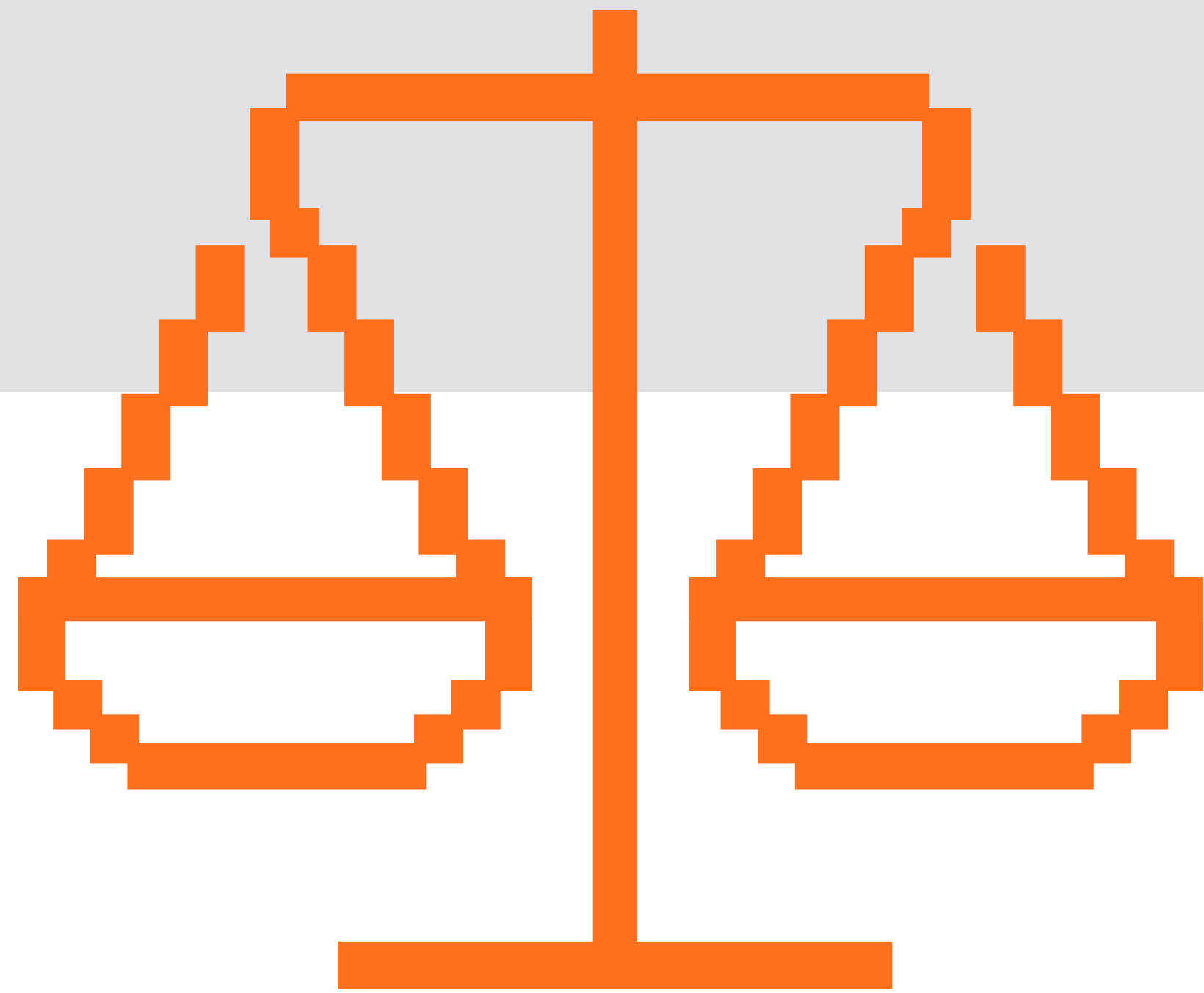
3.4

# DESAFIOS JURÍDICOS NO BRASIL

Assim como em outros países, no Brasil também utiliza-se a criptografia como ferramenta de segurança e para a garantia de privacidade, segurança e a liberdade de expressão. Do ponto de vista legal, a criptografia é citada em algumas normas, sendo recomendada, incentivada ou assegurada sua importância pela Estratégia Nacional de Segurança Cibernética (**Decreto nº10.222/2020**), a Lei Geral de Proteção de Dados (**Lei nº 13.709/2018**), a Política Nacional de Segurança da Informação (**Decreto nº 9.637/2018**), e no decreto regulamentador do Marco Civil da Internet (**Decreto nº 8.771/ 2016**). É importante saber disso porque existem disputas em torno de como e onde a criptografia pode ser utilizada no país. Como tudo o que envolve privacidade e segurança online, o debate é bastante complexo e tem gerado algumas controvérsias.

Um dos exemplos diz respeito ao Whatsapp. Entre 2015 e 2016, decisões judiciais ordenaram o bloqueio nacional do aplicativo porque o Facebook (dona do Whatsapp) havia se recusado a fornecer acesso a mensagens de usuários durante uma investigação criminal. Na época, o Whatsapp alegou que a criptografia de ponta a ponta impedia que a empresa pudesse fornecer as mensagens. Isso fez com que duas ações fossem iniciadas no Supremo Tribunal Federal para determinar se o aplicativo pode ou não ser suspenso. O julgamento foi iniciado em 2020, mas ainda não foi concluído. Você pode entender mais sobre o caso [aqui](#) e [aqui](#).

Esse exemplo reforça a importância de explicar-mos para as pessoas por que a criptografia é uma ferramenta de segurança essencial para o nosso



dia a dia. Ainda que seja importante que as autoridades de justiça possam realizar investigações, inclusive de crimes cometidos na Internet, devemos ter cuidado antes de aceitar que isso aconteça de forma a afetar a segurança de todas as pessoas. Da mesma forma, devemos refletir se bloquear o acesso a um aplicativo tão popular não significaria uma restrição à liberdade de expressão das pessoas.

3.5

# DIREITOS HUMANOS E SERVIÇOS ESSENCIAIS

A criptografia está presente de forma imperceptível aos usuários em diversas atividades praticadas no ambiente online. A segurança de dados é central não só para o sigilo das comunicações e do bem-estar individual, mas também para a estabilidade e continuidade da oferta de produtos e serviços no meio digital, até mesmo da própria conexão à Internet.

Como nos explicou no webinar a Raquel Saraiva, do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.Rec), uma vez que garante a segurança e o sigilo das comunicações, a criptografia é muito utilizada por jornalistas, em apurações delicadas e sigilosas, além de movimentos sociais e grupos vul-neráveis e que geralmente sofrem algum tipo de perseguição, como defensores de direitos huma-nos, grupos feministas e LGBTQ+, entre outros.

Um exemplo é o caso Snowden. Edward Snowden, ex-funcionário da Agência de Segurança Nacional dos Estados Unidos, se utilizou de canais criptografados, como o próprio aplicativo Signal (cujo uso é recomendado por ele), para entrar em contato com os jornalistas Glenn Greenwald e Laura Poitras e fazer a denúncia do programa de vigilância executado pelo governo estadunidense. Snowden buscou a criptografia como forma de proteger suas comunicações com os jornalistas, dada a sensibilidade do conteúdo que ele pretendia compartilhar.

Além disso, a criptografia também está presente e é essencial para serviços de saúde, a fim de proteger dados sensíveis de pacientes e sistemas digitais hospitalares, e para proteger e garantir a estabilidade e a segurança de recursos críticos,

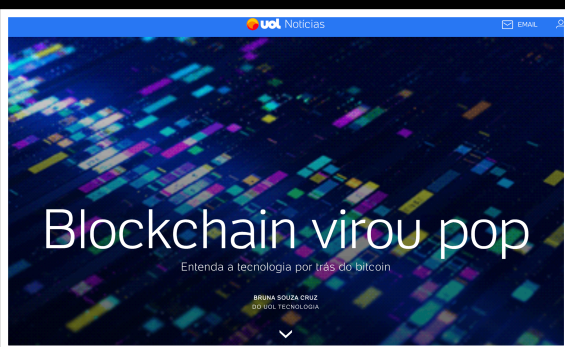
como as redes elétricas. A evolução da Internet e a melhoria dos usos que fazemos precisam da criptografia em muitos níveis, por isso é tão importante termos alguma noção básica sobre o que é e como funcionam. Outro exemplo bem atual de uso da criptografia é nas chamadas “Criptomoedas”, como o Bitcoin e outras. Não à toa, tem “cripto” logo no nome. As moedas digitais são criadas em uma rede blockchain que usa sistemas avançados de criptografia para garantir proteção às transações. Não vamos entrar nos detalhes, mas se quiser saber mais sobre criptomoedas pode começar [aqui](#).

A criptografia pode ser aplicada em dispositivos e aplicações diversas: celular, computador, pen drive, e-mail, aplicativos... Vejamos como usar no dia a dia!

PARA SABER MAIS



PAINEL: CRIPTOGRAFIA, SEGURANÇA E PRIVACIDADE



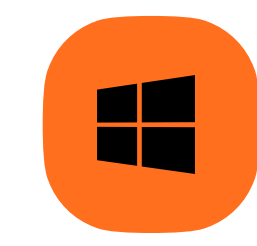
REPORTAGEM SOBRE BLOCKCHAIN

**3.6**

# COMO ATIVAR A CRIPTOGRAFIA

Alguns aplicativos como Whatsapp e Signal já possuem criptografia por padrão.

Confira os caminhos para saber mais e como ativar em outros serviços:



WHATSAPP

SIGNAL

TELEGRAM

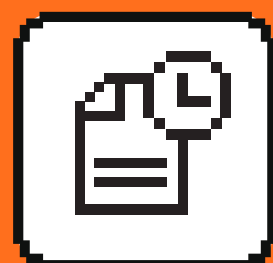
GMAIL

OUTLOOK

WINDOWS

APPLE





AI

## ATIVIDADE 1

Dinâmica com os estudantes utilizando o conceito de “cifrar” uma informação transformando-a em texto codificado.

Aproveitando a temática explorada neste bloco, é possível elaborar uma dinâmica com seus alunos utilizando o conceito de “cifrar” uma informação transformando-a em texto codificado. Esse texto codificado é criado segundo algum algoritmo, que pode ser bem simples ou extremamente complexo (senhas salvas em bases de dados digitais). Como vimos, uma técnica de criptografia mais rudimentar, embora funcional, é a de simples substituição de uma letra do alfabeto deslocada de alguma forma, a chamada “Cifra de César”. O padrão de deslocamento à esquerda de três letras no alfabeto (exemplo: o “A” vira “D”, e o “B” vira “E”) é bem simples e pode gerar uma atividade divertida. Você pode materializar o conceito com os estudantes, tanto em sala de aula como no formato remoto.

É possível variar o deslocamento e criar inúmeras combinações distintas para codificar uma senha/ um texto. Uma proposta é:

**1** Divida a turma em três grupos: os remetentes de uma senha (exemplo de dado sensível), os destinatários da senha (que já conhecem o deslocamento do alfabeto, previamente acertado com os remetentes) e os interceptadores (que podem receber a informação do deslocamento algum tempo depois). O objetivo é decifrar a senha escrita pelos remetentes.

**2** Depois, alterne os grupos!

Para produzir uma ferramenta manual do deslocamento do alfabeto, orientando a criação também por parte dos seus alunos, você pode consultar o vídeo “Entendendo Melhor a Cifra de César”, do canal Erica Villaca, disponível no [link](#). Em meios digitais, você pode acessar o site [rOT13](#) e experimentar cifras a partir de diferentes deslocamentos.

Ao fim da dinâmica, que tal retomar com os alunos a problemática da segurança e da proteção de dados? Algumas perguntas podem orientar a discussão: -

- Existe proteção 100% segura?
- Por que precisamos cuidar dos dados que compartilhamos na rede mesmo usando espaços privados?
- Qual a importância da criptografia no dia a dia?

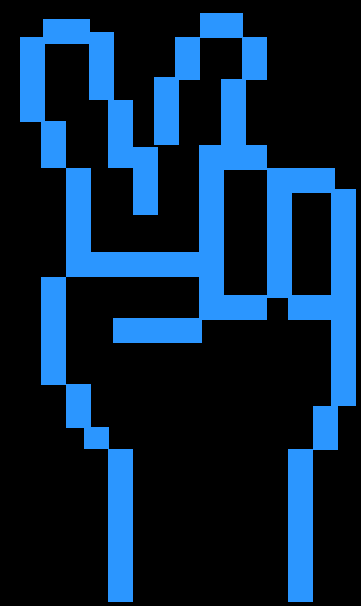
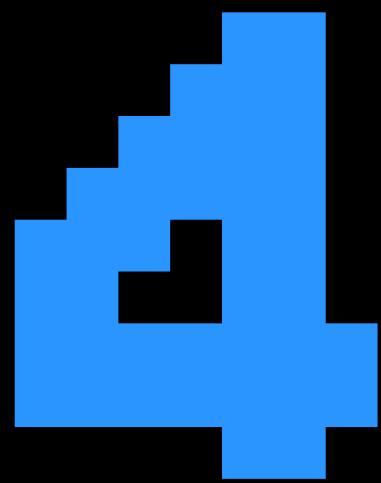
## DICA

MATERIAL COMPLEMENTAR  
PARA A ATIVIDADE:

CONFIRA O PASSO A PASSO EM  
"COMO CODIFICAR E DECODIFICAR  
USANDO A CIFRA DE VIGÈNERE"



CAPÍTULO

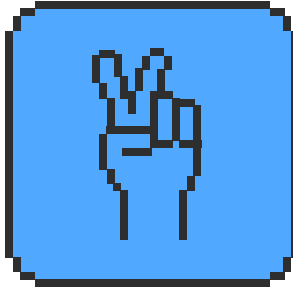


# COMPORTAMENTOS POSITIVOS


Ao falarmos sobre Relacionamentos saudáveis na rede: Respeito, empatia, comportamentos positivos, teremos mais condições de prevenir e e enfrentar a violência online. Destacaremos aqui: Discriminação, cyberbullying, vazamento de imagens íntimas, violência contra mulheres e sextorsão.




### RESUMO



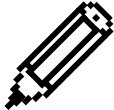

---

 **3 HORAS**

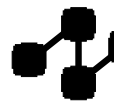
---

 **7 VIDEOS**


---

 **4 SUGESTÃO DE ATIVIDADE**

---

 **3 INFOGRÁFICOS**

A nossa abordagem de comportamentos positivos na rede pode se estender à análise e à discussão de temáticas como direitos humanos, respeito, empatia, justiça, equidade, saúde e combate à violência e à discriminação de qualquer ordem. Elementos transversais e habilidades específicas de diferentes componentes curriculares podem ser trabalhadas.



### PARA ASSISTIR



Webinar com Daniele Fontes, gerente de bem-estar do Facebook, Mariana Valente, diretora do Internet Lab, e mediação de Juliana Alencar.




### PARA SABER MAIS SOBRE O TEMA


Confira uma das muitas campanhas com recursos em vídeo que podem ajudar a realizar atividades pedagógicas com o tema.

**Bullying na Internet**  
Mini videoaula animada para falar de empatia como forma de combate ao bullying.

### PARA APLICAR EM SALA DE AULA

Recursos práticos para usar em sala de aula (remota ou presencial)



**SUGESTÃO DE ATIVIDADES**

**ATIVIDADE 1**  
Exercício sobre Respeito e Empatia

**ATIVIDADE 2**  
Relacionamentos Saudáveis online

**ATIVIDADE 3**  
Como debater sobre Sextorsão

**ATIVIDADE 4**  
Vídeos para debater questões raciais

### OUTROS MATERIAIS COMPLEMENTARES

Confira material extra na versão online da formação para aprofundar seus conhecimentos..

Glossário LGBTQIA+ (UNICEF)

Série de vídeos do #Orgulho Família


Lista de vídeos sobre injustiça racial

Vídeos para falar sobre racismo com crianças

Livro O corpo é código

Artigo Portal Geledés sobre educação antirracista

e muito mais ...



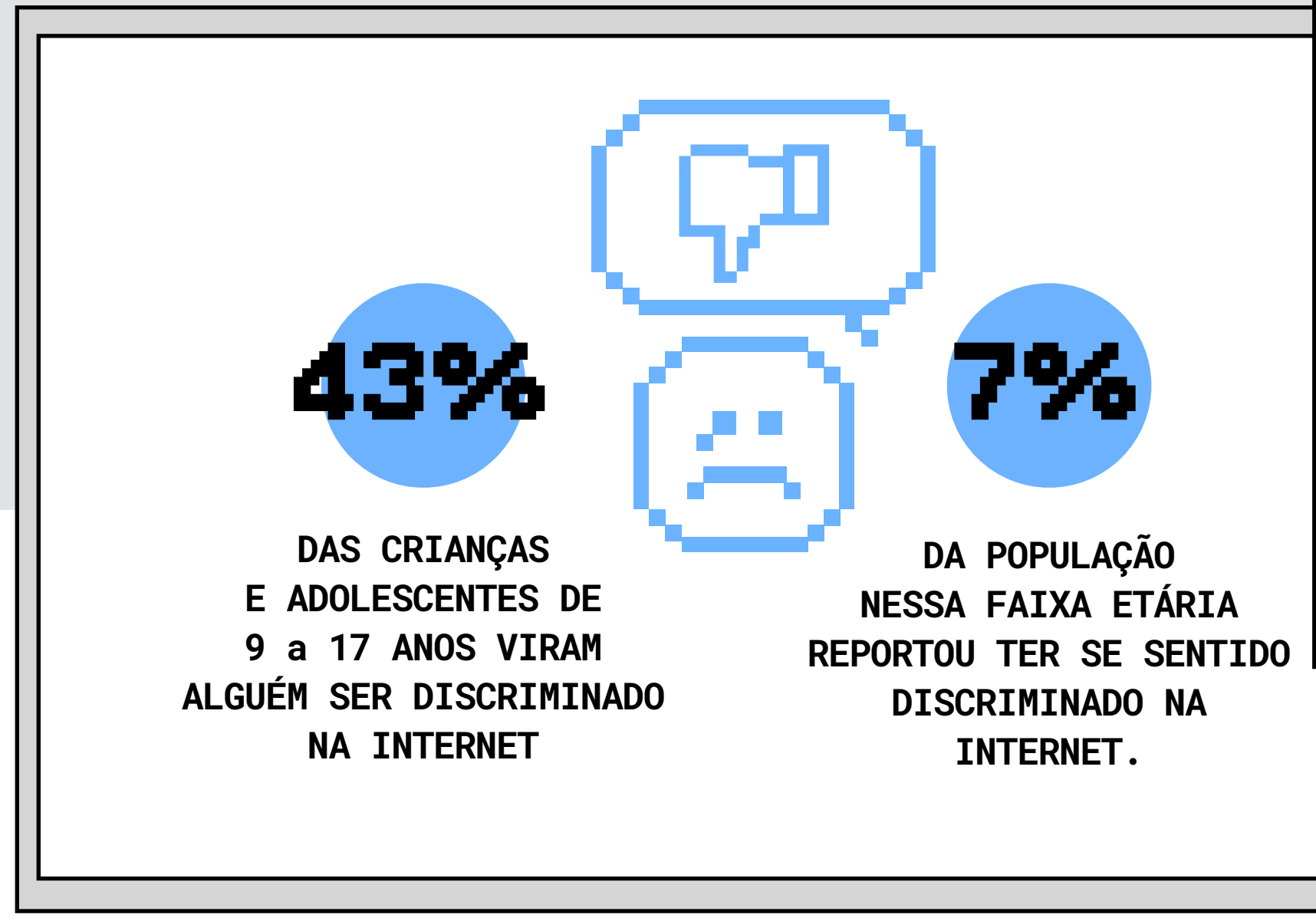
4.1

# CONTEXTO

A experiência online é sempre muito plural e relacionada ao contexto no qual as pessoas vivem. Por isso, tanto as oportunidades de comportamentos positivos quanto as variadas formas de violência e discriminação podem ser encontradas nas redes digitais.

Os dados da pesquisa TIC Kids Online nos ajudam a observar algumas experiências de adolescentes em relação à discriminação:

**Conforme a idade aumenta, testemunhar situações de discriminação torna-se mais frequente, sendo uma experiência relatada por 14% das crianças com idade entre 9 e 10 anos e por 59% dos adolescentes com idade entre 15 e 17 anos** (TIC Kids Online 2019, CETIC.br).

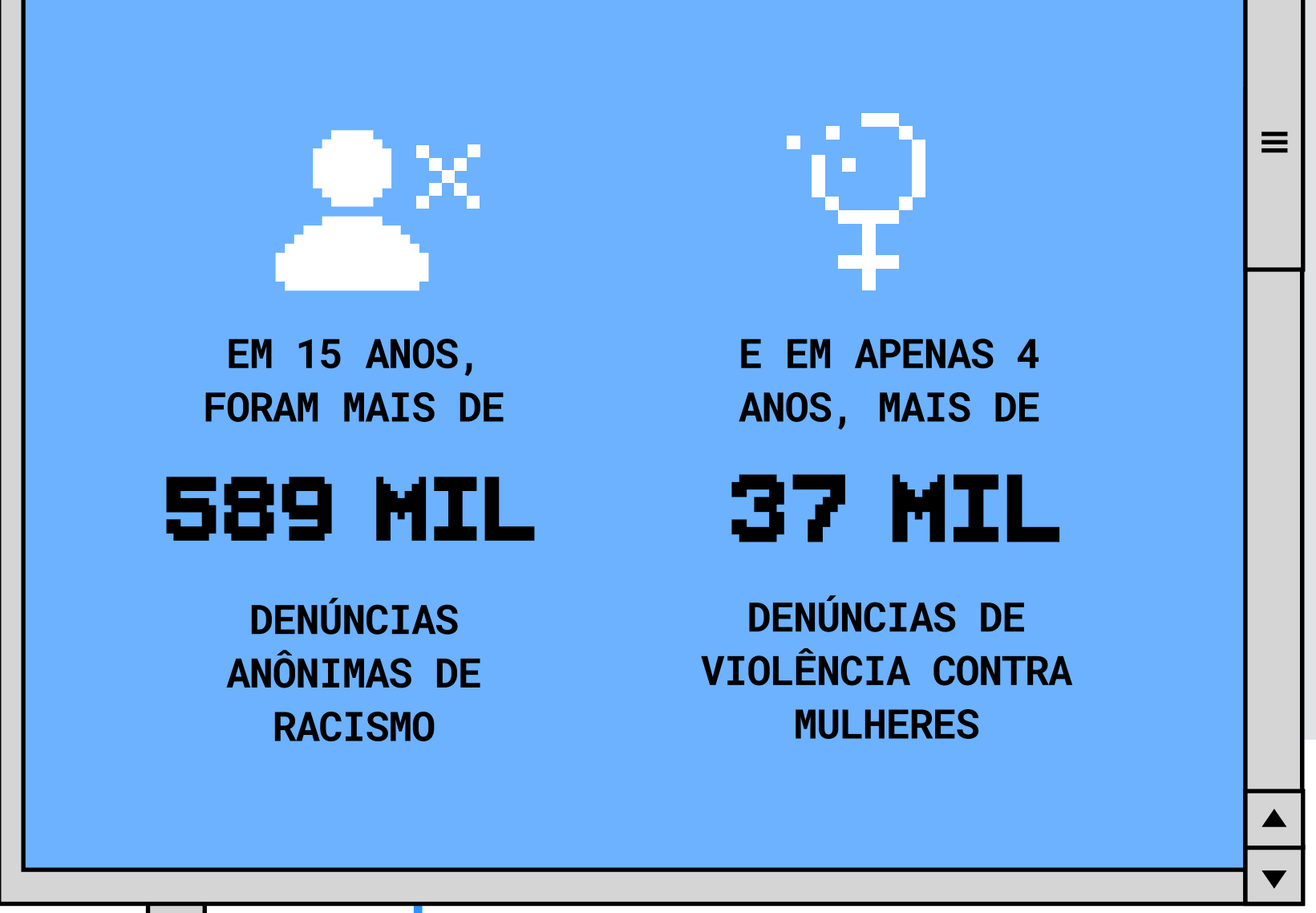


**Os tipos de discriminação mais frequentes refletem as graves desigualdades e violências estruturais presentes em outros ambientes, com destaque para discriminação pela cor da pele (26%), pela aparência física (21%) e por gostar de alguém do mesmo sexo (15%), conforme os dados detalhados da pesquisa.**

Os dados indicam ainda que adolescentes mais velhos e as meninas são tratados de forma ofensiva com maior frequência.

Em geral, as vítimas de ofensas na internet buscam mais os amigos da mesma idade para relatar esse tipo de violência, daí a importância de sensibilizarmos os pares. É preciso dar mais condições para que eles e elas saibam reconhecer as situações de problema para poderem acolher e ajudar a encaminhar os casos graves para adultos de confiança ou para os canais de ajuda apropriados.

Outro aspecto importante para destacar nas atividades de sensibilização com



adolescentes é a mudança de percepção sobre a Internet como "mundo paralelo".

A internet é uma "extensão" da nossa sociedade e combater as violências online também é desafiar estruturas sociais que muitas vezes reforçam discriminações. Discutir estas situações de discriminação e ofensas na rede pode acontecer em sintonia com os debates mais amplos sobre violências no cotidiano.

No **Canal de denúncias da SaferNet**, que recebe denúncias anônimas de páginas suspeitas de violações de direitos humanos na Internet, o racismo, a violência contra mulheres e outras formas de discriminação também estão refletidas.

**4.1 CONTINUAÇÃO**

Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, operada pela Safernet Brasil em parceria com o Ministério Público Federal e a Polícia Federal, tiveram aumento de mais de 100% em 2020, com total de 156.692 denúncias, frente a 75.428 no ano anterior. Entre os principais tópicos denunciados estão racismo, homofobia, apologia e incitação a crimes contra a vida e pornografia infantil. **Os dados de 2020 tiveram um salto no contexto da pandemia do COVID-19**, o que exige ainda mais esforços de educação e prevenção para proteção de crianças e adolescentes nas redes.

No **Canal de Ajuda da SaferNet**, em 2020, os dois principais temas dos pedidos foram justamente relacionados às agressões à dignidade sexual e ao Bullying ou Discriminação. A violência de gênero é muito marcada na exposição de

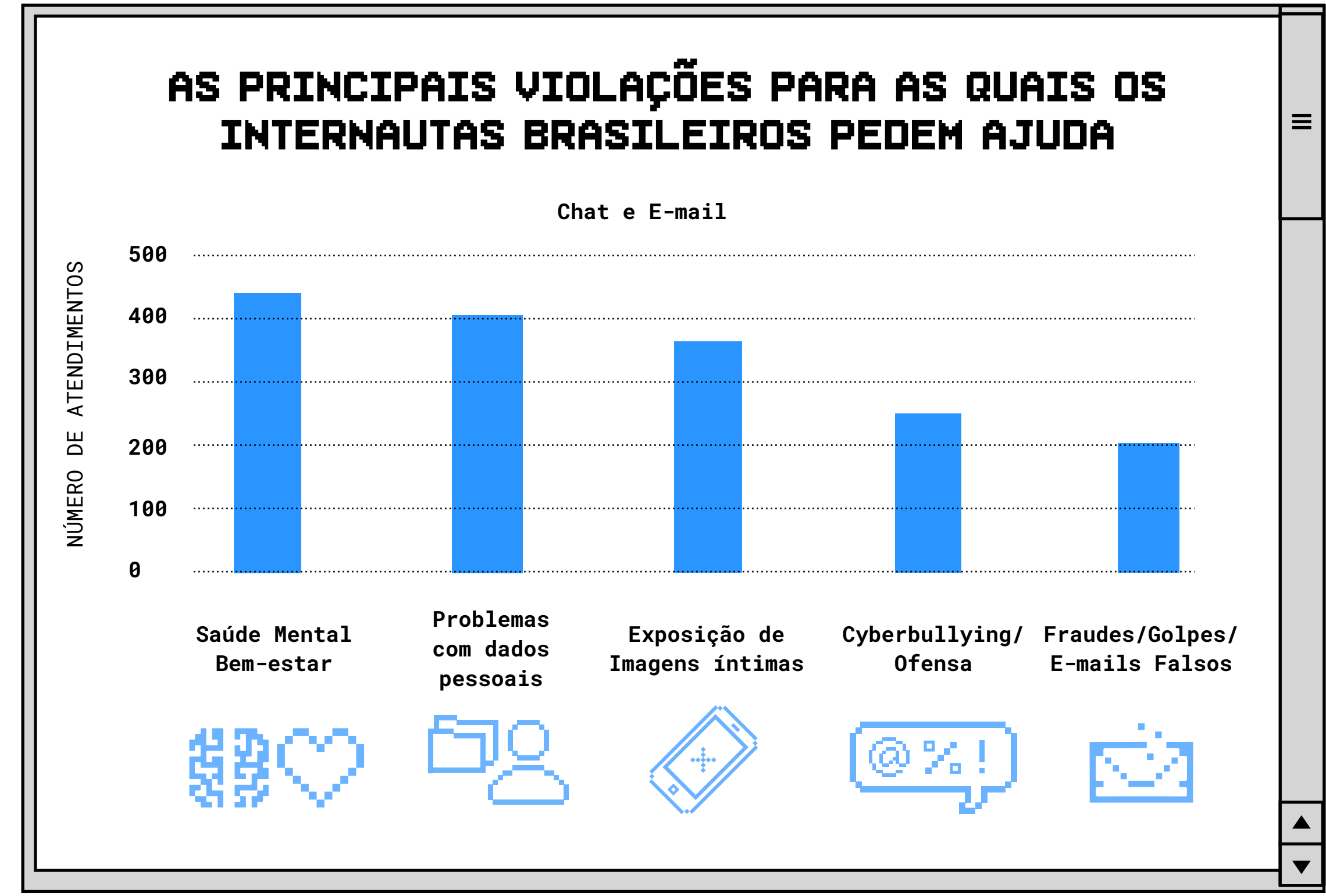
imagens íntimas (“nudes”). Ainda que o compartilhamento sem autorização destes conteúdos possa ocorrer com qualquer pessoa, as meninas e as mulheres são muito mais vítimas já que a sua liberdade sexual é sistematicamente violentada.

No **Relatório Violência de gênero na Internet** realizado pelo Internet Lab, há dados e análise que ajudam a entender esta violência na rede.

Na publicação **Dinâmicas de gênero no uso das Tecnologias Digitais**, é possível conhecer os resultados sobre a transversalidade da raça e do gênero no uso das TIC, e o papel das TIC com relação a questões de identidade de gênero e sexualidade. Os grupos focais e entrevistas com adolescentes ajudam a compreender como representam suas próprias experiências e vivências. As desigualdades na mediação parental e a culpabilização por situações de exposição, por exemplo, são muito marcantes na vida das meninas participantes, ressaltando a necessidade de uma postura mais crítica para não perpetuar estas violências.

Para fechar esta rodada de contexto e de dados que nos ajudam a compreender algumas das dimensões das violências online, vale olhar para os indicadores apontados no Webinar sobre a remoção de conteúdos nas plataformas digitais. É importante conhecer os dados das ações que efetivamente as plataformas digitais

tomam para remover conteúdos violentos. No caso do Facebook e do Instagram, o **relatório de transparência** sobre remoções de conteúdos que violam as políticas das comunidades traz dados específicos sobre conteúdos relacionados aos **Padrões da Comunidade para Bullying e Assédio**.



4.2

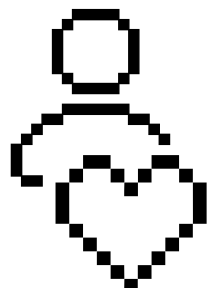
# RESPEITO E EMPATIA

No programa Cidadão Digital acreditamos que estimular os comportamentos positivos é um caminho vital para enfrentar as várias formas de violência que acontecem também online. No Webinar destacamos como formas de violência online mais comuns entre adolescentes o cyberbullying, a discriminação e o compartilhamento de imagens íntimas sem autorização.

Apostamos que, para além de informar todo mundo sobre como denunciar e solicitar remoção de conteúdos violentos, **é urgente atuar na promoção de uma postura mais positiva, com mais respeito e empatia, estimulando relacionamentos saudáveis online.** Nas atividades com adolescentes, valorizar os comportamentos positivos ajuda a evitar o “bloqueio automático” que muitos fazem ao discurso adulto de restrição e punição. Esse tipo de discurso geralmente é o que

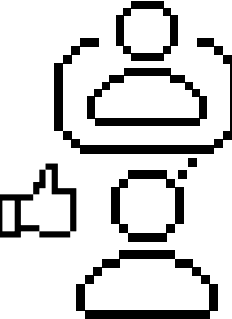
vem com uma lista enorme de leis sem contexto e regras de comportamento que não se conectam com a experiência online cotidiana. Por isso a necessidade, também, de buscarmos formas alternativas de trazer a discussão, investindo em ações que também deem voz às e aos adolescentes.

Começando pelo bullying na Internet, o chamado **ciberbullying**, nosso desafio é quebrar o silêncio de quem sofre, além de “ativar” aqueles que assistem passivos e que, de alguma forma, deixam a violência rolar — as chamadas “testemunhas” ou audiências. Na rede é a galera que visualiza, compartilha e comenta, ainda que em conversas privadas, mas que não ajudam a interromper o ciclo da violência nem oferecem apoio às vítimas. Algumas ficam em silêncio por medo, outras por não gostarem da vítima ou por indiferença. Empatia é a chave aqui. Seja qual for a posição de quem está assistindo.



**EMPATIA**

Capacidade de identificar e compreender as emoções de outras pessoas, de imaginar o que alguém pode estar sentindo.



**SIMPATIA**

Sentir pelo outro em vez de sentir com ele, ou ainda sentir e pensar de forma parecida, ter afinidade com alguém.

**4.2 CONTINUAÇÃO**

Na Campanha Acabar com o Bullying #ÉdaMinhaConta, criada pelo Instagram + SaferNet + Unicef, há cards, stories, vídeos do **IGTV** e um infográfico para ajudar a quebrar o ciclo do silêncio nas agressões, e estimular mais respeito e empatia nas interações pelas redes.

Vale conferir o **infográfico** com o passo a passo para os diferentes atores envolvidos. Sim, quem só vê também participa, e precisa assumir isso — sem se colocar em risco, claro ;) O Infográfico pode estimular exercícios interessantes nas escolas, pensando inclusive em detalhar situações que não estão descritas ali mas que acontecem no dia a dia. A campanha contou, ainda, com uma série de conversas no IGTV com participação artistas e influencers. Xuxa recebeu convidados para falar do #ÉdaMinhaConta debatendo a importância da resiliência, da empatia, das redes de apoio, de quebrar o silêncio e muito mais. Vale assistir no link ao lado.

E para ajudar a diferenciar brincadeira de violência, vale conferir o super vídeo criado com a embaixado-



ra do Cidadão Digital em 2020, mentora em 2021, Jade Christine puxando uma direta que pode iniciar atividades com estudantes de diferentes idades.

No final, o importante é conseguir estimular mais respeito e empatia, sensibilizando para que todo mundo reconheça o valor da diversidade. Mais do que “respeitar” o diferente, podemos perceber o incrível valor e privilégio de poder conviver com pessoas diferentes e ter contato com realidades plurais, dentro e fora das redes. E se tem uma coisa que a Internet pode favorecer, é o contato com pessoas e conteúdos plurais. Se fizermos isso com empatia, melhor serão nossas experiências e ainda melhor será a própria Internet.

**VIDEO**



**MINI AULA DESCONTRAÍDA SOBRE TEMA**

**CAMPANHA #ÉDAMINHACONTA**

**INFOGRÁFICO**



**PASSO A PASSO PARA ENTENDER AS DIFERENTES PARTICIPAÇÕES NO BULLYING**

**IGTV**



**VÍDEOS EMOCIONANTES COM PERSONALIDADES COMPARTILHANDO SUAS HISTÓRIAS**

## 4.2 CONTINUAÇÃO



Ah sim, conhecer a lei é importante. O desafio é justamente não banalizar o bullying como uma forma de “brincadeira” entre crianças ou adolescentes, tampouco ignorar os danos que podem ser causados à saúde mental das vítimas. O problema nunca é individual (só da vítima ou só do agressor), porque o bullying cria um ambiente de convivência tóxico na escola e prejudica a todos e todas.

Ao mesmo tempo, não nos parece saudável e nem pedagógico judicializar todas as situações de conflitos entre crianças e adolescentes. O efeito colateral da judicialização pode ser muito prejudicial, inclusive para as vítimas e seus familiares.

Em 2015 foi criada a lei que obriga todas as instituições de ensino a terem ações sistemáticas de prevenção ao bullying e ao cyberbullying. A **Lei 13.185/2015** concentra os esforços na prevenção e não na punição. Um ponto importante é que ela define o entendimento sobre Bullying como violência sistemática. Ou seja, não ajuda se tudo for chamado de bullying: piadas, zoeiras, brincadeira, sem especificar a violência.

**§ 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática ( bullying ) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas.**

**Nos casos mais graves de bullying, e nos casos de discriminação previstos em lei, as e os adolescentes (acima de 12 anos) respondem na justiça pelos atos**

**infracionais equivalentes aos crimes previstos em lei.** Quando as violências são praticadas por crianças menores de 12 anos, os responsáveis legais podem ser condenados na justiça especializada. Mesmo nos casos graves que podem ser judicializados, não podemos perder de vista o objetivo principal: educar para a convivência pacífica e ética, e isso precisa valer também para a Internet.

Ou seja, bullying ou cyberbullying em si não são um tipo de crime, mas as atitudes específicas podem sim ser enquadradas como crimes ou atos infracionais, independentemente de acontecerem dentro ou fora da Internet. Um exemplo são os chamados crimes contra a honra (calúnia, difamação e injúria), que você pode ver na imagem abaixo. O mesmo podemos falar sobre bullying ou cyberbullying com motivação racista e que podem ser enquadrados como injúria racial (**Artigo 140, parágrafo parágrafo 3º, do Código Penal**), ou racismo (**Lei nº 7.716/1989**). Importante lembrar que, no âmbito da lei, injúria racial/racismo dizem respeito não apenas à cor da pele das

pessoas, mas também etnia, religião, origem, condição de pessoa idosa ou com deficiência.

Desde 2019, por entendimento do Supremo Tribunal Federal, a lei que pune o racismo também protege pessoas contra discriminação motivada por orientação sexual ou identidade de gênero. Vale lembrar ainda que alguns tipos de discriminação podem estar associados ao cyberbullying, mas toda e qualquer discriminação por questões de raça, etnia, orientação sexual ou religiosa pode ser considerada crime independentemente de ser repetitiva/sistemática. Mensagens de ódio e discriminação podem ser chamadas pelos nomes diretamente: **racismo**, **homofobia**, **misoginia** e os responsáveis respondem judicialmente pelos atos. Para facilitar a diferenciação dos casos de ofensas e bullying dos casos mais específicos relacionados aos crimes de ódio, vale conferir o infográfico do projeto **SaferLab** da SaferNet, bem como o **Guia de produção de contra-narrativas** que provoca a construção de diálogos sem alimentar a polarização.



**4.2 CONTINUAÇÃO**

Na mesma lógica do que vimos com o bullying, apostamos que estimular relacionamentos positivos e saudáveis é uma forma importante de enfrentar os relacionamentos tóxicos e abusivos por trás da maior parte dos casos de exposição íntima sem autorização na Internet.

Os casos de exposição íntima sem consentimento têm sido destaque nos pedidos de ajuda que chegam nos canais de ajuda da SaferNet. Os materiais da campanha **#PareaSextorsão**, criada pela Thorn com apoio do Facebook e realizada no Brasil pela SaferNet, ajudam a debater este tema com adolescentes, explicando o que é Sextorsão e sinalizando caminhos para fortalecer a rede de apoio às vítimas (que geralmente são revitimizadas ao serem consideradas culpadas ao invés de vítimas).

**LEI SOBRE EXPOSIÇÃO DE CONTEÚDO ÍNTIMO NÃO AUTORIZADO**

O Marco Civil da Internet (**Lei nº 12.965 / 2014**), no Art. 21 estabelece uma importante exceção para remoção de conteúdos da Internet sem ordem judicial: quando o conteúdo expõe a intimidade de uma pessoa. Nesses casos, basta que a vítima solicite diretamente à plataforma. Caso um provedor de aplicações de Internet (uma plataforma de rede social, por exemplo) não retire um conteúdo íntimo após a solicitação direta da pessoa atingida, esse provedor pode ser responsabilizado judicialmente.

Pela nova redação do Código Penal, alterada pela **Lei 13.718/2018**, esse tipo de exposição não consentida passou a ser crime:

**Art. 218-C - “Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia”**

O simples registro de conteúdo íntimo sem consentimento já é considerado crime pela **Lei nº 13.772**, de 2018, que também alterou o Código Penal:

**Art. 216-B - Registro não autorizado da intimidade sexual.**

No site da campanha **#PareaSextorsão** há ainda recursos para usar com **educadores** e **pais**, sabendo que há ainda muito tabu para falar da liberdade sexual de adolescentes e jovens, especialmente com as meninas. No **Infográfico** criado pela SaferNet, há um passo a passo para solicitar remoção de conteúdos íntimos da Internet.

**CAMPANHA #PAREASEXTORSÃO**

VIDEO

INFOGRÁFICO



**A IMPORTÂNCIA DE QUEBRAR O SILÊNCIO E MONTAR REDES DE APOIO #NÃOÉSUASULPA**



**PASSO A PASSO SOBRE COMO REPORTAR E SOLICITAR REMOÇÃO DE CONTEÚDO ÍNTIMO**

**4.2 CONTINUAÇÃO**

É essencial divulgar esse processo, porque, em muitos casos, o desconhecimento sobre o que fazer gera ainda mais angústia nas vítimas. Quando as imagens envolvem menores de 18 anos, estamos diante de casos de Pornografia Infantil, crime grave previsto no artigo 241 do Estatuto da Criança e do Adolescente.

O Guia Sem meu consentimento, criado pelo Facebook para orientar sobre o que fazer em casos de exposição não autorizada na plataforma, é também uma leitura importante para sabermos lidar com situações de ameaça de exposição sem consentimento.

**NOVA LEI DE PERSEGUIÇÃO E STALKING**

Em 2021, tivemos a aprovação de uma nova lei no Brasil que pune especifica-

mente perseguições, inclusive online. Na internet, esse tipo de conduta é conhecida como stalking, do inglês “perseguição”. A Lei nº 14.132/2021 tipifica o crime de perseguição como:

**Artigo 147-A do Código Penal**  
**Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.**

Importante lembrar que, para ser considerada perseguição, as condutas da pessoa agressora devem ser reiteradas, ou seja, acontecer mais de uma vez, de forma consecutiva. Nos casos online, podemos pensar, por exemplo, no envio constante de mensagens ou conteúdos

indesejados, postagens expondo o nome da vítima ou ligações indesejadas.

**VIOLÊNCIA CONTRA MENINAS E MULHERES**

Fortalecer as redes de proteção e apoio contra a violência online é urgente. Conhecer os tipos de violência mais comuns que atingem meninas e mulheres na internet e as leis que protegem as vítimas é um caminho que a SaferNet adotou no Guia Meninas em rede, criado com o apoio do Unicef Brasil. Além de mostrar um passo a passo para amigas/os, pais, mães e educadoras/es sobre o que fazer caso seja ou conheça alguma menina que tenha sido alvo de alguma violência desse tipo.

O guia ainda traz sugestões de atividades para que você aprenda a fazer um mapeamento e um plano de ação para



**COMO AGIR EM RESPOSTA AO COMPARTILHAMENTO DE IMAGENS ÍNTIMAS SEM PERMISSÃO**



**GUIA PODEROSO PARA FORTALECIMENTO DE REDES DE PROTEÇÃO**

4.2 CONTINUAÇÃO

fortalecer as redes locais de proteção e apoio. O Guia “Meninas em Rede” pode ser uma ferramenta poderosa para inspirar ações com os estudantes, estimulando ações concretas além da tomada de consciência.

Um outro recurso poderoso para iniciarmos boas reflexões é o vídeo da série feita com os embaixadores jovens do Programa Cidadão Digital para debater o compartilhamento não autorizado de imagens íntimas em 2020. Neste episódio, a discussão ajuda a enfrentar o tabu em torno do tema e a destacar dicas de proteção.

Já o Projeto Caretas, experiência de interação online desenvolvida pelo Unicef no Brasil, em parceria com as empresas Sherpas e Chat-Tonic, o Facebook e a

Safernet, usa inteligência artificial para criar uma das primeiras peças de ficção sobre o tema por meio do storytelling. Nele, Fabi Grossi, uma personagem fictícia, interage com adolescentes e jovens entre 13 e 24 anos por um chat na internet, e a história avança segundo essas interações. Confira como funciona participando da experiência.

WEBNAR



PROJETO CARETAS



MINI AULA ANIMADA SOBRE TEMA

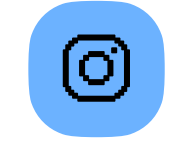


UMA EXPERIÊNCIA ENTRE A FICÇÃO E A REALIDADE PARA SENSIBILIZAÇÃO

4.3

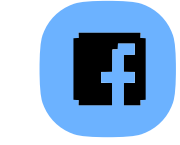
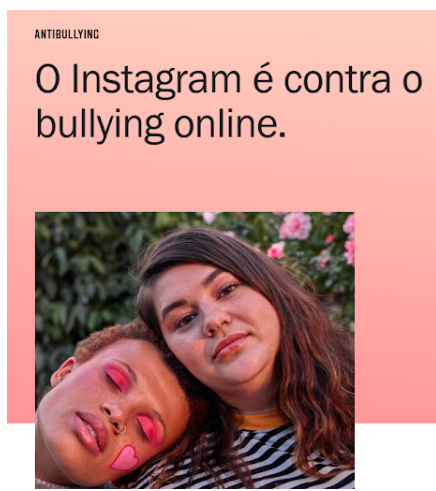
# FERRAMENTAS

Agora que vimos alguns dados e exemplos de materiais de apoio, vamos falar de ferramentas que ajudam a lidar com o tema na prática.



### INSTAGRAM

Central com recursos de segurança do Instagram. É possível filtrar comentários, #, palavras e pessoas. Além de bloquear e denunciar, é possível restringir contatos e ainda selecionar quem pode entrar e contato via mensagens diretas.



### FACEBOOK

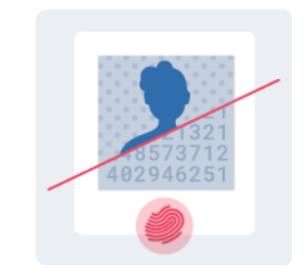
Central de prevenção ao Bullying do Facebook. Recursos de apoio aos jovens, educadores e famílias.



Se você está sofrendo bullying



Projeto Piloto do Facebook que usa tecnologia para prevenção ao compartilhamento de imagens íntimas na rede. Entenda como funciona.

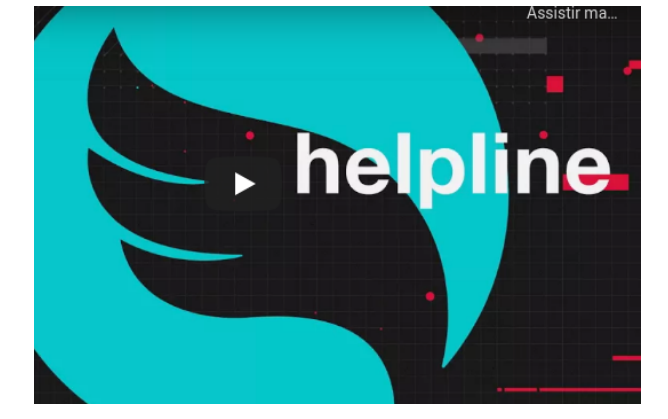


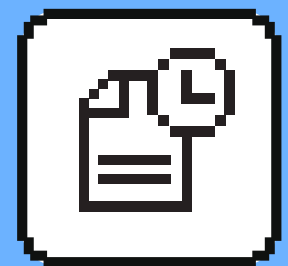
Piloto sobre imagens íntimas compartilhadas sem permissão



### HELPLINE

Canal de Ajuda da SaferNet que orienta estudantes, educadores e famílias sobre como enfrentar violências na Internet.





**A1**

**ATIVIDADE 1**

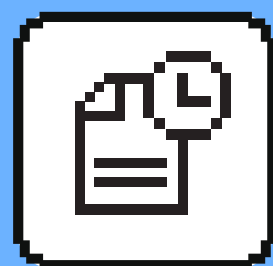
O Guia Cidadão Digital (páginas 24 a 37), traz sugestões de atividades presenciais que podem ser adaptadas para o contexto remoto. Há uma sugestão de Palestra e 2 atividades em grupo para debater cada um dos temas:

- 1. Respeito e Empatia (p. 24 a 30) e
- 2. Relacionamentos Saudáveis (p. 31 a 37).

**GUIA CIDADÃO DIGITAL**

**COMPORTAMENTO POSITIVO  
RESPEITO  
E EMPATIA**

**COMPORTAMENTO POSITIVO  
RELACIONAMENTOS  
SAUDÁVEIS ONLINE**



A2

ATIVIDADE 2

Sugestão de atividade da Biblioteca de alfabetização digital do Facebook que pode ser adaptada e ajuda a pensar outras atividades sobre a forma como nos relacionamos com outras pessoas pela Internet. Quais diferenças? Quais vantagens? E quais os riscos?



Biblioteca de Alfabetização Digital

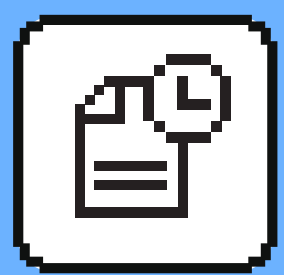
Comportamento positivo

# Relacionamentos saudáveis online

De [Youth & Media](#)

Iniciar esta lição

Baixar pacote de lições



A3

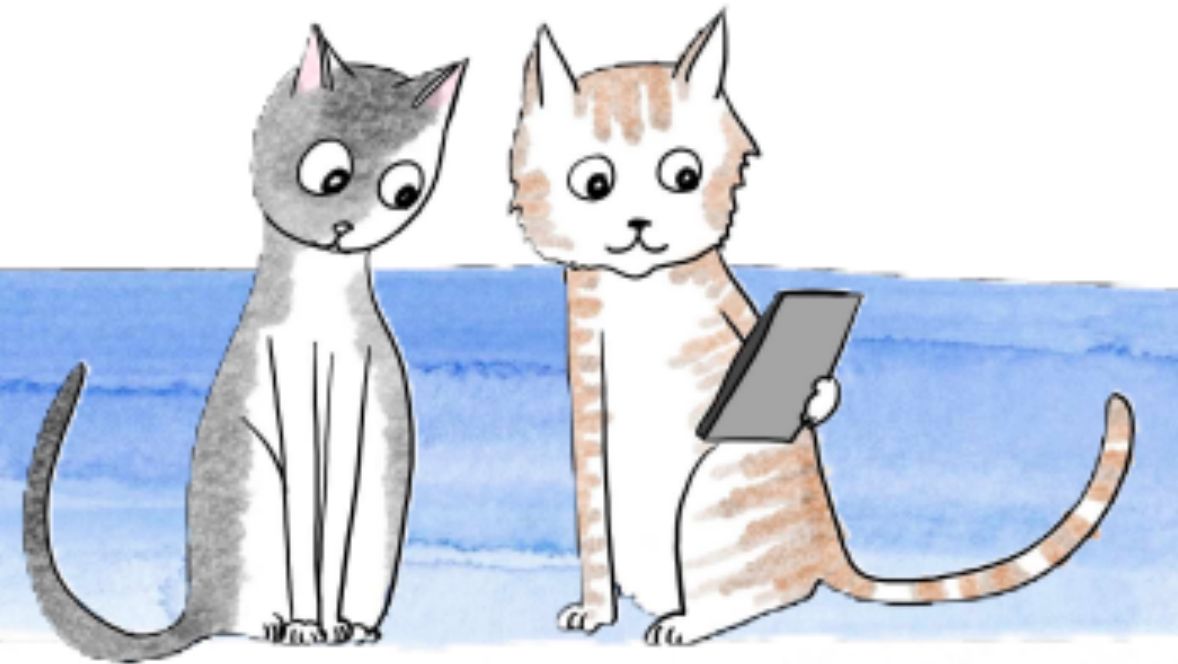
ATIVIDADE 3

### Como debater sobre Sextorsão

Sugestão de atividade da campanha #PareaSextorsão. Uma forma descontraída e segura para falar de temas sensíveis e romper com o ciclo de revitimização.



# PARA EDUCADORES SEXTORSÃO.

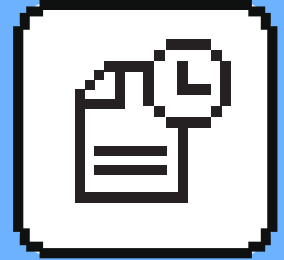


“

PODERÍAMOS TRAZER O TEMA PARA A ESCOLA. FALAR SOBRE ESTE ASSUNTO IMPORTANTE QUE NÃO É SUPER PESADO E NÃO FARIA MAL PARA A TURMA. SERIA VALIOSO PARA OS ORIENTADORES.

- Adolescente, conselho jovem Thorn / EUA

”



A4

ATIVIDADE 4

Vídeos para debater questões raciais

Curadoria de vídeos do Youtube para trabalhar no contexto educacional. Seleção de 70 vídeos feito pelas jovens do coletivo Adélias e uma das equipes vencedoras do programa SaferLab da SaferNet Brasil.

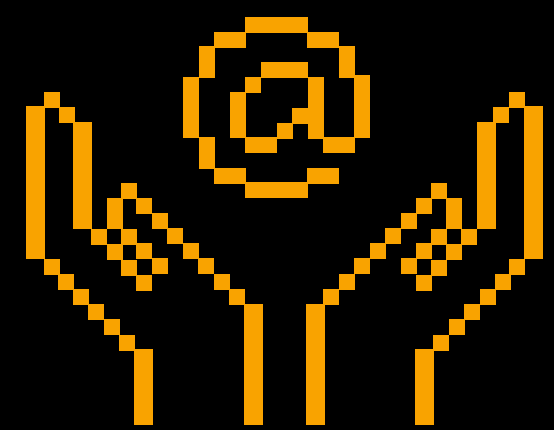




CAPÍTULO

# 5

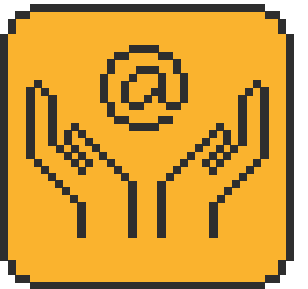
# AUTOCUIDADO ONLINE




Vamos entender a importância de pensar o bem-estar e a saúde mental nas nossas rotinas digitais. Apresentaremos alguns conceitos e campanhas que podem inspirar você. Também gostaríamos que você utilizasse esses materiais para o seu próprio autocuidado. Afinal, precisamos estar bem e saudáveis para podermos ajudar outras pessoas, certo?




**RESUMO**



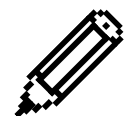

---

 **3 HORAS**


---

 **8 VIDEOS**


---

 **4 SUGESTÃO DE ATIVIDADE**

---

 **1 INFOGRÁFICO**

Ao enfatizar o autocuidado, podemos desenvolver um rico trabalho com aspectos da saúde emocional, mental e física, aliando competências sociais, relacionais e cognitivas na direção da busca do bem-estar. Podemos mobilizar habilidades nas áreas de linguagens com a expressão pessoal e muitas competências gerais previstas.



**PARA ASSISTIR**

Webinar com Karen Scavacini, psicóloga fundadora do Vita Alere, Gabriel Recalde, gerente de políticas públicas do Instagram e mediação de Guilherme Alves, gerente de projetos na SaferNet.




**PARA SABER MAIS SOBRE O TEMA**

Campanhas com recursos em vídeo que podem ajudar a realizar atividades pedagógicas com o tema.

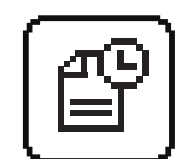
**Autocuidado e Saúde Emocional**

Mini videoaula animada para falar de saúde mental e autocuidado nas redes.




**PARA APLICAR EM SALA DE AULA**

Recursos práticos para usar em sala de aula (remota ou presencial)



**SUGESTÃO DE ATIVIDADES**

**ATIVIDADE 1**

Playlist do Autocuidado

**ATIVIDADE 2**

O que fazemos para nos sentirmos bem nas redes?

**ATIVIDADE 3**

Roteiro de Co-criação

**ATIVIDADE 4**

Roteiro de Co-criação

**OUTROS MATERIAIS COMPLEMENTARES**

[Confira material extra na versão online da formação](#) para aprofundar seus conhecimentos.


Conferência sobre Bem-estar na era digital com a pesquisadora de Harvard, Sandra Cortesi.

Série bem-estar criada pelo Portal Nova Escola

Guia de saúde mental para educadores da Nova Escola

Alerta da SaferNet sobre desafios violentos (“Momo”)

Recursos de apoio para debater séries violentas



**5.1**

# CONTEXTO

Segundo a Organização Mundial de Saúde, a compreensão sobre saúde não pode ser limitada à ausência de doenças. O mesmo vale para o entendimento sobre Saúde Mental: **um estado de bem-estar no qual a pessoa percebe suas próprias habilidades, pode lidar com os estresses cotidianos, pode trabalhar produtivamente e é capaz de contribuir para sua comunidade (OMS).**






Esses aspectos positivos e preventivos da promoção de saúde mental também podem ser aplicados aos ambientes digitais. E da mesma forma como temos as situações de vulnerabilidade e que podem causar danos na Internet, há possibilidades de conexão com redes de apoio, conteúdos inspiradores de com-

portamentos saudáveis e com oportunidades para estimular o desenvolvimento de habilidades para a vida.

Os **dados da pesquisa TIC Kids Online 2019** (indicador G18) apontam que um número considerável de adolescentes relatam ter tido contato com conteúdos online que podem causar desconforto. O contato com conteúdos sensíveis que podem estar relacionados ao autodano é bem expressivo, especialmente para as meninas.

### AUTODANO E CONTEÚDOS SENSÍVEIS\*

% DE CRIANÇAS E ADOLESCENTES DE 11 a 17 ANOS USUÁRIOS DA INTERNET

	TOTAL	MASCULINO	FEMININO
 CENAS DE VIOLÊNCIA OU COM MUITO SANGUE	22	17	27
 FORMAS PARA FICAR MUITO MAGRO	15	10	21
 FORMAS DE COMETER SUICÍDIO	15	9	22
 FORMAS DE MACHUCAR A SI MESMO	12	7	18
 EXPERIÊNCIAS OU USO DE DROGAS	10	8	13

### SITUAÇÕES VIVENCIADAS AO USAR A INTERNET NOS ÚLTIMOS 12 MESES

% DE CRIANÇAS E ADOLESCENTES DE 11 a 17 ANOS USUÁRIOS DA INTERNET (2019)

Tentei passar menos tempo na internet, mas não consegui	25
Passei menos tempo que devia com a minha família, amigos ou fazendo lição de casa porque fiquei muito tempo na Internet	24
Me peguei navegando na Internet sem estar realmente interessado (a) no que via	21
Me senti mal em algum momento por não estar na Internet	21
Deixei de comer ou dormir por causa da Internet	20

Mas precisamos destacar que nem todo o contato com estes conteúdos está diretamente associado a situações graves. Muitas/os adolescentes podem acessar por curiosidade, na busca de informação para ajudar alguém, para trabalhos escolares e não obrigatoriamente para si própria/o. A pesquisa pergunta se as/os adolescentes viram esse tipo de material, que muitas vezes é recebido de outras pessoas ou até mesmo de notícias que circulam nas redes.

Outro ponto destacado pelo próprio público adolescente é que nem sempre elas e eles conseguem **controlar seu uso** como gostariam.

Os prejuízos no sono, na qualidade da alimentação e mesmo nas relações sociais são alguns dos problemas relacionados ao uso excessivo e problemático. Vale destacar que isso é bem diferente de “vício” ou “dependência”.

**5.1 CONTINUAÇÃO**

O desafio das ações educativas é debater com as e os adolescentes sobre esses temas de forma aberta e propositiva. Ou seja: não adianta só dizer que usar “muito” a Internet é prejudicial, ou que não devemos acessar “certos tipos” de conteúdo. É preciso abrir espaço para que esse público possa falar sobre o que sente e o que o motiva a certos comportamentos, para então aconselhar e propor alternativas mais saudáveis. Sabendo quais são os riscos e os potenciais danos, elas e eles vão saber o que fazer quando precisarem de ajuda ou quando precisarem ajudar alguém. Informar e orientar para que as pessoas saibam reagir ao risco e tomar uma atitude que não gere dano é nossa missão no Cidadão Digital, neste e nos outros temas.


**ALERTA**

Evitamos usar os termos “vício” e “dependência” pois eles dependem de uma avaliação médico-psicológica para que o diagnóstico seja realizado nos casos extremos. Há muita controvérsia nas evidências científicas, ainda que haja uma nova classificação médica para uso compulsivo de jogos eletrônicos. Aqui falamos de uso excessivo, problemático ou empobrecido para destacar que há alternativas de qualificar o repertório de uso. Ou seja, é possível entender quando um uso é positivo ou não, e ter consciência disso é essencial para o bem-estar nas redes.

Estimular os comportamentos positivos visando o autocuidado passa também por conhecer as situações de problema mais severas, para que possamos minimizar os danos e concentrar nas oportunidades. Do ponto de vista da saúde mental, não são poucos os casos de conteúdos online que fazem apologia ao suicídio, tema cada vez

mais relevante na adolescência e juventude. **Os dados do Ministério da Saúde** apontam que os casos de violência auto-provocada entre adolescentes e jovens (15 a 29 anos) vêm aumentando no Brasil.

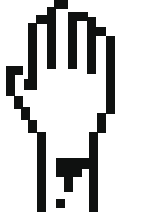
Os óbitos por suicídio entre adolescentes e jovens na população indígena é ainda mais preocupante, segundo dados do **Boletim Epidemiológico nº 37** publicado pela Secretaria de Vigilância em Saúde do Ministério da Saúde em 2020. Ao endereçar o tema de violência autoprovocada — como suicídio e autolesão — precisamos sempre tratar a discussão com seriedade e empatia, mas evitando abordagens alar-



**AUTOLESÃO**

Dano intencional ao próprio corpo, com a intenção de aliviar sentimentos negativos ou punir-se, por exemplo. É diferente do comportamento suicida porque não tem a intenção de causar a própria morte. Envolve cortes, queimaduras, arranhões e socos autodirigidos, isto é, está ligada ao dano intencional sobre a pele.

GRANDCLERC, et.al., 2016; GIUSTI, 2013



**VIOLÊNCIA AUTOPROVOCADA**

Qualquer comportamento intencional associado à dor e ao sofrimento emocional, cuja finalidade abarque alívio, autopunição ou morte.

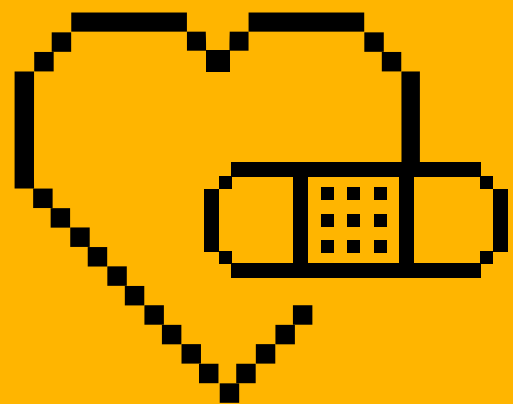
## 5.1 CONTINUAÇÃO

mistas que podem acabar contribuindo para um tabu ainda maior sobre o tema. Estimular o diálogo, ou seja, ouvir o que as e os adolescentes pensam sobre o tema, é essencial.

Por mais sensível que seja, uma das formas mais eficazes de falar sobre violência autoprovocada é fazer circular informações de qualidade e confiáveis, como veremos em seguida. E as redes podem ajudar muito não apenas com informação, mas também com canais de ajuda especializada.

**Para pensarmos nas ações com as e os adolescentes nas escolas (e também as ações virtuais), precisamos sempre lembrar que:**

- + Saúde mental envolve sempre uma diversidade de fatores
- + Nunca podemos limitar o tema (nem a doença nem a saúde) a uma relação de causa-efeito
- + O tabu que silencia o debate sobre temas sensíveis deixa as pessoas ainda mais vulneráveis
- + Empatia, acolhimento, franqueza e diálogos abertos são essenciais
- + Precisamos respeitar nossos limites quando os temas nos mobilizam demais
- + Prestar atenção aos gatilhos e divulgar os recursos de ajuda especializada no início e no fim das atividades



**5.2**

# LEIS E DIRETRIZES

Em 2006 foi lançado no Brasil o **Plano Nacional de Prevenção do Suicídio**, através da Portaria nº 1.876, que anunciava o desenvolvimento de estratégias de promoção de saúde mental, qualidade de vida, informação, comunicação e sensibilização de toda a sociedade diante da temática do suicídio.

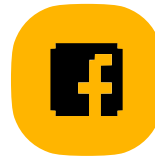




Em 2019 foi instituída a **Política Nacional de Prevenção da Automutilação e do Suicídio** pela Lei 13.819 que traz objetivos relacionados à prevenção e promoção de saúde, cabendo às instituições de ensino a notificação aos Conselhos Tutelares de casos de Violência Autoprovocada em crianças e adolescentes. Essa lei constitui um passo fundamental para o estabelecimento de políticas públicas efetivas

quanto ao cuidado e à prevenção da Violência Autoprovocada.

Os casos que envolvem páginas na Internet, redes sociais ou aplicativos de mensagem **podem ser reportados também nas próprias plataformas.**

Da mesma forma como vimos em relação à outras formas de violências que ferem as Políticas de uso das plataformas, a incitação ao suicídio ou à violência autoprovocada devem ser denunciadas.

**Reporte diretamente nas redes:**

				
				
<u>INSTAGRAM</u>	<u>FACEBOOK</u>	<u>TWITTER</u>	<u>YOUTUBE</u>	<u>GOOGLE</u>

PARA SABER MAIS



PLANO NACIONAL DE PREVENÇÃO DO SUICÍDIO



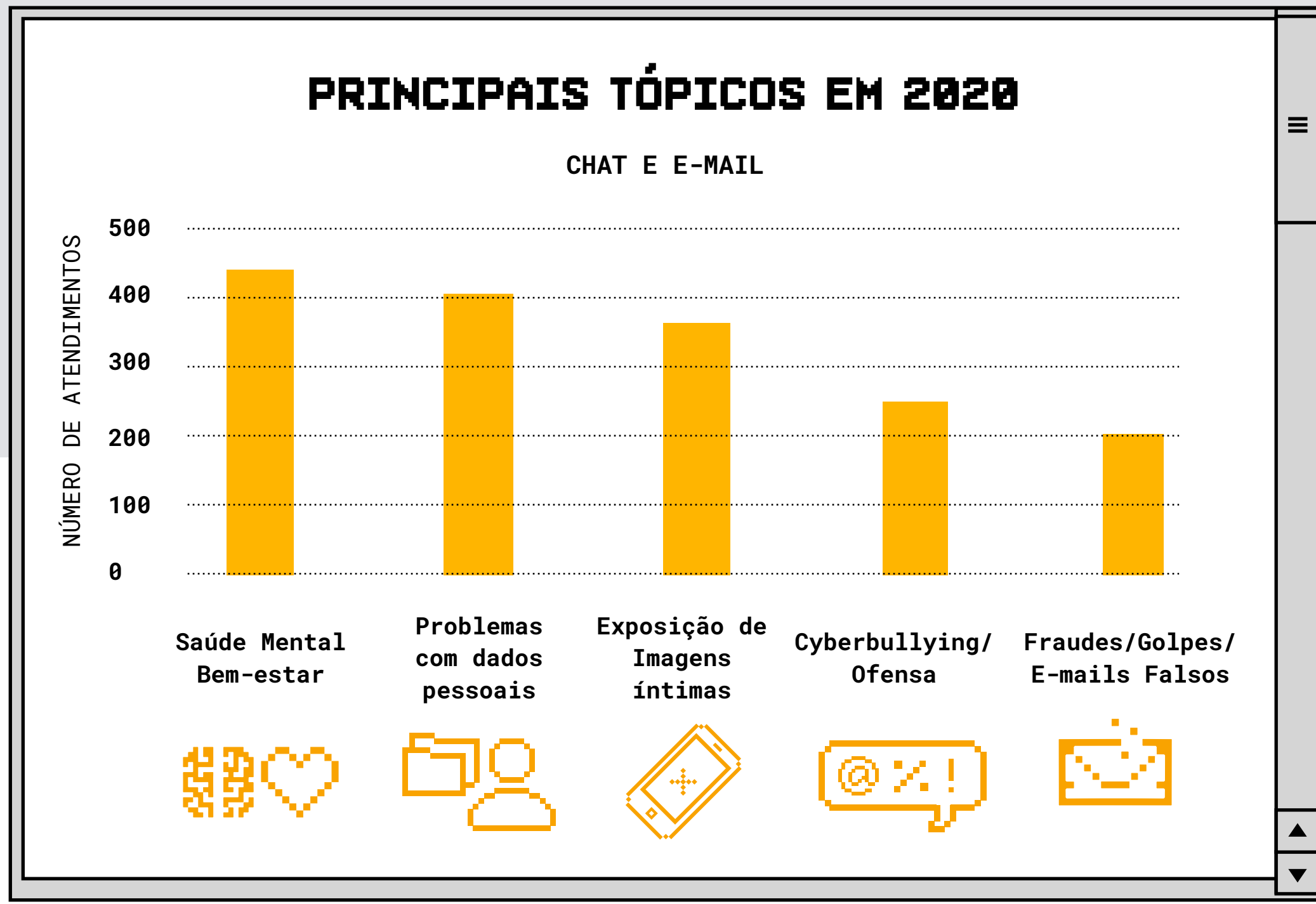
POLÍTICA NACIONAL DE PREVENÇÃO DA AUTOMUTILAÇÃO E DO SUICÍDIO - LEI 13.819

5.3

# SAÚDE MENTAL E COVID

O contexto da COVID-19 tem impactado diretamente a qualidade de vida e a saúde mental de todas as pessoas. Apesar de ser ainda tudo muito recente, a pesquisa **“Juventudes e a Pandemia do Coronavírus”** ajuda a entender alguns efeitos na vida de jovens no Brasil. Com o objetivo de apoiar a construção de políticas baseadas em evidências e sustentadas por um amplo processo de diálogo e articulação social, o Conselho Nacional da Juventude (CONJUVE) e organizações parceiras produziram, com a participação direta dos jovens, o estudo com base na metodologia PerguntAção, desenvolvida pela Rede Conhecimento Social que ouviu mais de 30 mil jovens entre 15 e 29 anos.

De modo geral, jovens sentem que as condições física e emocional foram prejudicadas desde o início do isolamento social.



A ansiedade, o tédio e a impaciência foram apontados como os sentimentos mais presentes durante o isolamento social. Acolhimento aparece como o sentimento mais positivo, sentimento que pode estar relacionado tanto ao convívio familiar quanto às interações remotas.

No **Canal de Ajuda da SaferNet**, a busca por orientação relacionada à saúde mental teve aumento expressivo em 2020, representando um em cada 5 atendimentos, sendo mais de 64% de

crianças ou adolescentes, ao lado de situações de exposição de imagens íntimas e problemas com dados pessoais. Os impactos da pandemia na qualidade de vida e na saúde mental são relevantes em **quase todos os países**, o que sinaliza a importância de ações que favoreçam o autocuidado e a promoção de saúde em todas as faixas etárias. Para muitas pessoas, a Internet se tornou o principal meio para interação social, trabalho, estudo e lazer, o que intensificou as experiências vividas online.

PARA SABER MAIS



**Juventudes e a Pandemia do Coronavírus**

Conheça a Pesquisa realizada com mais de 68 mil jovens de todo o Brasil sobre os impactos da pandemia em suas vidas e na sociedade.

[Ver relatório completo Juventudes e a Pandemia](#)

**PESQUISA "JUVENTUDES E A PANDEMIA DO CORONAVÍRUS"**



#INDICADORESHELPLINE

TOTAL DE ATENDIMENTOS: **32.579**

UNIDADES DA FEDERAÇÃO: **27**

PESSOAS ATENDIDAS: **8.944**

UNIDADES DA FEDERAÇÃO: **3.913**

PESSOAS ATENDIDAS: **2.308**

UNIDADES DA FEDERAÇÃO: **17.414**

**INDICADORES DO CANAL DE AJUDA DA SAFERNET**

5.4

# CAMPANHAS DE AUTOCUIDADO

Um caminho para promoção de saúde mental nas redes é estimular que as pessoas “saíam do automático” e assumam mais controle e cuidado com suas experiências online.

**Alguns exemplos de atitudes que podem favorecer um uso mais saudável e positivo:**

**Materiais que podem ajudar**

a iniciar este debate com os adolescentes. Destacamos primeiro a Campanha Digital Sem pressão:

- + Cuidar das relações que estabelecemos nas redes
- + Refletir antes de compartilhar algo sobre outras pessoas
- + Manter uma rotina equilibrada de atividades desconectadas das telas
- + Selecionar com cuidado a qualidade dos conteúdos que consumimos
- + Dosar o tempo que dedicamos às telas
- + Checar sempre a fonte e credibilidade de informações sobre saúde nas redes

CAMPANHA #DIGITALSEMPRESSÃO



VÍDEOS INSPIRADORES



GUIAS DE ORIENTAÇÃO



GUIAS DE ORIENTAÇÃO



ILUSTRAÇÕES

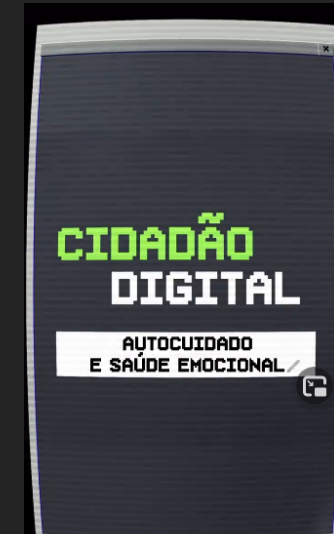


CO-CRIAÇÃO DE CARTAZES



PALESTRA COM LEANDRO KARNAL

SÉRIE CIDADÃO DIGITAL



CAMPANHA "COMO CRESCER"





5.5

# CAMPANHAS SOBRE AUTOVIOLÊNCIA

Sabemos que suicídio e outras formas de autodano são temas super sensíveis. Mas é possível sim falar sobre eles de forma propositiva e sem tabu. E antes do suicídio, precisamos falar de sofrimento emocional e saúde emocional, já que reconhecer os próprios estados emocionais na experiência online é muito importante, como vimos nos tópicos anteriores.

Como indicado pela Karen no webinar, há muitas formas de usarmos as tecnologias a favor da vida, para promoção de saúde emocional e no fortalecimento das redes de apoio.

**FESTIVAL AMARELO**




**PALESTRAS**

**CAMPANHA #EUESTOU**





**CVV**

**SAÚDE MENTAL DE ADOLESCENTES**




**MAPA SAÚDE MENTAL**





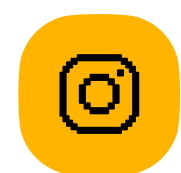










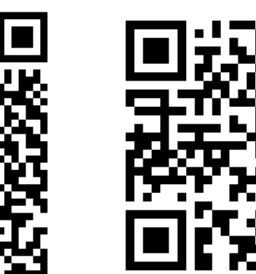

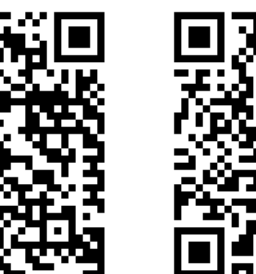

**5.6**

# FERRAMENTAS

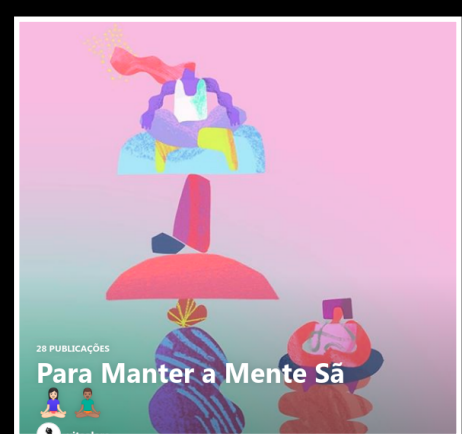
Assumir maior controle sobre os usos das redes é um passo sem volta para manter um uso positivo e saudável. Isso vale para todas as plataformas.

Vamos conferir alguns caminhos práticos que valem para você fazer seu check-up e para exercitar com os adolescentes nas atividades.

**Confira os caminhos nas principais redes:**

						
						
<u>INSTAGRAM</u>	<u>FACEBOOK</u>	<u>TWITTER</u>	<u>ANDROID</u>	<u>APPLE</u>	<u>PLAYSTATION</u>	<u>XBOX</u>

**GUIAS DE ORIENTAÇÃO PARA AS FAMÍLIAS**



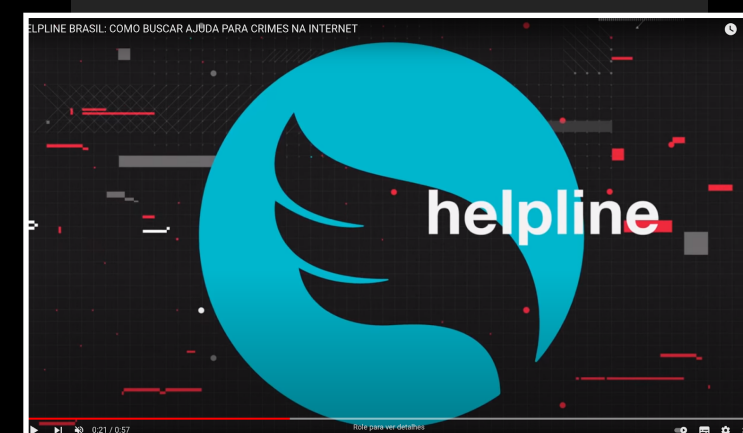
GUIAS INSTAGRAM PARA MANTER A MENTE SÃ



GUIAS PARA FAMÍLIAS



GUIA GOOGLE DE BEM-ESTAR



CANAL DE AJUDA SAFENET



A1

## ATIVIDADE 1

**1** Reserve um momento da sua semana (cerca de 15 minutos) para reflexão. Se possível, fique sozinho/a em um lugar silencioso, longe do celular, das notificações e de outras pessoas. Pense um pouco sobre você, sobre os caminhos trilhados até este momento de sua vida, nesta escola/ Instituição. Tente pensar naquilo que traz força, paz, inspiração e alegria a você.

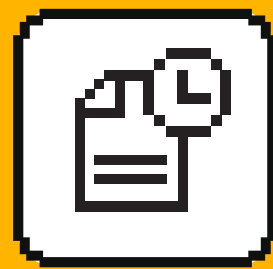
~~2~~ Convide algumas pessoas (amigas/os ou familiares) que se conhecem e que confiam umas nas outras para uma conversa honesta sobre saúde mental e internet. Não precisa ter roteiro, mas você pode usar perguntas catalisadoras para começar, como "o que na internet faz você se sentir ansiosa/o ou triste?", "o que faz você se sentir viva/o, feliz e esperançosa/o?", "o que faz quando percebe que a experiência on-line gera desconforto?", ou "como faz para controlar o tempo de conexão e desplugar?". Essa conversa pode acontecer em uma videoconferência, num grupo de WhatsApp, por meio de uma ligação telefônica, como for possível. Procure exercer a escuta ativa e registrar os principais pontos trazidos.

**3** Agora, que tal propor essa mesma dinâmica aos estudantes? Neste momento de ensino remoto emergencial, os minutos dedicados à reflexão podem ser combinados entre um encontro virtual e outro. O roteiro da conversa pode também ser antecedido aos alunos, acompanhado do convite para que levem a discussão a familiares e amigos com quem se sintam confortáveis para realizar a conversa. Depois, proponha a pauta aos próprios estudantes, deixando-os à vontade para que expressem suas posições, além de impressões que tiveram das conversas com os familiares (para aqueles que conseguiram desenvolver essa etapa).

**4** Ao final da discussão com os estudantes, ~~convide-os a montar uma lista. A ideia é reunir~~ músicas, vídeos, filmes, séries, aplicativos ou outros conteúdos que trazem sentimentos positivos para o grupo enquanto navegam. Vocês podem montar essa lista usando qualquer serviço disponível. Para músicas, indicamos serviços de streaming, como Spotify, Deezer, Google Play Music, etc. Uma outra opção para

músicas, e que também serve para filmes e séries (você pode procurar pelos trailers), é o Youtube. Você pode também propor que criem um post em uma rede social, caso queiram indicar aplicativos ou conteúdos a outros adolescentes, tanto da escola quanto de fora dela, aproveitando o exercício de cocriação para trocarem referências, dicas e ideias. Para encerrar, convide para que selecionem um nome criativo e compartilhem a lista nas suas redes, usando a hashtag #DigitalSemPressão, #InternetMaisPositiva e #CidadãoDigital.

**5** A última etapa da atividade é individual. ~~Após o exercício de cocriação, convide cada~~ aluno a fazer uma análise pessoal da experiência, incentivando que compartilhe se ela alterou a forma como vê a internet e fez repensar suas condutas ou não. Se preferir, mantenha essa parte da atividade "em privado", de modo que cada aluno compartilhe com você algum ponto ou angústia que não conseguiu socializar no grupo.



**A2**

**ATIVIDADE 2**

**O que fazemos para nos sentirmos bem nas redes?**

Na campanha **Digital Sem Pressão**, a discussão sobre saúde, física e mental, ganhou a voz dos jovens. Esta atividade propõe uma sequência do processo criativo com turmas de alunos adolescentes. Ela pode ser realizada nos formatos presencial ou remoto. A ação terá o foco na expressão de sentimentos e ideias para a preservação da saúde emocional e mental no uso de redes sociais, aplicáveis também ao dia a dia. Ela explorará, do ponto de vista da mensagem, o compartilhamento de dicas sobre o que podemos fazer para nos sentirmos bem e evitarmos o desânimo na internet. Do ponto de vista da mídia, convidará à experimentação de outros formatos, além dos cartazes (possibilidades, aliás, que o próprio módulo anuncia).

**Como começar?**

Convide os alunos a levantarem ideias sobre o que fazem para se sentirem bem ou evitarem o desânimo na internet. Encoraje-os a pensarem sobre situações difíceis que já viveram e sobre o que fizeram na ocasião. Depois, estimule-os a pensar sobre como essas dicas poderiam ser compartilhadas com outros adolescentes como eles. Apresente alguns formatos, mas esteja atento(a) e sensível às mídias e redes que os próprios adolescentes sugerirem (Instagram, TikTok, Twitter, entre outros). Também recomende que façam, independentemente da mídia a ser utilizada, um pequeno roteiro ou briefing, abordando: O que querem dizer? Por que é importante? Como a mensagem será veiculada?

**Sugestões de formatos**

**(Quadrinhos e charges)**

**Quadrinhos, memes e charges** remetem a aspectos como humor e descontração, mas isso não significa que mensagens importantes não possam se valer desses

recursos, sobretudo quando destinadas ao público jovem. Uma ferramenta interessante - e de uso simples - para a criação de memes é a **Imgflip meme generator**, disponível **[AQUI](#)**.

**Áudio e vídeo**

Áudios e vídeos com as mensagens dos jovens podem ser capturadas com seus dispositivos digitais e, depois, editadas em aplicativos on-line ou instalados nos computadores ou celulares. Confira **[exemplos de editores de vídeo](#)** que rodam no celular (disponíveis para Android e iOS) e ajudam a criar conteúdos. Já a matéria "**[Os 10 melhores aplicativos para edição de áudio no Android](#)**", produzida pelo TecMundo, traz opções de editores de áudio para o sistema operacional Android, também bastante intuitivas para uso em celulares.

**ATENÇÃO!**

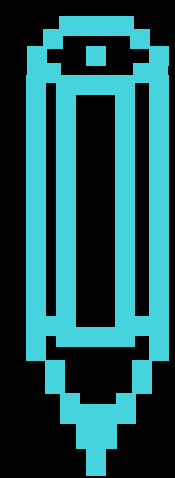
AO TRABALHAR COM IMAGENS, VÍDEOS E ÁUDIOS COM SEUS ALUNOS, É FUNDAMENTAL TOMAR CUIDADOS LEGAIS. SE UM VÍDEO POSSUIR IMAGEM OU VOZ DE OUTRAS PESSOAS, POR EXEMPLO, HÁ NECESSIDADE DA ASSINATURA DE UM TERMO DE AUTORIZAÇÃO. NO CASO DE CRIANÇAS OU ADOLESCENTES COM MENOS DE 18 ANOS, A ASSINATURA COLHIDA DEVE SER DOS PAIS OU RESPONSÁVEIS.

**ALGUMAS DICAS DE FONTES DE MÍDIAS GRATUITAS PARA USO:**

PARA ÁUDIO:  
**[JAMENDO](#)**

PARA IMAGENS E VÍDEOS:  
**[PIXABAY](#)**

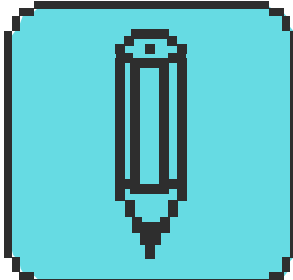
CAPÍTULO



# EDUCAÇÃO MIDIÁTICA

Vamos discutir mais sobre o fenômeno da desinformação e entender por que prestar atenção antes de postar ou compartilhar algo, e mesmo dominar caminhos básicos para checagem de informações, tornaram-se habilidades básicas para qualquer pessoa que usa a Internet hoje.

### RESUMO




**5 HORAS**

**5 VIDEOS**

**5 SUGESTÃO DE ATIVIDADE**

O trabalho com o campo jornalístico-midiático, que contextualiza a produção, curadoria e checagem de informação, é previsto no componente de Língua Portuguesa. Os campos de atuação na vida pública, artístico-literário e de estudo e pesquisa são igualmente mobilizados pela temática..



### PARA ASSISTIR

Webinar com Nina Weingrill (Agência ÉNois) e Mônica Rosina (Facebook) debatendo estratégias para minimizar o problema da desinformação e promover educação midiática. A mediação é de Thiago Tavares (SaferNet).




### PARA SABER MAIS SOBRE O TEMA


Campanhas com recursos em vídeo que podem ajudar a realizar atividades pedagógicas com o tema.

**Desinformação e Saúde**  
Mini videoaula animada para falar de desinformação, leitura crítica, checagem no contexto da saúde.




### PARA APLICAR EM SALA DE AULA

Recursos práticos para usar em sala de aula (remota ou presencial)



**SUGESTÃO DE ATIVIDADES**

**ATIVIDADE 1**  
Caminhos da Checagem

**ATIVIDADE 2**  
Teste do "Falso"

### OUTROS MATERIAIS COMPLEMENTARES

Confira material extra na versão online da formação para aprofundar seus conhecimentos.


Vídeos do Palavra Aberta sobre: **leitura crítica** e **ceticismo**

Glossário Essencial da Desinformação

O guia para iniciantes de A a Z sobre Inteligência Artificial

Estudo “Jornalismo, fake news & desinformação: manual para educação e treinamento em jornalismo” da Unesco

Ferramentas, cursos complementares e muitos outros recursos



6.1

# CONTEXTO

Sem dúvida, viver em um mundo repleto de informações é muito melhor do que não ter acesso a elas. Mas isso não quer dizer que tudo esteja bem: não há qual-quer garantia de que as mensagens que chegam até nós são confiáveis ou de quali-dade. Entender o fenômeno da desinfor-mação e dominar caminhos básicos para checagem de informações tornaram-se habilidades básicas para todas as pessoas no mundo cada vez mais digital.

News literacy, ou “educação midiática” (uma das muitas traduções possíveis) é justamente o desenvolvimento de habilidades para uso crítico das mídias e capacidade diferenciar a qualidade dos conteúdos. O termo **fake news** (notícia falsa) ganhou força a partir de 2016, mas, como vimos no webinar, não se trata de um debate novo — **neste vídeo** você pode

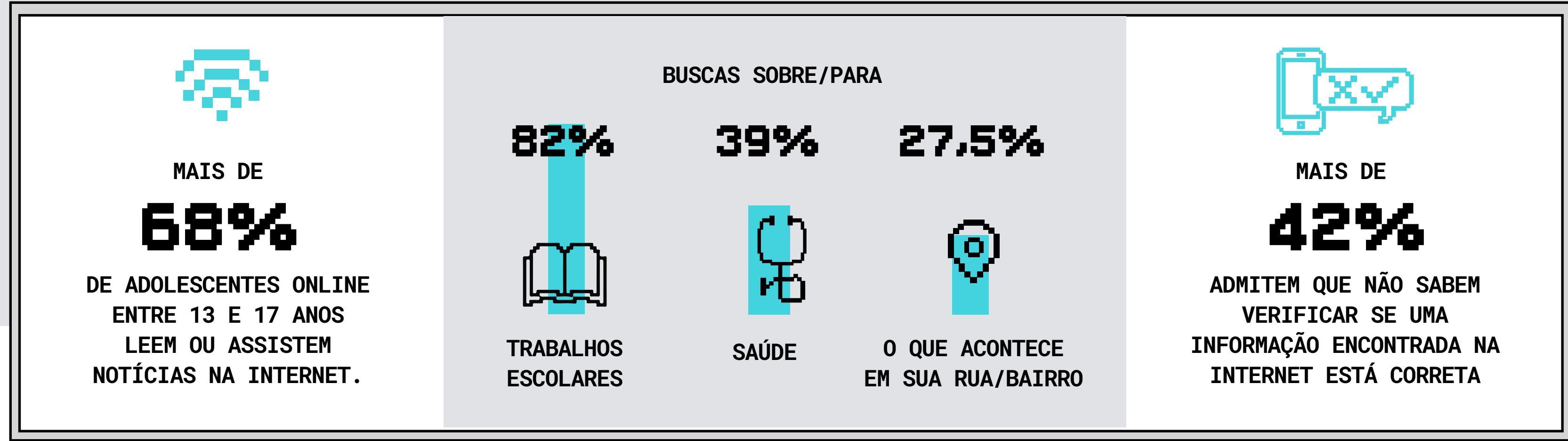
entender como as notícias falsas fazem parte do debate público há muitos séculos. Entretanto, é fato que cada vez mais o fluxo de informações falsas ou enganosas na Internet têm impactos reais na vida das pessoas e mesmo nos regimes políticos. Boatos, conteúdos enganosos e mentiras podem impactar negativamente a saúde mental e mesmo a convivência harmônio-sa das pessoas nas redes, facilitando, inclu-sive, a propagação de discursos de ódio.

“**Notícias falsas**”, porém, é um termo que reduz o debate. Isso porque nem sempre estamos falando de notícias — pensando em termos jornalísticos — e nem sempre elas são falsas — já que po-dem ser, por exemplo, descontextualiza-

das. Como se trata do termo que se popu-larizou, faz sentido empregá-lo para que as pessoas entendam do que estamos falan-do, principalmente se nossa audiência tem pouca familiaridade com a discussão. Mas, sempre que possível, precisamos explicar que o problema é mais complexo e não afeta só o jornalismo. É bastante comum utilizarmos, como substituto de “notícias falsas”, o termo “**desinformação**”, que tira um pouco do peso da notícia jornalística e também da relação falso/verdadeiro, mas mesmo este termo pode ser ampliado.

E é assim que chegamos ao conceito de “**desordem informacional**”, que procura explicar a dificuldade que existe, hoje, para que nós possamos selecionar,

compreender e avaliar informações. Com o crescimento acelerado da circulação de informações, nós assistimos ao surgimento de um ambiente online poluído e ruidoso, no qual conteúdos enganosos, inverídicos, enviesados ou descontextualizados circulam com tanta rapidez quanto aqueles que são verídicos. Essa poluição dificulta o processo de criar, distribuir, interagir e compartilhar conteúdos de qualidade, baseados em fatos ou evi-dências, e, por vezes, enfraquece vozes importantes em uma democracia, como os governos legitimamente eleitos, cientistas e pesquisadores, jornalistas e movimentos sociais que pautam a busca por igualdade e inclusão.



**6.2**

# DESORDEM INFORMACIONAL

No contexto da desordem informacional, podemos pensar em três grandes fenômenos. O esquema abaixo foi proposto pelo First Draft (em inglês). Não há uma tradução direta para os termos em inglês, mas podemos seguir o proposto pela pesquisadora Tatiana Dourado:

- **informação errada** (misinformation),
- **desinformação** (disinformation) e
- **desinformação maliciosa** (mal-information).

Perceba que os três fenômenos estão inseridos em um espectro que contempla a ideia de informações falsas e/ou com intenção de prejudicar.

**1** **Informação errada (misinformation)**

São informações falsas, mas que não foram criadas ou compartilhadas deliberadamente com objetivo de prejudicar algo ou alguém. É comum que sejam compartilhadas, por exemplo, com a intenção de ajudar uma pessoa ou causa, como quando pessoas compartilham receitas de remédios caseiros ineficazes ou arrecadações falsas de dinheiro acreditando que irão ajudar amigos ou parentes.

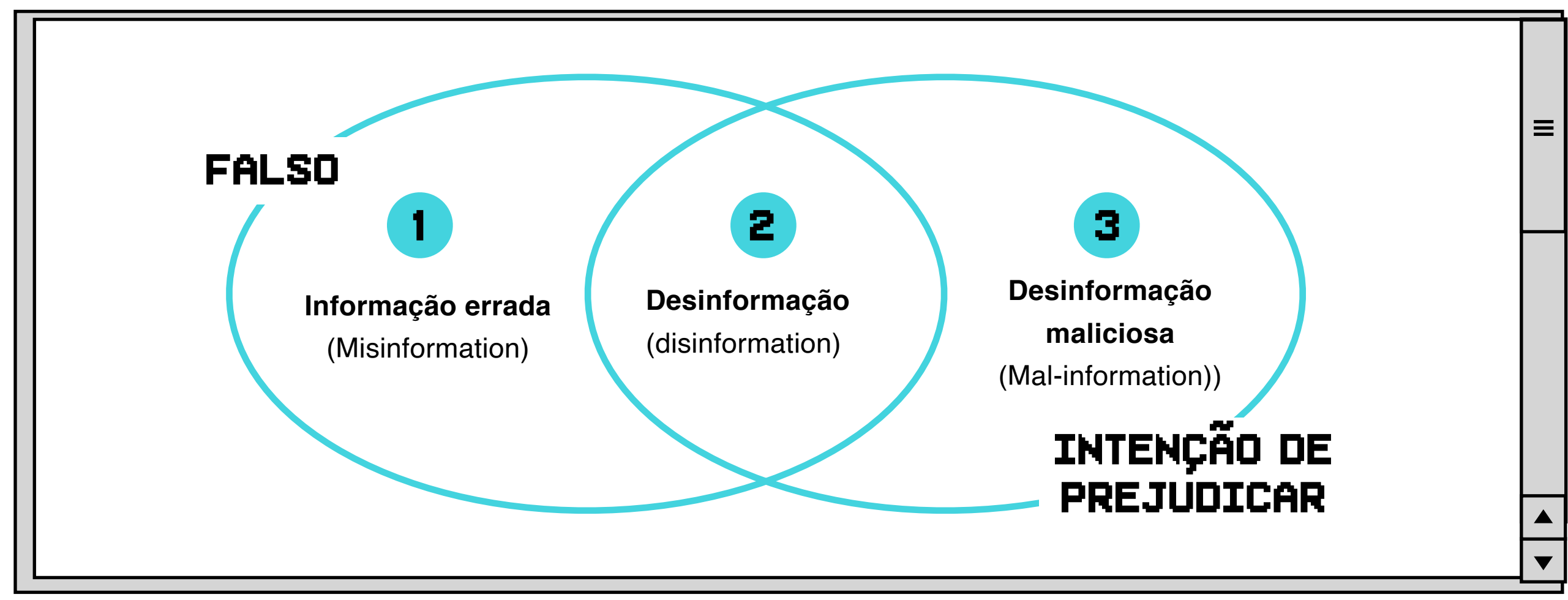
**2** **Desinformação (disinformation)**

A desinformação se refere a informações falsas, criadas ou compartilhadas com intenção deliberada de causar dano direcio-

nado ou enganar. São motivadas principalmente por lucro, influência política, emoção ou desejo de causar distúrbios sociais. Aqui entram desde conteúdos criados para afetar a reputação de alguém até mesmo propagandas disfarçadas de notícias que procuram induzir pessoas a comprar um produto ou serviço “milagroso”.

**3** **Desinformação maliciosa (mal-information)**

São informações verdadeiras usadas para causar dano direcionado. Por exemplo, informações vazadas de governos, empresas, organizações ou pessoas (incluindo doxing, o compartilhamento de dados pessoais).

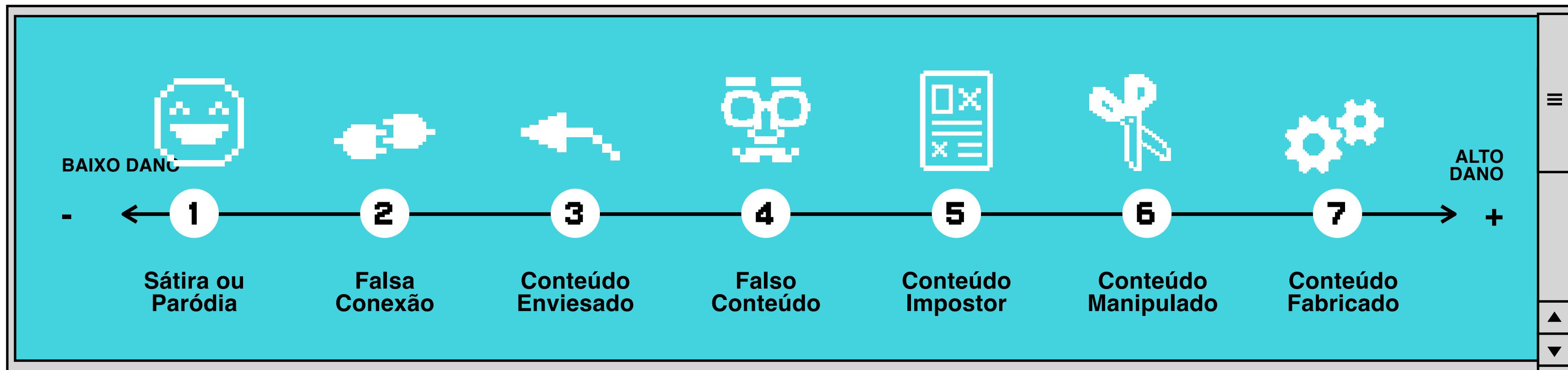


**IMPORTANTE**

Para facilitar a compreensão do tema, vamos utilizar neste módulo o termo “desinformação” como um guarda-chuva que compreende diferentes tipos de conteúdos inverídicos, enviesados, descontextualizados e manipulados. Sugerimos que você faça o mesmo ao realizar atividades educativas sobre o tema, mas sempre que possível explique as características enganosas ou prejudiciais do conteúdo sobre o qual você está falando.



**6.2 CONTINUAÇÃO**



**TIPOS DE DESINFORMAÇÃO**

Deu pra perceber que existem muitas nuances, certo? O First Draft (em inglês) também propõe que, dentro da desordem informacional, existem pelo menos 7 tipos diferentes de conteúdos desinformativos, que podem ser entendidos de um espectro que vai de conteúdos com menor potencial de dano (as sátiras ou paródias) até aqueles com maior potencial (os conteúdos fabricados).

**1** **Sátira ou Paródia**

BAIXO DANO ←

conteúdo geralmente humorístico, de caráter crítico ou opinativo, que cria, exagera ou satiriza fatos, pessoas ou instituições reais. Pode causar dano quando tomado como literal ou verdadeiro por quem interage com ele. Nem sempre a sátira ou a paródia é evidente, e quando compartilhada de forma descontextualizada (por exemplo, através de um print ou cópia do arquivo, e não da URL original), seu potencial enganoso aumenta. **Exemplo.**

**2** **Falsa Conexão**

conteúdos em que títulos, legendas ou ilustrações, verdadeiros em si, são erroneamente conectados para justificar um determinado viés. O uso de imagens e fotos de bancos de arquivos sem a devida explicação de que se trata de conteúdo apenas ilustrativo e não factual é uma das estratégias da falsa conexão. O mesmo vale para títulos sensacionalistas que se valem da estratégia do clickbait (isca de cliques), comum em diferentes conteúdos desinformativos. **Exemplo.**

**3** **Conteúdo Enviesado**

trata-se do uso enganoso de informações para enquadrar de forma negativa uma pessoa ou assuntos específicos. A informação pode ter um fundo verdadeiro, mas é usada de forma propositalmente enviesada, podendo-se, por exemplo, omitir partes que levariam a uma interpretação correta do conteúdo ou fato. **Exemplo.**

**6.2 CONTINUAÇÃO**

**IMPORTANTE**

nem sempre é possível determinar exatamente um único tipo de desinformação em dado conteúdo. Essa divisão em tipos tem como objetivo apenas nos ajudar nesse processo.



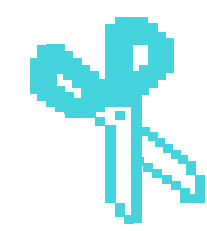
**4 Falso Contexto**

conteúdo verdadeiro, mas compartilhado de forma descontextualizada. São os casos, por exemplo, em que uma notícia ou conteúdo é compartilhado como sendo atual, quando na verdade é antigo, ou quando é compartilhado como tendo acontecido em determinado lugar, quando aconteceu em outro. **Exemplo.**



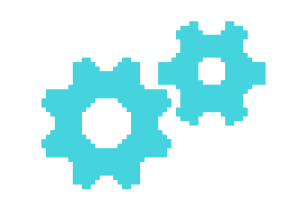
**5 Conteúdo Impostor**

uso de fontes genuínas (como o nome, a logo ou mesmo uma URL similar a de uma instituição ou pessoa) para enganar. Em aspecto amplo, pode se referir também a conteúdos publicitários inseridos em sites e perfis de forma disfarçada, levando o usuário a acreditar que se trata de um conteúdo criado pelo titular do site ou perfil. **Exemplo.**



**6 Conteúdo Manipulado**

quando informações verdadeiras (texto, fotos, vídeos, áudios) são alteradas para enganar. Recentemente, os deep fakes têm ganhado destaque. Tratam-se de manipulações hiper-realistas de vídeos ou áudios, criados usando ferramentas de aprendizagem de máquina, e que geralmente simulam o rosto de uma pessoa no corpo de outra ou simulam uma fala que nunca existiu de verdade. **Exemplo.**



**7 Conteúdo Fabricado**

informações completamente falsas, criadas geralmente com aspecto sensacionalista (clickbait, ou seja, buscam atrair cliques), e sempre com algum tipo de interesse implícito. Em aspecto amplo, pode se referir também a práticas de content farming (“fazenda de conteúdo”), em que um mesmo conteúdo é compartilhado como sendo original por um número expressivo de páginas, canais ou perfis controlados por uma mesma pessoa ou instituição, geralmente com propósito de ganhar dinheiro com publicidade gerada a partir do tráfego de visitantes. **Exemplo.**

ALTO DANO +

**6.3**

# ANÁLISE CRÍTICA DE MÍDIAS

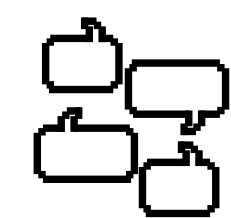
Após entender melhor sobre o contexto da desinformação, precisamos avançar em aprender formas de driblar esse problema. A educação midiática passa, necessariamente, por uma análise crítica de mídias e por tomarmos consciência de que todo mundo tem responsabilidade sobre o que posta e o que compartilha. O **vídeo criado** pela equipe do Palavra Aberta para o Cidadão Digital ajuda a compreender.

A pandemia de Covid-19 trouxe urgência para esse tipo de educação. Afinal de contas, desinformação na saúde pode até matar. Foi o que aconteceu, por exemplo, no Irã, quando centenas de pessoas acreditaram em uma informa-

ção falsa e beberam álcool na esperança de combater a Covid-19, ainda no início da pandemia: **Ingestão de álcool para falsa cura contra coronavírus já matou 300 no Irã.**

O papo é tão sério que a própria Organização Mundial da Saúde (OMS) criou uma palavra para nos alertar de um outro perigo além da pandemia em si: **infodemia**.

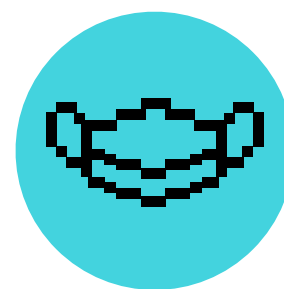
Aqui no Brasil, a Fiocruz pegou carona no aviso da OMS e também chamou a atenção da população para o perigo das informações falsas, principalmente sobre as vacinas: A pandemia da desinformação.



## INFODEMIA

Ambiente de excesso de informações, nem todas confiáveis, que mais confunde do que ajuda no momento em que precisamos encontrar dados para cuidar de nossa saúde.

Fonte: Desinfodemia - Decifrar a informação sobre a Covid-19.



Um levantamento da Unesco identificou quatro formatos principais de desinformação sobre a Covid-19:

**1**

### Narrativas e memes emotivos

Informações falsas com um tom para despertar nossas emoções; podem se misturar com informações incompletas, opiniões e mesmo dados que são verdadeiros mas fora de contexto.

**3**

### Imagens e vídeos alterados ou fora de contexto

Histórias falsas contadas em imagens ou vídeos que viralizam. Criam confusão e desconfiança generalizada da população.

**2**

### Sites e perfis fabricados

Páginas da internet que têm um visual parecido com o de sites sérios ou oficiais. Publicam informações falsas mas com aspecto de verdadeiras, muitas fingindo ser reportagem.

**4**

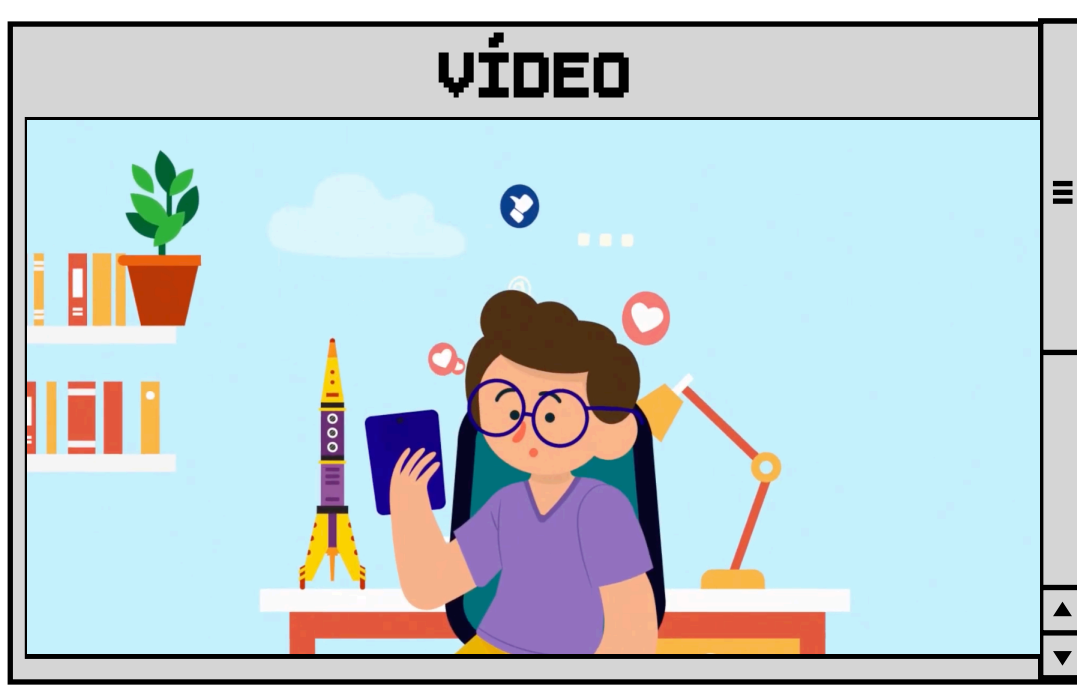
### Campanhas orquestradas

Conteúdo que procura semear desconfiança e discussões em comunidades online, promover o nacionalismo ou coletar dados. Pode envolver o uso de robôs (bots) para impulsionar as mensagens.

**6.3 CONTINUAÇÃO**

Como, então, encontrar as melhores informações e conseguir avaliar sua confiabilidade? Precisamos, o quanto antes, desenvolver habilidades básicas de curadoria e análise crítica de informações.

Não é que você tenha que desconfiar de tudo. Mas uma dose saudável de dúvida ajuda a filtrar e selecionar as informações mais adequadas a cada contexto. Com algumas estratégias você vai desenvolver o hábito de entrevistar a informação, e não simplesmente aceitar tudo o que está circulando por aí:



Essa postura mais reflexiva e questionadora não vale apenas para textos — imagens, vídeos, áudios, videogames e até embalagens de produtos podem (e devem!) passar pela nossa análise crítica. Vamos a algumas dicas práticas.

**PRATIQUE O CÉTICISMO SAUDÁVEL**

Pra começo de conversa, se você estiver em dúvida sobre a veracidade de alguma informação, pare um pouquinho e respire! Pode parecer bobagem, mas alguns minutinhos de reflexão podem te livrar da cilada de acreditar ou compartilhar algum conteúdo falso. A frase a seguir, criada pela especialista em comunicação e educação Erin Gibson, funciona como um alerta diante de qualquer informação suspeita:

**CÉTICISMO SAUDÁVEL**

**“EPA, PERAÍ, O QUE?!”**

A informação causou em você **choque, surpresa** ou raiva?

Pause! Não passe adiante ainda!

Dedique um momento para **investigar** a informação

**SINAIS DE ALERTA**

**! NOTÍCIAS OU POSTS EM TEXTO**

- Não tem autoria (ou seja, não dá para saber quem escreveu ou publicou o conteúdo)
- Não traz as fontes de dados (ou elas não existem)
- Linguagem ofensiva, alarmista ou com discurso de ódio
- Não separa o que é opinião, o que é publicidade e o que é fato
- Não existem outras fontes tratando do assunto (principalmente em casos de temas graves ou urgentes)

**! IMAGEM**

- Fotos borradas, com resolução baixa ou com partes distorcidas
- Não identifica o autor, a data e o contexto
- Repetição de padrões, como em fotos que buscam aumentar multidões

**VÍDEOS**

- ! Rostos de rosto pouco nítidos, diferentes do restante do vídeo
- Dentes sem separação e olhos sem foco
- Sombras que não coincidem com a direção da luz
- Vídeos com cortes abruptos ou velocidade alterada

Fonte: Educamídia - Palavra Aberta.

6.3 CONTINUAÇÃO

QUATRO PASSOS SIMPLES PARA VERIFICAR A INFORMAÇÃO

Recebeu alguma informação e quer checá-la de forma ágil? O autor Mike Caulfied propõe alguns movimentos em sua metodologia batizada como SIFT, que leva em consideração quem criou a mensagem e em qual contexto.

**IMPORTANTE**

quando falamos sobre a fonte da informação, estamos tentando descobrir o autor dela e não quem compartilhou ou nos repassou aquele conteúdo em alguma rede social ou no WhatsApp, por exemplo. Em várias situações é bem complicado rastrear quem originou a mensagem e, na dúvida, o melhor a fazer é não passar adiante.

**PASSO 1: PAUSE**

Você conhece e confia neste site ou na fonte da informação? Se não conhece, não compartilhe ou passe adiante a informação. Vá para os próximos passos para tentar saber mais claramente o que está lendo. Se em algum momento se sentir perdida/o, ou se afastar do seu objetivo inicial, pause e comece de novo.

**PASSO 2: INVESTIGUE A FONTE**

Quem está dizendo isso? Quais as suas qualificações e motivações? É um prêmio Nobel? Um site de teorias da conspiração? É alguém que pode ter uma agenda comercial ou política implícita? É uma propaganda disfarçada? É claro que até um prêmio Nobel pode estar enganado, e que organizações e empresas com interesses políticos ou comerciais publicam muitas informações de qualidade. Ainda assim, antes de ler, procure conhecer melhor quem escreveu/publicou. Vale a pena gastar algum tempinho para estabelecer se a fonte em questão é confiável ou relevante, e até mesmo se o texto merece a sua atenção. Caso a fonte nem possa ser identificada, simplesmente não compartilhe!

**PASSO 3: BUSQUE MAIS INFORMAÇÕES**

O próximo passo é buscar a mesma informação em outras fontes que você conhece e nas quais confia. Qual a melhor fonte de informação que você consegue encontrar sobre isso? Faça uma busca e escaneie os resultados. Tente encontrar uma cobertura mais confiável, mais aprofundada ou mais equilibrada. Melhor ainda, procure descobrir se há consenso sobre essa afirmação. Você não precisa concordar, mas conhecer o histórico e o contexto de determinada afirmação irá lhe ajudar a ter uma melhor avaliação.

**PASSO 4: ENCONTRE O CONTEXTO ORIGINAL**

De forma intencional ou não, a internet pode ser um 'telefone sem fio'. Afirmações, dados e imagens muitas vezes são retirados de seu contexto original e apresentados de forma isolada, oferecendo um recorte da realidade. Outras vezes, podem ter sido remixados para criar uma nova mensagem. Elementos deixados de fora de uma imagem ou vídeo, legendas que não combinam com o que está na foto ou informações científicas superficiais são exemplos de mensagens descontextualizadas. Procure a informação completa.

**6.3 CONTINUAÇÃO**

**LEITURA LATERAL**

Talvez você já saiba que existe um ramo do jornalismo especializado na checagem de informações (fact-checking), que faz um trabalho detalhado de confirmação de dados, afirmações e postagens — veja mais sobre na próxima seção. Jornalistas são treinados para essa atividade, que não tem como ser exercida por todo mundo o tempo todo. Mas podemos nos inspirar em algumas técnicas da área para avaliar informações no nosso dia a dia: uma delas é a leitura lateral.

**Se você precisa avaliar a confiabilidade de um site ou post, não perca muito tempo nele mesmo, observando de alto a baixo seu conteúdo (leitura vertical). Saia dele e procure na internet outras informações relacionadas.**

**DESENVOLVENDO O HÁBITO DA INVESTIGAÇÃO**

Todas as mensagens de mídia são construções, ou seja, têm um/a autor/a que fez escolhas, e

essas escolhas muitas vezes obedecem um objetivo (que pode ser simplesmente o de relatar um fato, mas também o de enganar, vender algo ou nos influenciar, por exemplo). O processo de analisar e refletir sobre tais mensagens, questionando e ampliando nosso repertório, é chamado de decodificação. Conheça a estratégia proposta pelo Project Look Sharp (uma organização de educação midiática ligada ao Ithaca College).

**QUESTÃO DE AUTORIDADE**

Hoje todo mundo pode, além de consumir, produzir informações. Tem até um nome que resume essa junção de papéis: prosumer (produtor + consumidor, em inglês). Mas será que, simplesmente por ter a capacidade técnica de publicar mensagens, todas as pessoas estão aptas a falar sobre tudo?

É preciso lembrar que, na internet, encontramos desde o relato de fatos incontestáveis até opiniões que variam de acordo com os interesses e o ponto de vista de quem está se manifestando. No meio de tudo isso tem ainda propaganda, sátira, informação descontextualizada, dados defasados, títulos que só contam uma parte da história. É a desordem informacional que explicamos no início do módulo.

Fonte: Project Look Sharp

**PRINCIPAIS PERGUNTAS AO ANALISAR MENSAGENS DE MÍDIA**

- **AUTORIA**  
Quem criou isto?
- **TÉCNICAS**  
Que técnicas foram usadas para comunicar a mensagem? Qual a eficácia dessas técnicas?  
  
Quais são os pontos fortes ou fracos?  
  
Por que os autores escolheram estas técnicas?
- **REAÇÕES**  
Qual é a minha interpretação?  
  
Como experiências e crenças anteriores interferem na minha interpretação?
- **CONTEXTO ECONÔMICO**  
Quem pagou? Quem pode ganhar dinheiro com isso?

- **CREDIBILIDADE**  
É fato, opinião ou outro tipo de conteúdo?  
  
Qual a credibilidade desta informação? Quais são as fontes das ideias e das afirmações?  
  
As fontes têm autoridade para falar desse assunto específico?
- **CONTEÚDO**  
Sobre o que é a mensagem?  
  
Que idéias, valores e informações estão explícitos? Quais estão implícitos?  
  
O que foi deixado de fora mas seria importante saber?
- **IMPACTO**  
Quem pode se beneficiar esta mensagem? Quem pode ser prejudicado? Que vozes estão representadas ou foram privilegiadas? Que vozes foram omitidas ou silenciadas?

6.4

# CHECAGEM DE FATOS

Como vimos no webinar, a checagem de fatos se tornou essencial atualmente para que conteúdos de desinformação sejam descobertos. E apesar de ser um trabalho realizado principalmente por jornalistas especializados, vimos que a leitura crítica da mídia, que ajuda a balizar a checagem, pode estar ao alcance de praticamente qualquer pessoa.

Precisamos estimular entre adolescentes os princípios da checagem de fatos e de análise crítica de mídia para que elas e eles conheçam formas de identificar conteúdos desinformativos no seu dia a dia. Para entender um pouco mais sobre o histórico da checagem de fatos, leia este post da agência Aos Fatos. Bom também entender um pouco melhor quais são os princípios, criados por uma associação internacional de verificadores de fato (a **International Fact Checking Network**), que guiam essa atividade:

- **apartidarismo e imparcialidade,**
- **transparência de fontes**
- **transparência sobre a organização e sobre o financiamento dos profissionais de checagem**
- **transparência na metodologia usada na checagem**
- **política de correções aberta e honesta (ou seja, informar o público caso tenha havido algum erro).**

No Brasil, temos diversas agências de checagem especializadas principalmente nas notícias que mais viralizam nas redes. Algumas delas:

- **Agência Lupa**
- **Aos Fatos**
- **Estadão Verifica**
- **Projeto Comprova**
- **Agência Pública**

Além delas, também vale conhecer sites que atuam desvendando boatos e montagens que circulam pelas redes sociais. Eles não necessariamente seguem os princípios de checagem de notícias, mas ajudam a entender como certas correntes, montagens e boatos se espalham nas redes:

- **E-Farsas**
- **boatos.org**

O **vídeo da série produzida com os jovens do Cidadão Digital** faz um excelente resumo com dicas práticas aplicadas ao contexto da desinformação em saúde. Pode ser um ótimo disparador de debates com os estudantes em atividades remotas ou presenciais. Veja na barra ao lado:

VIDEO



**6.5**



# RESPONSABILIDADE DAS PLATAFORMAS

No webinar, falamos bastante sobre a responsabilidade das plataformas de redes sociais a respeito do problema. No Brasil, é importante lembrar, o Marco Civil da Internet (**Lei nº 12.965/2014**) assegura que são os usuários os responsáveis pelos conteúdos postados na Internet. As plataformas só estão obrigadas a retirar conteúdos do ar após decisão judicial — com exceção de material íntimo, cuja retirada deve ser feita após solicitação direta da pessoa violada. Vale lembrar que as principais plataformas de redes sociais possuem regras de comunidade, ou seja, regras do que pode ou não ser postado naqueles espaços.



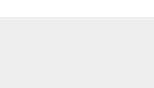
**LEI SOBRE "FAKE NEWS"**

Em 2019, a Safernet esteve em audiência pública no Senado Federal tratando do tema fake news e desinformação (**assista aqui**). Importante destacar que não apenas a Safernet, mas também outras organizações da sociedade civil afirmaram a necessidade de cautela ao tratar do tema em legislações devido a sua implicação direta com direitos como a liberdade de expressão. Foi emitida uma nota a respeito dos problemas do PL 2630 com relação aos direitos da infância e juventude (**leia aqui**), e a Coalizão Direitos na Rede também listou os principais problemas do relatório final (**leia aqui**). A lista de notas da sociedade civil, empresas, acadêmicos e comunida-de técnica está disponível **aqui**.

### REGRAS DE COMUNIDADE DE REDES SOCIAIS

-  [Padrões de Comunidade do Facebook - Notícias Falsas](#)
-  [Verificação de fatos no Facebook \(para empresas\)](#)
-  [Regras do Twitter](#)
-  [Diretrizes da Comunidade do TikTok](#)
-  [Diretrizes da Comunidade do Instagram](#)
-  [Diretrizes de Comunidade do Youtube](#)
-  [Termos de serviço do Youtube Kids](#)

### RELATÓRIOS DE TRANSPARÊNCIA SOBRE A APLICAÇÃO DESSAS REGRAS:

-  [Facebook e Instagram](#)
-  [Twitter](#)
-  [Youtube](#)
-  [TikTok](#)

**REPORTAGEM**





[INFORMAÇÕES FALSAS SOBRE COVID-19](#)

**REGRAS**



[NOVAS REGRAS DO FACEBOOK](#)



[REGRAS NO TWITTER](#)



[REGRAS NO TIK TOK](#)



6.6

# FERRAMENTAS

Não existe um caminho único para a checagem de conteúdos e notícias, e muitas vezes uma simples pesquisa no Google já é suficiente para retornar sites confiáveis de checagem que desmentem ou explicam melhor o contexto de conteúdos que viralizaram. Além das dicas dadas na seção “Análise crítica de mídias”, separamos algumas dicas práticas que podem ajudar você a investigar um conteúdo. Essas ferramentas também são bacanas para compartilhar em suas atividades educativas.

1 Usando o modo anônimo do seu navegador, use o **Google**, o **DuckDuckGo** ou outro site de pesquisa para investigar o conteúdo. Jogue palavras-chave que têm a ver com ele e inclua expressões como "é verdade" ou "checagem". Analise os resultados e, se não houver nenhum site confiável (como o de veículos de jornalismo profissional ou de checagem de fatos), tente filtrar os resultados por mais

recentes, como no último mês ou último ano. Você também pode usar a **pesquisa avançada do Google** para obter resultados mais apurados.

2 Utilize as pesquisas avançadas e ferramentas nas redes sociais. Facebook, Twitter e Instagram possuem selos de verificação para contas de marcas e pessoas públicas, diminuindo a chance de que uma conta inautêntica se passe por outra. No Twitter, a **pesquisa avançada** permite saber se um determinado perfil de fato publicou um tweet (caso ele não tenha sido apagado).

3 Caso você se depare com um link que não está mais no ar, é possível procurá-lo no **Internet Archive**, que armazena arquivos de milhões de sites na web. Essa ferramenta também é útil para ajudar a descobrir se um mesmo conteúdo foi postado de uma forma e depois alterado.

4 Para checar a autenticidade de imagens, use o **TinEye** (ajuda a descobrir quando uma imagem foi publicada pela primeira vez na Internet) ou a pesquisa por imagens do **Google Imagens**. Com essas ferramentas, é possível entender se uma imagem é recente ou não. Caso ela tenha sido usada para reforçar uma notícia que se diz recente, mas está circulando há anos na Internet, provavelmente se trata de desinformação — não confunda com imagens de arquivo que são usadas de forma ilustrativa, inclusive por veículos jornalísticos, como quando a matéria é sobre desemprego e a foto ilustrando é de uma carteira de trabalho; nesses casos, a foto não serve para reforçar um fato em si, e sim para ilustrar um contexto maior. Em alguns casos, essas ferramentas ajudam também a descobrir imagens que foram manipuladas.

PARA SABER MAIS



MAIS SOBRE O GOOGLE IMAGES



MAIS SOBRE MANIPULAÇÃO DE FOTOS



INTERNET ARQUIVO

## 6.6 CONTINUAÇÃO

**5** O **InVid Project** (em inglês) permite a busca por vídeos a partir de frames congelados. Útil para tentar rastrear um vídeo e saber se ele foi postado em algum site anteriormente.

**6** Caso você queira confirmar um dado específico, use a máxima do jornalismo de “ir direto na fonte”. Ou seja, procure pelo site da organização dada como fonte daquele dado e tente confirmar se tanto ela quanto o dado realmente existem. Por exemplo: se houver a citação de que “segundo o Instituto de Pesquisa X, mais de Y% dos brasileiros aprova medida Z”, pesquise diretamente pelo nome do instituto e depois pelo dado apresentado. Se o dado for público, ele provavelmente estará disponível no site. Se não houver menção a ele em nenhum outro lugar ou não houver confirmação no site oficial, desconfie. Também desconfie de dados que vêm de organizações

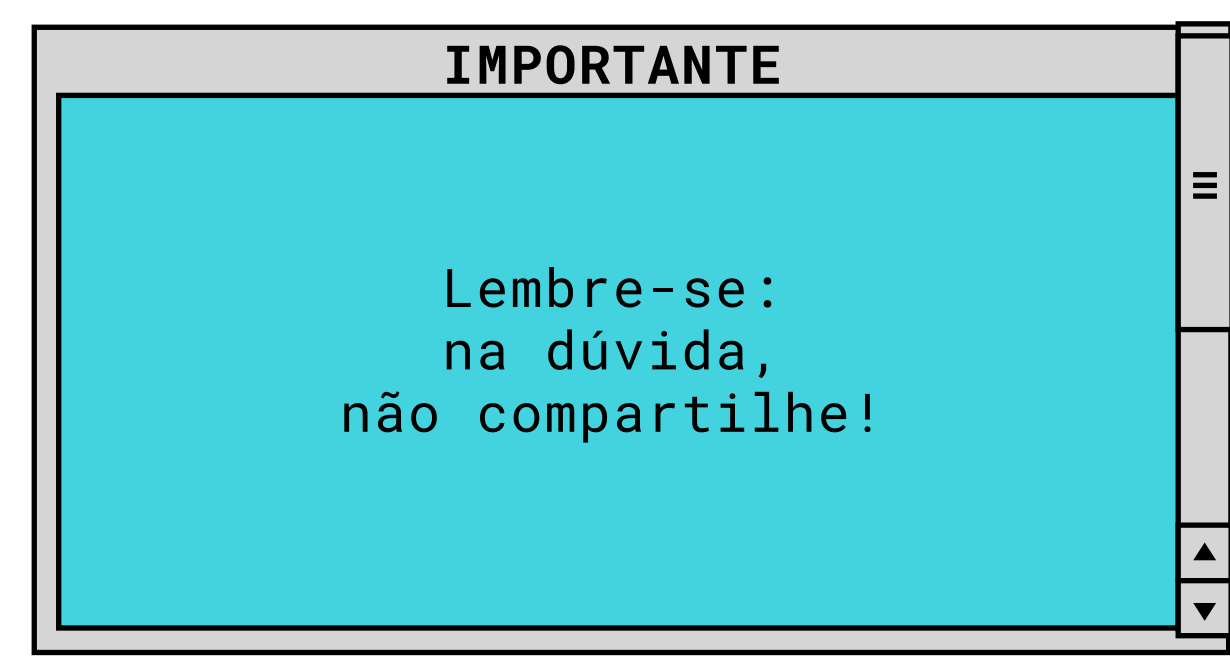
com pouca relevância. Existem “institutos de pesquisa” privados que publicam dados com pouca confiabilidade. Você pode usar o **Google Acadêmico** para pesquisar se determinado instituto de pesquisa figura como referência bibliográfica em um artigo científico. Ou procurar menção a ele em alguns veículos jornalísticos. Esses são possíveis indicativos de que se trata de uma fonte confiável — mas nunca baseie seu julgamento apenas por isso, sempre procure mais indícios de confiabilidade.

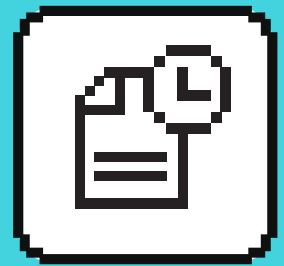
**7** Atenção a detalhes. Pequenos sinais podem indicar a possibilidade de o conteúdo ter sido manipulado ou estar descontextualizado. Lembre-se que nem sempre o conteúdo é totalmente falso.

**8** Caso confirme que se trata de desinformação, divulgue o que você encontrou, mas evite repostar o

conteúdo original — já que isso pode levar a mais visualizações e engajamento nas redes. Você pode, inclusive, relatar para as pessoas na sua rede caso você tenha buscado informações e não tenha encontrado; assim, mais pessoas podem procurar sobre e manter-se alertas.

**9** Como falamos, nem sempre é possível determinar se o conteúdo é verdadeiro ou falso. Podemos usar, por exemplo, o esquema de checagem da agência **Aos Fatos**, que classifica os conteúdos em verdadeiro, impreciso, exagerado, distorcido, contraditório, insustentável ou falso.





**A1**  
**ATIVIDADE 1**

## Caminhos de Checagem

**Objetivo:** Imagine que você está fazendo mais uma ação com os adolescentes da comunidade que referimos no tópico "Privacidade e reputação" (que vai receber pela primeira vez a internet). Você será responsável por debater um destes temas: privacidade e reputação, comportamentos positivos, autocuidado ou ações inspira-doras on-line. Como parte da sua atividade, você irá mostrar como podemos investigar se uma notícia ou conteúdo (vídeo, imagem, mensagem viral) sobre um desses temas é verdadeiro ou contém desinformação

### Como funciona

Agora começa o desafio: selecione uma notícia ou conteúdo que tenha circulado nas redes no último mês e que pareça potencialmente falsa ou enganosa — retome as dicas que demos sobre esse tipo de identificação.

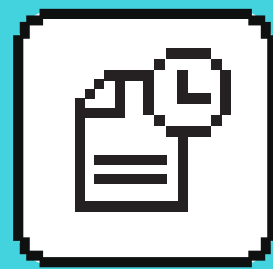
Seguindo a proposta, esse conteúdo deve estar relacionado a algum dos temas debatidos nestes itinerários de formação do Cidadão Digital. Faça o caminho da checagem, seguindo as dicas de passo a passo que exploramos no bloco ferramentas. Descreva esse caminho do início ao fim na forma de lista numerada: pode ser por meio de infográfico, cards (imagens), vídeo, thread (fio) do Twitter, texto do tipo blog post, ou outra forma que você preferir. O importante é que você consiga contar como fez a checagem, imaginando que está explicando seu passo a passo para os adolescentes que vão receber o material. Se possível, inclua prints que ajudem a entender o que você fez. A ideia é mostrar que a checagem é possível, embora você também possa

relatar as dificuldades que porventura teve no processo.

Ao final, dê o seu veredito, classificando a notícia ou conteúdo em verdadeiro, impreciso, exagerado, distorcido, contraditório, insustentável ou falso, e explicando o porquê (use a lista de sete tipos de desinformação). Caso queira, você pode compartilhar o seu caminho da checagem nas suas redes, usando as hashtags #CidadãoDigital e #ChecagemDeFatos.

### Para refletir

**Assim que concluírem** as atividades com os estudantes, convide-os a comentar sobre o processo. Acharam difícil? Teve alguma informação procuraram e não conseguiram encontrar? Por que acham que as pessoas ainda praticam pouco a checagem de conteúdos que elas postam ou compartilham nas redes? Que estratégias podemos adotar para tornar essa prática mais popular na escola / instituição?



A1

**ATIVIDADE 1****Teste do "Falso"**

**Objetivo:** Dar início ao assunto desinformação (“fake news” e conteúdos enganosos) de maneira divertida com o público jovem, por meio de uma proposta que envolve autoria, criatividade e investigação.

**Recursos e materiais**

Você pode implementar a proposta já no período de ensino remoto, utilizando um sistema de enquete on-line (como **Enquetes** ou **Perguntas** no Instagram ou no **Facebook**, o **“StrawPoll”** ou mesmo um Google Form) e uma sala de webconferência que estiver disponível em sua instituição e seja conhecida pelos estudantes (atualmente o **Google Meet** e o **Zoom** possuem a função enquete disponível), assim como adotá-la no modelo presencial: neste caso, bastará ativar a imaginação dos estudantes!

**Contextualizando**

Conforme a BNCC (BRASIL, 2018, p. 136), “a questão da confiabilidade da informação, da proliferação de fake news, da manipulação de fatos e opiniões tem destaque e muitas das habilidades se relacionam com a comparação e análise de notícias em diferentes fontes e mídias”. A alfabetização midiática é uma demanda urgente, estimulando a análise crítica de fontes e informações.

**Como funciona**

Convide os alunos para que, individualmente, criem sentenças a seu respeito, podendo ser verdadeiras ou falsas. Por exemplo: “João tem cinco cachorros e dois gatos. Eles passeiam juntos todos os dias.” - “Ana adora ler e é um tanto distraída. Certa vez, o último capítulo de um romance fez com que descesse do ônibus seis paradas depois da sua.”

No formato remoto, cada estudante pode cadastrar sua sentença em uma enquete on-line.

Reunidos numa sala de webconferência com o serviço de chat, será o momento da votação. Cada aluno compartilhará a enquete com a sua sentença e a colocará em votação para a turma (as opções serão apenas “Verdadeiro” ou “Falso”).

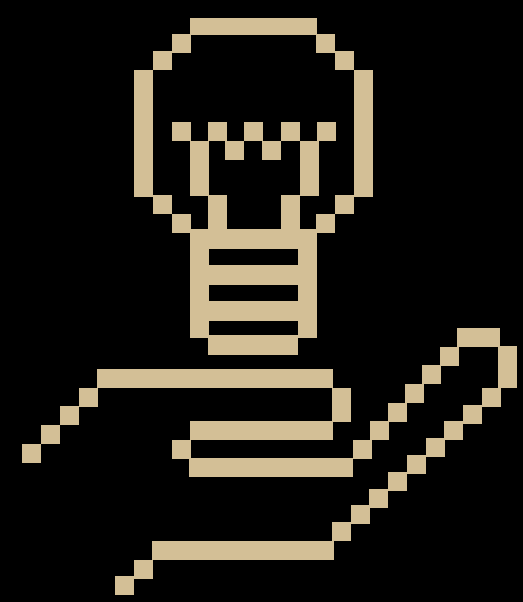
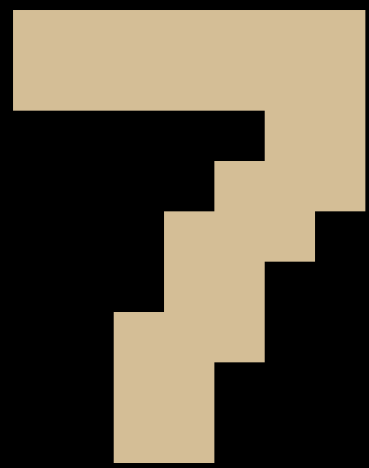
**Para refletir**

Como cada enquete gera um percentual de respostas, ao fim da dinâmica você pode solicitar que socializem as sentenças todos aqueles que criaram textos pessoais inverídicos

e obtiveram, por exemplo, mais de 60% de respostas “Verdadeiro”. Este é um mote para discutir as estratégias utilizadas para tornar críveis informações que eram falsas, abrindo oportunidade para o aprofundamento nos conceitos discutidos no módulo, incluindo meios de checagem e averiguação da qualidade editorial. Algumas questões podem ajudar. Para quem considerou verdadeiras sentenças falsas, pode-se questionar o que motivou tal palpite: a maneira como a frase estava construída? O conteúdo? Para aqueles que “acertaram”, pode-se indagar: o que denunciou que a sentença não era verdadeira? Que pistas havia? Será que podemos usar esses mesmos parâmetros na análise dos conteúdos das redes sociais e de outras mídias?

Mais perguntas são interessantes: Como diferenciar opinião de fato? Como diferenciar opinião de fato? Que cuidados e medidas tomar quando confirmamos que uma notícia é falsa? Como podemos orientar amigos e familiares quando vemos que compartilharam uma notícia falsa?

CAPÍTULO



# AÇÕES INSPIRADORAS

Ufa! Chegamos ao último bloco desta formação! Uma das lições que esperamos que você tenha captado é que os temas são transversais, ou seja, estão sempre relacionados e sempre se influenciando. Fecharemos com exemplos e dicas de ferramentas que podem ajudar a mobilizar, engajar e educar a partir dos recursos digitais.



### RESUMO



**5 HORAS**

**3 VIDEOS**


**1 SUGESTÃO DE ATIVIDADE**

Estratégias de criação, inovação, adesão e engajamento, cultura digital, pensamento computacional, robótica, programação e produção multimidiática (vídeos, podcasts, jogos) são alguns dos elementos que podem ser trabalhados e que são vitais ao desenvolvimento integral dos jovens na atualidade.



### PARA ASSISTIR

Webinar com o Steve ePonto, estrategista criativo do Facebook, e Nina da Hora, Cientista da Computação, pesquisadora, e hacker antirracista (@ninadhora). A mediação foi de Andrea Leal (Facebook).




### PARA SABER MAIS SOBRE O TEMA

Campanhas com recursos em vídeo que podem ajudar a realizar atividades pedagógicas com o tema.

**Guia com atividades**  
Estratégias voltadas para atividades presenciais ou híbridas



### PARA APLICAR EM SALA DE AULA

Recursos práticos para usar em sala de aula (remota ou presencial)



**SUGESTÃO DE ATIVIDADES**


**ATIVIDADE 1**

Cidadania Digital - Ativar!

### OUTROS MATERIAIS COMPLEMENTARES

Confira material extra na versão online da formação para aprofundar seus conhecimentos.

- Plataforma Juventude, Educação e Trabalho, da Fundação Roberto Marinho
- Pesquisa Juventudes e Pandemia do Coronavírus (Conjuve)
- Guia de implementação de estratégias de aprendizagem remota (CIEB)
- #OrgulhodeSer, vídeos no Youtube sobre visibilidade LGBT+
- Guia de Podcasts Negros
- Notícias inspiradoras



7.1

# CONTEXTO

Alimentar nossa criatividade é sempre muito poderoso para ter inspirações e traduzir os conteúdos em atividades que façam sentido para as e os adoles-centes de seu contexto. Neste bloco último bloco temos dicas de ferramen-tas que podem mobilizar, engajar e educar a partir dos recursos digitais.

Sabemos que mesmo antes da pandemia, tanto estudantes quanto educadores já usavam muito a Internet pelo celular dentro e fora das escolas. Os dados da pesquisa **TIC Educação 2019 (CETIC.br)** confirmam este cenário, e apontam que os aplicativos de mensa-gens instantâneas (como o Whatsapp) são os mais usados nas atividades escolares, seguidos pelas redes sociais.

Professoras e professores buscam criar formas de comunicação e interação com as e os estudantes usando a Internet em diferentes atividades.

Com a pandemia da Covid-19 e o fechamento de escolas em 2020, as atividades remotas vieram de vez como forma de tentar manter os processos de aprendizagem, ainda que à distância. A **Pesquisa Pannel Covid-19 - 3ª edição**, lançada pelo CETIC.br em novembro de 2020, reforça que o celular foi o dispositivo mais usado em atividades remotas: 69% dos estudantes brasileiros com 16 anos ou mais afirmam que usaram para participar de atividades escolares durante a pandemia. Do total de estudantes com 16 anos ou mais, 82%

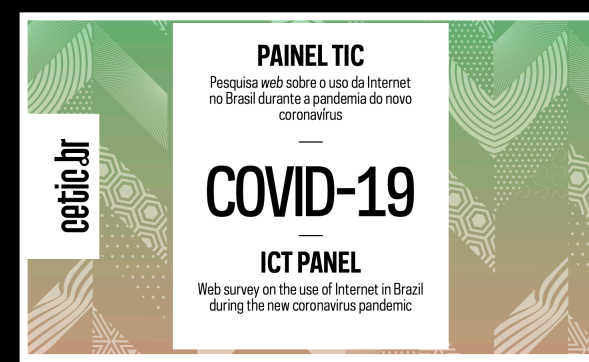
afirmaram que acompanharam alguma atividade remota ofertada pela escola ou universidade durante a pandemia.

A Pesquisa da Fundação Carlos Chagas, realizada entre abril e maio de 2020 com mais de 14 mil educadoras/es, aponta as redes sociais, orientações às famílias e materiais digitais como principais alternativas usadas para manter contato. Entretanto, é importante ter ciência de que o ensino remoto não acontece sem problemas. À falta de equipamentos e conexão de boa qualidade à internet somam-se as dificuldades de professoras/es e estudantes em aprender de forma totalmente virtual. Vamos ver algumas dessas questões.

PESQUISAS



**TIC EDUCAÇÃO 2019 (CETIC.BR)**



**PAINEL COVID-19**



**FUNDAÇÃO CARLOS CHAGAS**



**EDUCAÇÃO ESCOLAR**

## 7.1 CONTINUAÇÃO

Há diferenças entre os níveis de ensino. A Fundação Lemann realizou um mapeamento inicial da educação não presencial em maio de 2020, indicando, por exemplo, que 86% dos estudantes do ensino médio tiveram acesso a atividades remotas àquela época, contra 70% de estudantes do ensino fundamental I.

Como vimos desde o primeiro webinar, as desigualdades econômicas e regionais não podem ser ignoradas, pois significam experiências e oportunidades muito diferentes.

Precisamos lembrar que as escolas se adaptaram de formas muito diferentes ao fechamento durante a pandemia: enquanto umas aderiram ao ensino remoto já em março de 2020, outras demoraram meses para tal, e há ainda escolas que apostaram em estratégias que não dependiam da internet, adotando material impresso entregue nas casas das e dos estudantes e aulas via TV educativa.

Em 2021, tivemos o retorno às aulas presenciais em algumas redes, em um processo marcado, novamente, pelas diferenças entre os estados do país. O Conselho Nacional de Educação (CNE),

que assessora o Ministério da Educação (MEC), autorizou o ensino remoto até dezembro de 2021, embora já haja um protocolo de retomada de atividades presenciais preparado pelo Conselho Nacional de Secretários de Educação (CONSED) em 2020, apontando diretrizes mínimas para que isso ocorra com segurança. Tudo isso indica, portanto, que ao longo de 2021 teremos diferentes situações se apresentando, incluindo se considerarmos o possível avanço na vacinação contra a Covid-19.

Ao realizar atividades com uma escola, é essencial buscar entender previamente qual é o contexto na qual ela está inserida. Algumas perguntas que podem ser feitas para as e os professores, e mesmo estudantes, em um levantamento anterior, são:

**- Qual é a situação de conectividade das e dos estudantes?**

**- A escola sabe se o acesso à banda larga faz parte da vida da maioria? Se não, o acesso é por redes móveis (3G, 4G)?**

**- O que tem dado certo e o que não tem funcionado?**

O projeto “Conectividade na Educação”, do NIC.br e do CIEB pode ajudar você nessa investigação. O mapa traz dados sobre conectividade nas escolas de todo o país.

Essas informações são muito úteis e poderão ajudar você a planejar uma atividade remota utilizando plataformas que funcionem para a realidade daquela escola.

**- Como têm acontecido as aulas na escola? São remotas, presenciais ou híbridas?**

**- Se remotas, por quais meios de comunicação? E plataformas/sites?**

**UM RECADO**

Sabemos que o contexto é preocupante, e é justamente por isso que buscamos que o Cidadão Digital seja um auxiliar da educação e dos desafios que adolescentes, educadoras/es e famílias têm enfrentado. Com leveza, humor e criatividade, podemos contribuir para que o cenário educacional se torne melhor!



**7.2**

# PROJETOS INSPIRADORES

Aproveitando os caminhos apontados nos webinars, podemos avançar na construção de atividades remotas e presenciais usando as redes e recursos que estudantes e professores já conhecem.

As próprias atividades que você viu ao longo desta formação podem servir como inspiração nas suas atividades. Eles funcionam melhor em contextos nos quais você terá um contato mais duradouro com uma turma, realizando

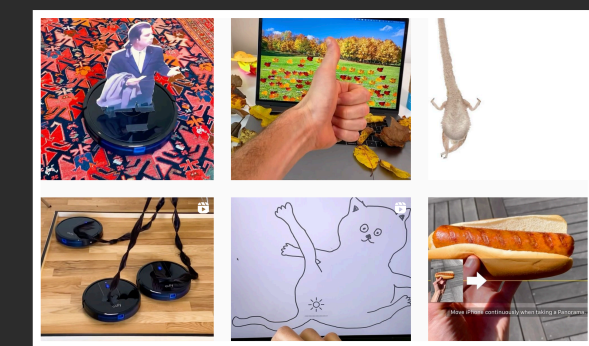
A **versão do Guia Cidadão Digital** foi pensada antes da pandemia e, portanto, tem a maior parte de suas estratégias voltadas para atividades presenciais. Considerando nossa realidade, estamos juntas e juntos criando alternativas para a aplicação dos temas no formato de ensino remoto e híbrido. Podemos adaptar estratégias e criar outras, partindo principalmente de ações inspiradoras que acontecem nas redes.



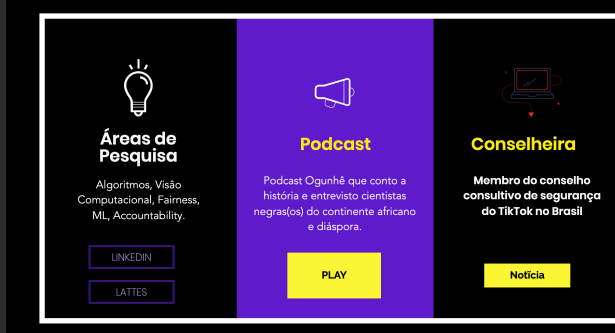
um ciclo de mais de uma atividade. Assim, é possível ter momentos para lançar os desafios e trazer feedback. Que tal uma gincana de quizzes, ou um concurso de melhores cards criados apenas com as ferramentas de edição dos Stories do Instagram? As possibilidades são muitas!

Há muitas ferramentas disponíveis para criação de conteúdos, a exemplo do Mobile Studio. Os materiais disponibilizados no site do Cidadão Digital também são boas fontes de inspiração para as atividades com as escolas, com memes, vídeos e cards. **Falando em memes, vale conferir esta orientação para usar com responsabilidade.**

**PROJETOS INSPIRADORES**



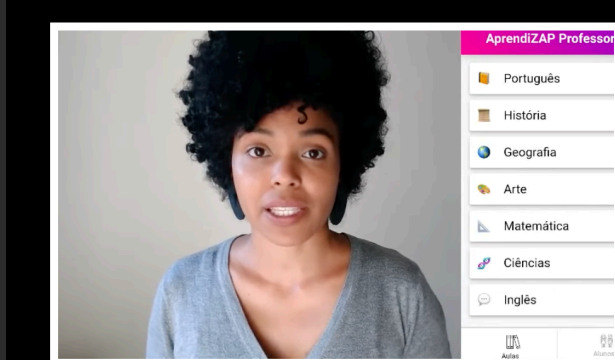
[@PABLO.ROCHAT](#)



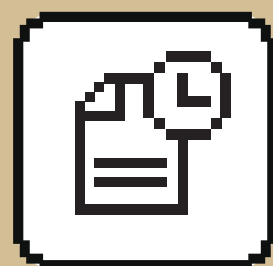
[NINA DA HORA](#)



[METODOLOGIAS ATIVAS](#)



[APRENDIZAP](#)



A1

## ATIVIDADE 1

## Cidadania Digital: Ativar!

**Objetivo:** Propor um exercício de construção e autoria, por parte dos estudantes, com foco na cidadania digital, de maneira a ampliar a mobilização acerca de um dois eixos temáticos abordados na formação.

### Recursos e materiais

Dispositivos móveis com um ou mais entre os aplicativos sugeridos instalados para a produção de uma pequena peça de comunicação.

### Contextualizando

Na sua fala para o webinar “Como usar as redes sociais para inspirar e mobilizar adolescentes?”, Steve ePonto enfatizou que é importante “ter a mensagem certa para pessoas certas no momento certo”. A iniciativa com os alunos têm, portanto, um propósito misto: a realização de escolhas técnicas, estruturais e de linguagem para compor um material informativo de impacto, exercitando “práticas de linguagem do campo jornalístico e do campo midiático de forma ética e responsável” (BNCC - BRASIL, 2018, p. 143).

### Como fazer?

A proposta de atividade consiste em desafiar os estudantes a produzirem uma chamada sobre cidadania digital, com foco em um dos eixos abordados na formação.

### DICAS

- Call to action: a chamada ou o anúncio deve apresentar um convite claro à ação do interlocutor (siga, faça, apoie, etc.);
- Produção de 15 segundos (capture a atenção rapidamente): é um verdadeiro desafio compactar a mensagem dessa maneira, não?
- Crie com som desligado: conteúdo que possa ser examinado e compreendido por meio do texto e da imagem, sem o som. Inserir legendas é útil e torna seu conteúdo mais acessível
- Estimule interatividade: encoraje os estudantes a buscarem meios de escutar seu público, via quiz, enquetes, fóruns.
- Aproveite as ferramentas: **aplicativos criativos, ferramentas gratuitas**

### Para refletir

Promover a avaliação por pares salientando a importância de trocas e devolutivas respeitadas, construtivas e produtivas. Incitar a reflexão sobre a relevância do conteúdo x o imediatismo e a efemeridade das informações, o convite à análise crítica x formas de expressão sintéticas.

- Após a criação da “chamada” para a ação, que outros meios poderiam utilizar para aprofundar os assuntos relacionados à cidadania digital?
- Como tornar uma mensagem “marcante” diante da multiplicidade de ofertas nos meios digitais?
- O que significa impactar, mobilizar e gerar adesão?
- As redes digitais ajudam ou não nesses objetivos? Por quê?
- É possível estimular mudança concreta de comportamentos com estas mobilizações?

# CRÉDITOS

Publicado em setembro de 2021 sob licença Creative Commons Atribuição-Compartilhado 4.0 Internacional (CC BY-SA 4.0)

## COORDENAÇÃO E CONTEÚDOS

**Guilherme Alves**  
(Gerente de projetos SaferNet)

**Rodrigo Nejm**  
(Diretor de Educação SaferNet)

## REVISÃO

**Anna Emanuely Laurindo, Emanuella  
Ribeiro Halfeld Maciel, Isabella Ferro,  
Jade Christinne dos Santos e Lorena  
Santos Vilas Boas**  
(Mentoras Cidadão Digital 2021)

**Juliana Alencar**  
(Jornalista)

**Bianca Orrico**  
(Psicóloga - SaferNet)

## ESPECIALISTAS NOS WEBINARS

**Andrea Leal** - Facebook  
**Bruno Bioni** - Data Privacy Brasil  
**Daniele Fontes** - Facebook  
**Dario Durigan** - WhatsApp / Meta  
**Ecivaldo de Souza Matos** - UFBA  
**Gabriel Recalde** - Instagram  
**Karen Scavacini** - Vita Alere  
**Luísa Adib** - CETIC.br  
**Mariana Valente** - Internet Lab  
**Mônica Rosina** - Facebook  
**Nina da Hora** - Cientista da Computação  
**Nina Weingrill** - ÉNois  
**Raquel Saraiva** - Ip.Rec  
**Steve ePonto** - Facebook  
**Thiago Tavares** - SaferNet

# LICENÇA E REPRODUÇÃO



Fonte: [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



## VOCÊ TEM O DIREITO DE:

**COMPARTILHAR:** copiar e redistribuir o material em qualquer suporte ou formato

**ADAPTAR:** remixar, transformar e criar a partir do material, para qualquer fim, mesmo que comercial

## DE ACORDO COM OS SEGUINTE TERMOS:

**ATRIBUIÇÃO:** você deve dar o crédito apropriado, prover um link para licença e indicar se mudanças foram feitas. você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso

**COMPARTILHA/IGUAL:** se você remixar, transformar, ou criar a partir do material, tem de distribuir as contribuições sob a mesma licença que o original

REALIZAÇÃO



∞ Meta

