Como Fazer a Internet um Espaço Mais Seguro? Atualização Guias Internet Segura

Miriam von Zuben

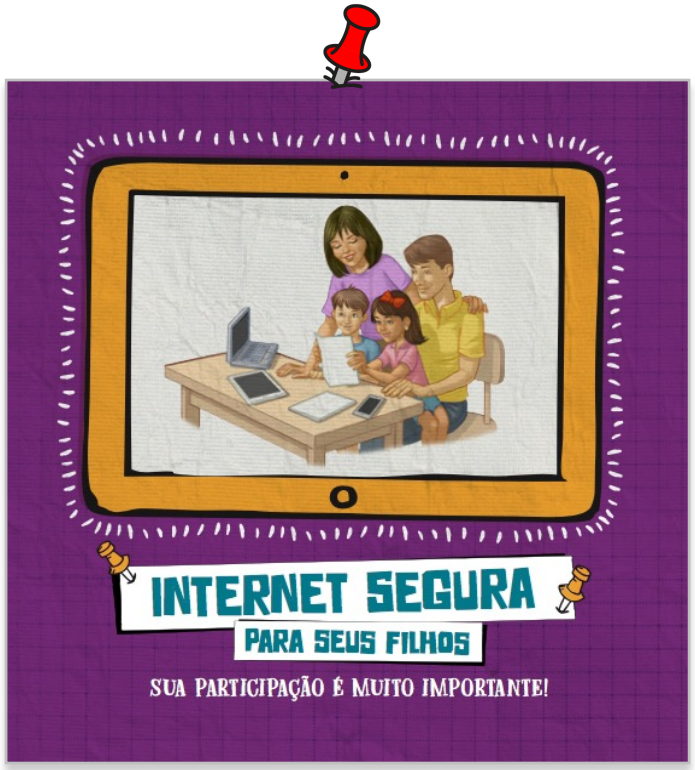
Analista de Segurança
CERT.br/NIC.br

11º Simpósio Crianças e Adolescentes na Internet
São Paulo, SP – 29 de outubro de 2026

cert.br nic.br cgi.br

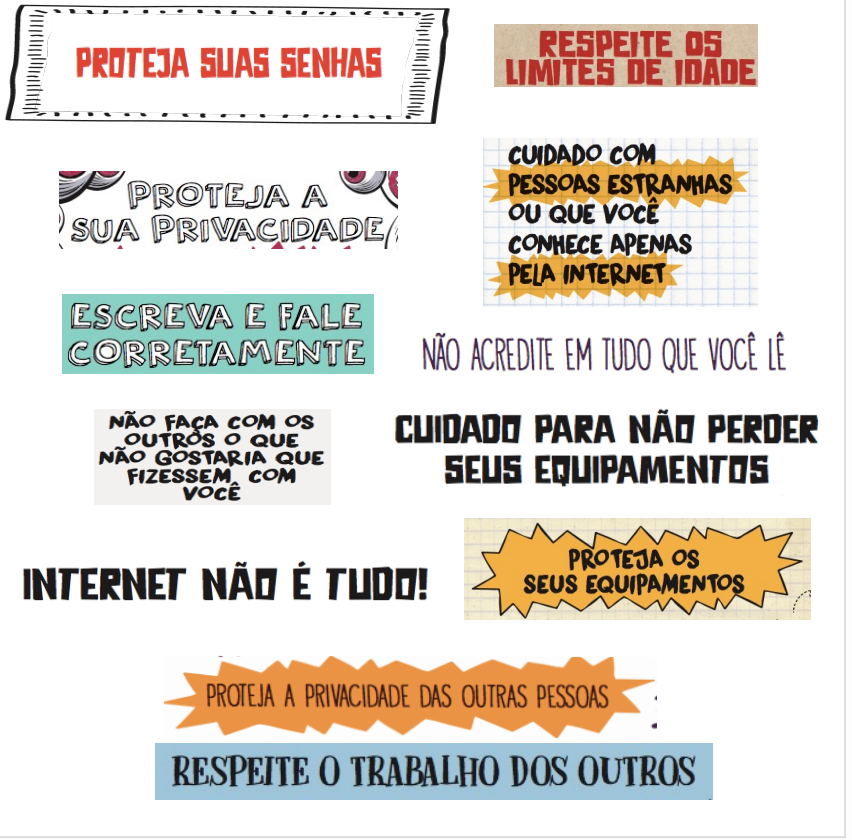
Guias Internet Segura
1ª Edição – 2017

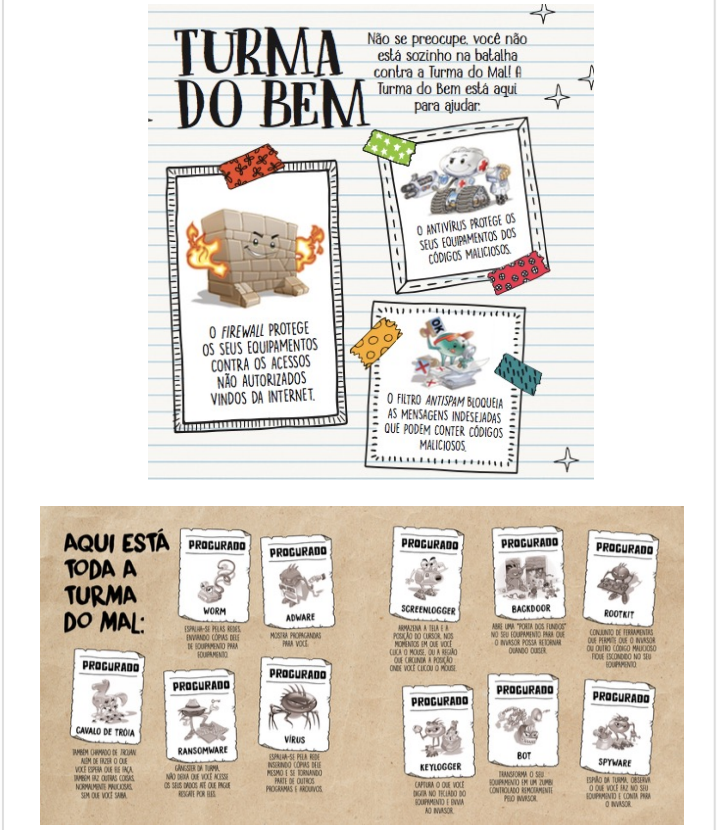




Guia Internet Segura – 1ª Edição
Divirta-se e aprenda a usar a Internet de forma segura!









Guia Internet Segura – para seus filhos – 1ª Edição
Sua participação é muito importante!









Exemplo
Diálogo
Pessoas estranhas
Comportamento

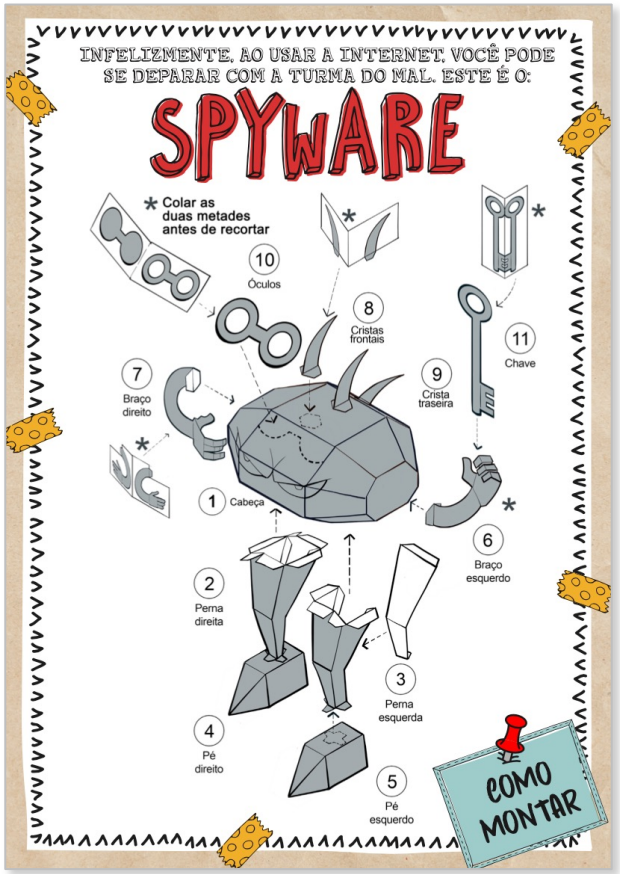
Privacidade
Cyberbullying
Limites de idade
Regras

Controle parental
Contas de acesso
Senhas
Equipamentos

Personagens para Montar – 10/2020







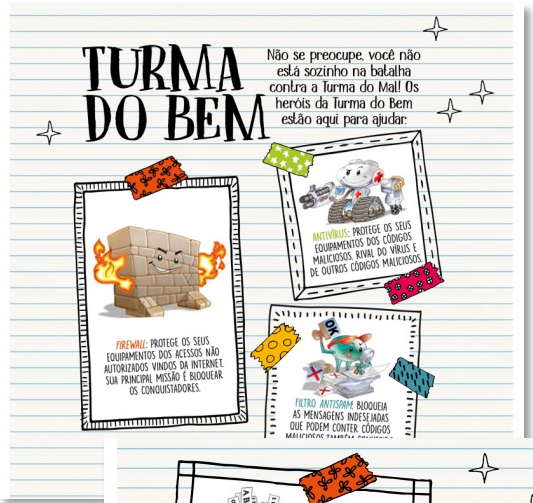


Guias Internet Segura
2ª Edição – 2022



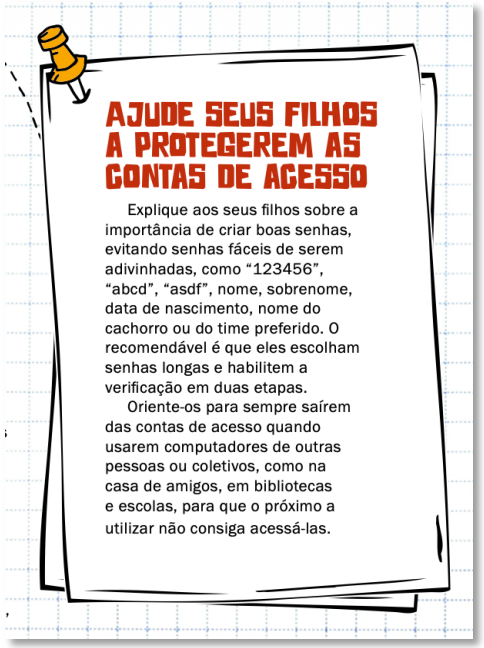


Guias Internet Segura – 2ª Edição
Principais Atualizações

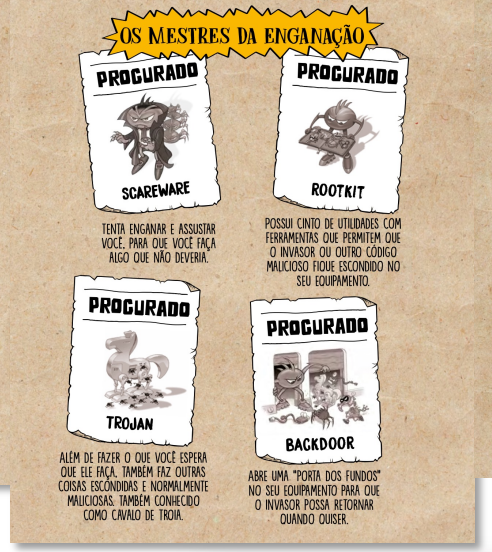














Jogos de Tabuleiro

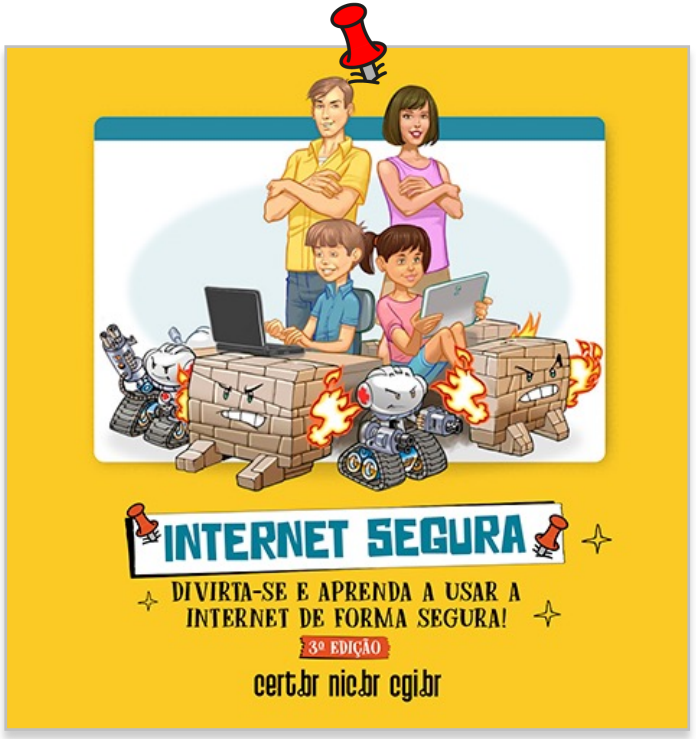


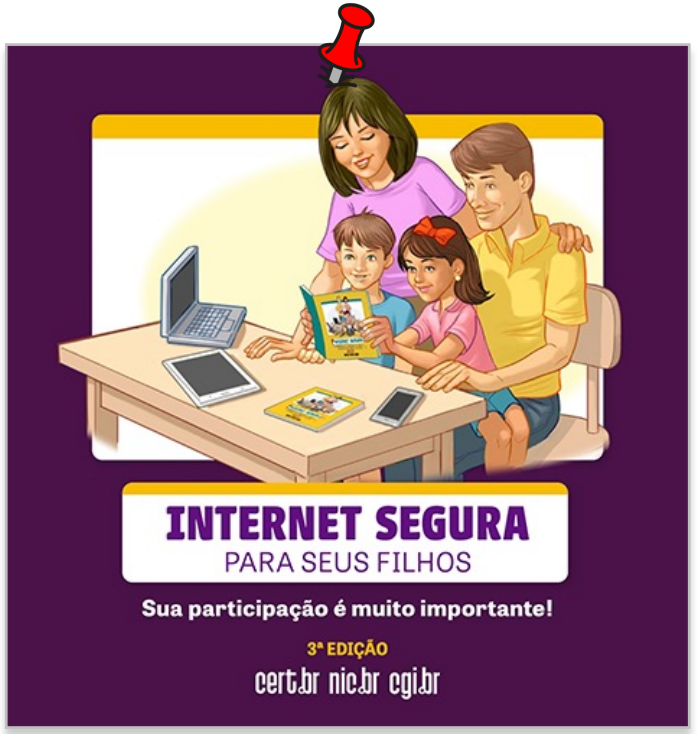
Comportamento Seguro
02/2024



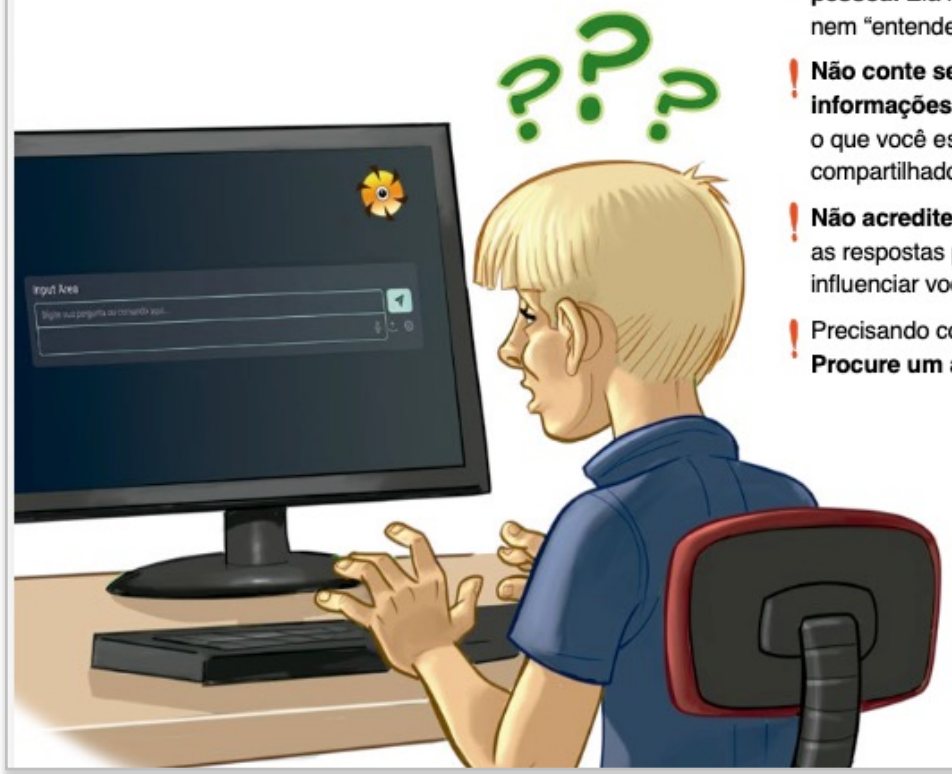
Segurança *Online*
02/2025

Guias Internet Segura
3ª Edição – 2026





CUIDADO AO CONVERSAR COM INTELIGÊNCIA ARTIFICIAL



- Lembre-se: a **IA não é uma pessoa.** Ela não tem emoçõe
  nem "entende" você.
- **Não conte segredos nem informações pessoais**:
  o que você escreve pode ser
  compartilhado com quem crio
- **Não acredite em tudo que a**
  as respostas podem estar erra
  influenciar você.
- Precisando conversar com alg
  Procure um amigo de verda



VAI USAR IA NA LIÇÃO DE CASA?



A IA PODE AJUDAR VOCÊ A ESTUDAR, EXPLICAR MATÉRIAS E DAR IDEIAS, MAS NEM SEMPRE ACERTA. **USE A IA COMO APOIO, CONFIRA AS INFORMAÇÕES E REVISE O QUE ELA PRODUZIR.**

A lição de casa ou o trabalho são seus.

O resultado deve mostrar o que você aprendeu e ser escrito com suas palavras.



NÃO ACREDITE EM TUDO NA INTERNET

Na Internet, nem tudo o que você vê, lê ou recebe é verdadeiro ou confiável. Conheça alguns exemplos.

SPAM É UMA MENSAGEM QUE VOCÊ RECEBE SEM TER PEDIDO, ENVIADA POR ALGUÉM QUE VOCÊ NÃO CONHECE.

BOATO É UMA INFORMAÇÃO QUE SE ESPALHA ANTES DE SABER SE É VERDADE.

CORRENTE É UMA MENSAGEM COM CONTEÚDO FALSO QUE PEDE PARA VOCÊ COMPARTILHÁ-LA RAPIDAMENTE COM MUITAS PESSOAS.

FAKE NEWS
É COMO SÃO CHAMADAS AS NOTÍCIAS QUE TENTAM SE PASSAR POR REPORTAGENS VERDADEIRAS E QUE POSSUEM CONTEÚDO FALSO, IMPRECISO OU DISTORCIDO.

DEEPFAKES
SÃO IMAGENS, VÍDEOS OU ÁUDIOS FEITOS OU MODIFICADOS POR IA PARA PARECER QUE UMA PESSOA FEZ OU DISSE ALGO, MESMO QUE NÃO SEJA VERDADE.

PROPAGANDA DISFARÇADA
(OU VELADA) É UM ANÚNCIO APRESENTADO COMO SE FOSSE UMA OPINIÃO OU CONTEÚDO COMUM.

NEM SEMPRE É FÁCIL RECONHECER ESSES CONTEÚDOS. POR ISSO, ANTES DE ACREDITAR OU COMPARTILHAR, PERGUNTE-SE:

- O conteúdo pede para eu compartilhar com muitas pessoas?
- Ele promete algo bom demais ou diz que algo ruim vai acontecer se eu não compartilhar?
- De onde veio essa informação?
- Essa informação aparece em outros lugares?
- Essa pessoa realmente diria ou faria isso?
- A imagem, vídeo ou áudio pode ter sido alterado?
- A mensagem fala sobre dinheiro, prêmios ou pede meus dados?
- Ela tenta me apressar, me assustar ou mexer com meus sentimentos?
- Estão tentando me induzir a comprar algo?



USE SERVIÇOS ADEQUADOS PARA SUA IDADE

VOCÊ JÁ REPAROU QUE ALGUNS JOGOS, *APPS* E REDES SOCIAIS TÊM UMA IDADE MÍNIMA PARA SEREM USADOS?

ESSA INFORMAÇÃO APARECE NAS REGRAS DO SERVIÇO OU NA CLASSIFICAÇÃO INDICATIVA. ELA AJUDA A SABER SE O SERVIÇO É ADEQUADO PARA A SUA IDADE.

O QUE ACONTECE QUANDO VOCÊ USA UM SERVIÇO NÃO ADEQUADO PARA SUA IDADE?

QUANDO ISSO ACONTECE, ALGUMAS PROTEÇÕES ESPECIAIS OFERECIDAS PARA CRIANÇAS PODEM NÃO ESTAR DISPONÍVEIS E VOCÊ FICAR MAIS EXPOSTO A CONTEÚDOS, CONTATOS, FUNCIONALIDADES OU SITUAÇÕES QUE COLOQUEM VOCÊ EM RISCO.

RESPEITE AS RESTRIÇÕES DE IDADE

VOCÊ SABE O QUE É CLASSIFICAÇÃO INDICATIVA?

A CLASSIFICAÇÃO INDICATIVA[1] AJUDA A SABER PARA QUAL IDADE UM JOGO OU *APP* É ADEQUADO. ELA NÃO CONSIDERA APENAS O QUE APARECE NELE, TAMBÉM LEVA EM CONTA O QUE PODE ACONTECER QUANDO VOCÊ USA O SERVIÇO. POR EXEMPLO:

- VOCÊ CONSEGUE INTERAGIR COM OUTRAS PESSOAS OU COM UMA IA?
- VOCÊ PODE FAZER COMPRAS?
- SUA LOCALIZAÇÃO PODE SER COMPARTILHADA?
- VOCÊ PODE COMPARTILHAR FOTOS, VÍDEOS OU ÁUDIOS?
- O JOGO OU *APP* PODE RECOMENDAR CONTEÚDOS PARA VOCÊ?

Essas informações ajudam a definir a classificação indicativa. Ela pode ser "livre" ou indicar que o jogo ou *app* não é recomendado para menores de 6, 10, 12, 14, 16 ou 18 anos.

[1] https://www.gov.br/mj/pt-br/assuntos/seus-direitos/classificacao-1/classind-audio-visual-2025-vs-10-nova-faixa.pdf



CONHEÇA OS RISCOS

O ambiente digital oferece muitas oportunidades para seus filhos aprenderem, criarem, se divertirem e manterem contato com familiares e amigos. Mas também existem riscos que você precisa conhecer para poder orientá-los e protegê-los.

CONTATO COM PESSOAS MAL-INTENCIONADAS

- Pessoas mal-intencionadas podem ganhar a confiança das crianças para **obter informações pessoais ou imagens íntimas e envolvê-las em situações de exploração e abuso sexual.**
- O contato também pode envolver **ameaças e chantagens** (sextorsão), além de **perseguições e contatos insistentes e indesejados** (*cyberstalking*).
- Crianças também podem sofrer **tentativas de influência ou recrutamento** por pessoas ou grupos que promovem o ódio, ideias extremistas ou violência.

SITUAÇÕES OFENSIVAS OU PREJUDICIAIS

- Crianças podem ser **vítimas de *cyberbullying*** e de outras situações de ofensa, exclusão ou humilhação.
- Crianças também podem **compartilhar conteúdos que ofendam, ridicularizem ou prejudiquem outras pessoas**, mesmo sem essa intenção.

CONTATO COM CONTEÚDOS INADEQUADOS

- Crianças podem se deparar com **conteúdos violentos, extremistas, ofensivos, manipulados ou falsos**, inclusive gerados ou modificados por Inteligência Artificial (IA).
- De forma intencional ou acidental, elas podem ter contato com **pornografia ou outros conteúdos sexualmente explícitos**.
- Elas podem encontrar ainda **conteúdos que incentivam comportamentos prejudiciais à saúde**, como automutilação e práticas alimentares nocivas.
- Plataformas, *sites* e aplicativos podem expor as crianças a **conteúdos que incentivam apostas *online***, exploram sua vulnerabilidade e estimulam comportamentos de risco.



PUBLICIDADE E CONSUMO

- Crianças podem ter contato com **conteúdos que divulgam marcas ou produtos**, como publicações de influenciadores ou criadores de conteúdo, **sem perceber que se trata de publicidade**.
- Dados de crianças podem ser cole… e usados por empresas para **direci… publicidade personalizada, recom… conteúdos ou produtos e influenci… hábitos de consumo e seu compor…**

GOLPES E RISCOS DE SEGURAN…

- Crianças podem sofrer **tentativas d… manipulação para obter informaçõ… pessoais, acessar contas ou explor… recursos financeiros da família.**
- Os **dispositivos** usados pela criança… ser **invadidos ou infectados** por cód… maliciosos (*malware*), compromete… dados e contas.
- **Nomes, fotos ou outras informaçõe… ser usados por terceiros** para criar… falsos e se passar pela criança.



RISCOS À PRIVACIDADE

- A divulgação inadequada ou excessiva de informações, fotos e vídeos da criança pode **criar uma presença digital antes que ela possa decidir sobre isso.**
- Em conversas com *chatbots* e outras ferramentas de IA, as crianças podem **compartilhar informações pessoais sem perceber como poderão ser usadas.**
- **Brinquedos conectados**, como bonecas "inteligentes", **podem coletar dados e permitir interações *online***, sem que os riscos envolvidos e os cuidados necessários estejam claros.

RISCOS AO BEM-ESTAR

- **Ferramentas de IA podem simular relações de amizade e afeto e influenciar emoções e comportamentos, aumentando o risco de manipulação.**
- Crianças podem ter **dificuldade para lidar com críticas, avaliações negativas e interações abusivas**, o que pode gerar frustração, ansiedade e baixa autoestima.
- Plataformas podem usar recursos para prolongar o uso e estimular interações frequentes em redes sociais, jogos e aplicativos de vídeos.
- **O uso excessivo de telas pode afetar a saúde física e mental, o desenvolvimento, o rendimento escolar e a vida social.**

cert.br nic.br cgi.br

NÃO SEJA VOCÊ O VILÃO

O compartilhamento excessivo de informações, fotos e vídeos sobre as crianças pela família, conhecido como *sharenting*, também pode colocá-las em risco.



- Expor informações sobre a rotina dos filhos, como onde estudam, quais atividades realizam e quais locais frequentam, pode **aumentar os riscos à segurança e à privacidade.**
- Publicações frequentes sobre os filhos podem resultar em **exposição contínua, pressão por desempenho, busca por aprovação e comentários ofensivos.**
- **Fotos de crianças nuas ou seminuas,** mesmo quando publicadas sem má intenção, como registros durante o banho, em momentos de troca de roupa ou na praia, **podem ser usadas para fins de exploração sexual.**
- Comentários negativos, apelidos íntimos ou situações constrangedoras podem **causar vergonha e servir de motivo para *bullying*.**

ATENÇÃO AO USO COMERCIAL DA IMAGEM DA CRIANÇA

Quando a criança participa de forma habitual da produção de conteúdo com finalidade comercial, é preciso observar as regras do ECA Digital (Lei nº 15.211) e de sua regulamentação[1,2]. Em determinados casos, a autorização dos pais não é suficiente: é necessário também obter alvará judicial e cumprir outros requisitos de proteção[3].

[1] Lei nº 15.211 (ECA Digital) – 2025 – https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm
[2] Decreto nº 12.880 – 2026 – https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm
[3] Resolução CNJ nº 687 – 2026 – https://atos.cnj.jus.br/atos/detalhar/327

CONHEÇA O AMBIENTE DIGITAL DOS SEUS FILHOS

Nem todos os ambientes digitais são adequados para crianças ou oferecem recursos de proteção compatíveis com sua idade. Por isso, acompanhar o que fazem *online* e conversar sobre suas experiências ajuda a identificar situações de risco e oferecer orientação quando necessário.

CONHEÇA OS *SITES*, APLICATIVOS, JOGOS E PLATAFORMAS

- Converse com seus filhos sobre o que acessam, jogam e utilizam. **Procure saber com quem interagem e quais recursos usam,** incluindo *chatbots* e outras ferramentas de IA.
- **Confira as regras e os termos de uso,** especialmente as informações sobre privacidade, coleta de dados e formas de interação.
- **Explore junto com seus filhos.** Criar uma conta ou jogar com eles permite conhecer melhor os ambientes e identificar possíveis desafios.

INCENTIVE O USO DE SERVIÇOS ADEQUADOS À FAIXA ETÁRIA

Os serviços digitais podem ter classificação indicativa[4] e oferecer recursos de proteção específicos para crianças. Ao usar serviços inadequados à idade, elas podem ficar expostas a riscos e deixar de contar com algumas dessas proteções.

- **Confira a classificação indicativa e os recursos de proteção oferecidos** pelos serviços digitais que seus filhos usam.
- **Priorize serviços que usem mecanismos de verificação de idade robustos e que preservam a privacidade.**

[4] O ECA Digital (Lei nº 15.211/2025) estabelece que crianças têm direito de acesso a produtos, serviços e experiências digitais adequados à sua faixa etária. Com a regulamentação da lei, a classificação indicativa de jogos eletrônicos e aplicativos passou a considerar, além dos conteúdos, riscos relacionados às funcionalidades e à forma de interação, como comunicação entre usuários, compras, estímulo ao uso excessivo e práticas manipulativas.



ACONTECEU UM PROBLEMA?

SAIBA O QUE FAZER

- **Mantenha a calma,** converse com seu filho, procure entender o que aconteceu e ofereça apoio.
- **Guarde as evidências,** como mensagens, imagens, perfis, *links* e registros das conversas.
- **Bloqueie contas, perfis ou contatos** relacionados ao problema.
- **Proteja as contas e os dispositivos:** altere as senhas, ative a verificação em duas etapas e verifique se houve acesso indevido.
- **Procure ajuda** quando houver ameaças, chantagem, violência, exploração ou outras situações que coloquem a criança em risco.
- **Denuncie** o ocorrido pelos canais adequados e, se necessário, procure ajuda especializada.

ONDE DENUNCIAR

- **Na própria plataforma:** para conteúdos ou situações que violem as regras do serviço.
- **Disque 100:** para violações de direitos de crianças.
- **SaferNet:** para crimes e violações contra os direitos humanos na Internet, como imagens e vídeos de abuso e exploração sexual de crianças.
- **Delegacias especializadas ou Polícia Civil:** para crimes contra crianças.
- **ANPD** (Agência Nacional de Proteção de Dados): para descumprimentos do ECA Digital, como ausência ou deficiência de mecanismos de aferição de idade ou de controle parental.
- **Ouvidoria do MJSP** (Ministério da Justiça e Segurança Pública): para descumprimentos das normas de Classificação Indicativa.

EM SITUAÇÕES DE EMERGÊNCIA, PROCURE AS AUTORIDADES POLICIAIS

Agradecimentos

Agradecimentos

Ilustrações

– Hector Gomez

Projeto gráfico e editoração

– André Martins



Revisão e Contribuições

– Carolina Carvalho (NIC.br)
– Evelise Carvalho (CPN-PREV / UQAM)
– Evelyn Eisenstein (Clínica de Adolescentes, CEIIAS)
– George Valença (Grupo ASPAS / UFRPE)
– Ivelise Fortim
– Kelli Angelini Neves (NIC.br)
– Lucimara Desiderá (NIC.br)
– Luísa Adib Dino (NIC.br)
– Marcus Lahr (NIC.br)
– Mariana Venâncio (NIC.br)
– Michelle Wangham (RNP, Univali)
– Rodrigo Nejm (Instituto Alana)



LANÇAMENTO 3ª EDIÇÃO DOS GUIAS INTERNET SEGURA.

Agora com alertas sobre os riscos do uso da inteligência artificial.

INTERNET SEGURA BR

INTERNET SEGURA BR

internetsegura.br

Obrigada!

para materiais de conscientização: doc@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br