



INTERNET SEGURA

PARA SEUS FILHOS

Sua participação é muito importante!

3ª EDIÇÃO

cert.br nic.br cgi.br

INTERNET SEGURA

PARA SEUS FILHOS

Sua participação é muito importante!

Público-alvo:

Pais, mães, responsáveis e educadores

3ª Edição:

Outubro/2026

Produção:

Centro de Estudos, Resposta e
Tratamento de Incidentes de
Segurança no Brasil — CERT.br

Núcleo de Informação e
Coordenação do
Ponto BR — NIC.br

Comitê Gestor da
Internet no Brasil — CGI.br

Coordenação Geral:

Cristine Hoepers

Redação:

Miriam von Zuben

Ilustrações:

Hector Gomez

Banco de imagens:

Shutterstock

Projeto Gráfico e Editoração:

André Martins

Agradecemos a todos que contribuíram
para a construção deste guia. Em nosso
site, você encontra a lista de revisores
e colaboradores, além de informações
sobre impressão e licença de uso:

<https://internetsegura.br/criancas/sobre>

Esse guia está disponível em

<https://internetsegura.br/>

Caso queira receber uma cópia
impressa, tenha sugestões ou encontre
erros, envie *e-mail* para **doc@cert.br**.

Versões anteriores:

1ª Edição

Fevereiro/2017

2ª Edição

Outubro/2022



(CC BY-NC-ND 4.0)

ISBN digital 978-65-6165-055-7

ISBN físico 978-65-6165-051-9

AJUDE SEUS FILHOS A USAR A INTERNET COM SEGURANÇA

Assim como você orienta seus filhos sobre cuidados no dia a dia, também é importante acompanhá-los e ajudá-los no uso seguro e responsável da Internet.

A conscientização é uma das melhores formas de prevenção. Quanto mais as crianças conhecem os riscos *online* e aprendem sobre eles, mais preparadas ficam para reconhecê-los e lidar com diferentes situações.

Pensando nisso, criamos o **guia Internet Segura**, com dicas para que as crianças aprendam, de forma divertida, a se proteger enquanto aproveitam as oportunidades da Internet. Você pode acessá-lo em <https://internetsegura.br/>.

A proteção das crianças no ambiente digital é uma responsabilidade de toda a sociedade, e a família tem um papel importante nesse processo. Por isso, criamos também este guia complementar, com dicas para apoiar você na orientação dos seus filhos e ajudá-los a usar a Internet de forma mais segura e consciente.



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

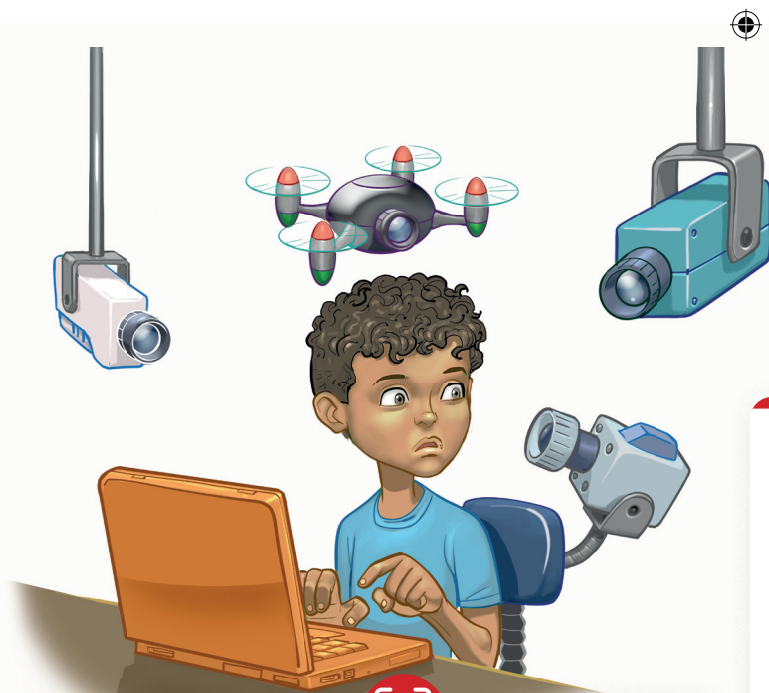
- ♦ Crianças podem ter contato com **conteúdos que divulgam marcas ou produtos**, como publicações de influenciadores ou criadores de conteúdo, **sem perceber que se trata de publicidade**.
- ♦ Dados de crianças podem ser coletados e usados por empresas para **direcionar publicidade personalizada, recomendar conteúdos ou produtos e influenciar seus hábitos de consumo e seu comportamento**.



GOLPES E RISCOS DE SEGURANÇA

- ♦ Crianças podem sofrer **tentativas de manipulação para obter informações pessoais, acessar contas ou explorar recursos financeiros da família**.
- ♦ Os **dispositivos** usados pela criança podem ser **invadidos ou infectados** por códigos maliciosos (*malware*), comprometendo dados e contas.
- ♦ **Nomes, fotos ou outras informações podem ser usados por terceiros** para criar perfis 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 **difficuldade 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.**

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 proteção³.

¹ Lei nº 15.211 (ECA Digital) – 2025 – https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/115211.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>

RESPEITE A PRIVACIDADE, A INDIVIDUALIDADE E A INTIMIDADE DOS SEUS FILHOS

As crianças têm sua imagem, privacidade e intimidade protegidas pelas leis brasileiras. Sempre que possível, devem participar das decisões sobre sua exposição *online* e sobre a exclusão do que já foi publicado.

- ▶ Evite publicar informações sobre a rotina das crianças, situações constrangedoras ou apelidos familiares.
- ▶ Restrinja o acesso às suas publicações e mantenha seu perfil e suas configurações de privacidade ajustados.
- ▶ Antes de publicar, pense: isso precisa ser compartilhado? Com quem? A criança está de acordo?
- ▶ Considere a opinião dos seus filhos antes de registrar ou publicar algo relacionado a eles. À medida que crescem, envolva-os cada vez mais nas decisões sobre sua exposição *online*.



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 indicativa⁴ 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.

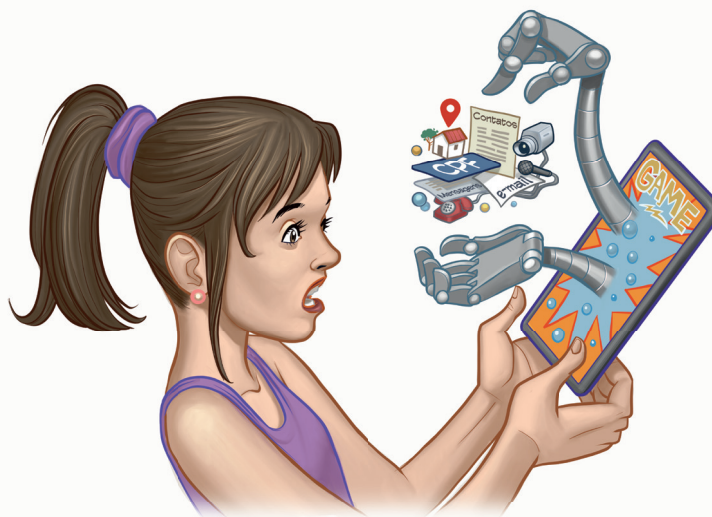
- ▶ **Confira a classificação indicativa e os recursos de proteção oferecidos** pelos serviços digitais que seus filhos usam.
- ▶ **Priorize serviços que usem mecanismos de verificação de idade robustos e que preservam a privacidade.**

⁴O 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.

CONHEÇA AS CONFIGURAÇÕES DE PRIVACIDADE E SEGURANÇA

As configurações de privacidade e segurança ajudam a definir quais informações podem ser compartilhadas, como são utilizadas e quem pode acessá-las.

- ▶ Explore junto com seus filhos essas configurações e ajuste-as conforme suas necessidades e preferências.
- ▶ Aproveite para conversar sobre os benefícios e riscos de cada escolha, buscando um equilíbrio entre exposição, privacidade e segurança.
- ▶ Verifique se os produtos e serviços oferecem orientações claras sobre essas configurações. Caso não ofereçam, procure alternativas ou canais para relatar o problema.



VERIFIQUE AS PERMISSÕES DE ACESSO

Alguns aplicativos e dispositivos conectados, como assistentes virtuais e brinquedos e relógios “inteligentes”, podem solicitar permissões para acessar recursos como localização, câmera e microfone, a fim de oferecer funcionalidades específicas. Esses acessos podem resultar na coleta de informações como imagens, voz, hábitos e rotina da criança.

- ▶ Verifique quais aplicativos e dispositivos possuem essas permissões e **mantenha apenas aquelas necessárias para seu funcionamento.**

ACOMPANHE O TEMPO DE USO DE TELAS E OS MOMENTOS DE ACESSO À INTERNET

O uso de telas faz parte do dia a dia de muitas crianças, em diferentes momentos e atividades.

- ▶ Acompanhe quanto tempo seus filhos passam diante das telas e quais atividades costumam realizar nesse período.
- ▶ Observe como a tecnologia é usada e se há recursos que estimulam o uso excessivo, como reprodução automática de vídeos e notificações frequentes⁵. Se identificar esses recursos, desative-os sempre que possível.
- ▶ Lembre-se: a qualidade das experiências digitais também importa.



ALGUNS SINAIS DE ALERTA

- ♦ Seu filho tem dificuldade de largar o celular quando você estabelece um limite?
- ♦ Quando o tempo de tela termina, ele fica irritado ou agressivo?
- ♦ Você só consegue acalmá-lo se deixar que ele use o celular?
- ♦ Ele só faz as refeições enquanto está usando telas?
- ♦ Ele deixa de brincar ou fazer outras atividades para continuar nas telas?
- ♦ O uso das telas tem prejudicado a convivência familiar, o sono ou os estudos?

Se a resposta for “sim” para uma ou mais dessas perguntas, pode ser o momento de rever a rotina de uso das telas.

⁵ O ECA Digital e sua regulamentação estabelecem medidas para coibir práticas manipulativas, enganosas ou coercitivas que explorem as vulnerabilidades de crianças ou interfiram em sua autonomia de decisão.

AJUDE SEUS FILHOS A SE PROTEGEREM

As crianças ainda estão em desenvolvimento e aprendendo a lidar com o ambiente digital, por isso o apoio dos pais é essencial para ajudá-las a usar a Internet com responsabilidade e segurança⁷.

ESTABELEÇA UMA ROTINA SAUDÁVEL

Uma rotina equilibrada ajuda as crianças a conciliar o uso das telas com outras atividades importantes para seu desenvolvimento.

- ▶ Procure conciliar o uso das telas com o sono, as refeições, os estudos, as brincadeiras, as atividades físicas e a convivência familiar.
- ▶ **Faça combinados com seus filhos sobre os horários de uso das telas** e os momentos em que elas não devem ser usadas, como durante as refeições ou à noite.
- ▶ **Revise esses combinados periodicamente**, conforme a criança cresce e amadurece.
- ▶ Evite usar o acesso às telas como recompensa ou punição.
- ▶ Os pais são a principal referência dos filhos. Por isso, **dê o exemplo, usando a tecnologia de forma equilibrada e priorizando os momentos de convivência em família.**



**CONSTRUAM JUNTOS
HÁBITOS DIGITAIS
MAIS SAUDÁVEIS**

⁷Esse apoio pode mudar ao longo do tempo, de acordo com a idade e o desenvolvimento da autonomia da criança.

ESTIMULE O DIÁLOGO

O diálogo com os filhos fortalece a confiança e facilita o apoio diante de diferentes situações *online*.

- ▶ **Converse com eles sobre os riscos e formas de agir.** Aproveite situações do cotidiano para abordar esses assuntos de forma natural.
- ▶ **Ouçá seus filhos, demonstre interesse pelo que fazem e leve suas experiências a sério.** Incentive-os a compartilhar dúvidas e situações que os deixem desconfortáveis.
- ▶ Se não souber algo, não tenha receio de admitir. Mostre que pode buscar respostas e ajudá-los. **Aproveite para aprender coisas novas com eles.**



PERGUNTAS PARA COMEÇAR A CONVERSA

- ▶ O que você mais gostou de fazer *online* esta semana?
- ▶ Como funciona esse jogo que você joga com seus amigos?
- ▶ Alguém já pediu segredo sobre uma conversa ou foto?
- ▶ Gostaria de conversar sobre alguma coisa da Internet?
- ▶ Se algo deixasse você desconfortável *online*, você me contaria?

OBSERVE O COMPORTAMENTO

Acompanhar o comportamento dos filhos pode ajudar a identificar mudanças que indiquem dificuldades ou situações de risco.

- ▶ Mantenha o computador da casa em um local que permita acompanhar, de forma natural, o uso que seus filhos fazem do ambiente digital.
- ▶ No caso de celulares e *tablets*, esse acompanhamento pode ser mais difícil. Ainda assim, **fique atento a mudanças de comportamento, como nervosismo** ao usar determinados aplicativos na sua presença, **irritação** quando não podem usar o aparelho, ou **dificuldade para falar sobre certas interações *online*.**



ENSINE SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

Ensinar as crianças a proteger suas informações pessoais ajuda a desenvolver hábitos mais seguros.

- ▶ Explique que **informações pessoais**, como endereço, escola e rotina, **devem ser protegidas e compartilhadas apenas quando necessário e em sites e aplicativos confiáveis**.
- ▶ Ensine-os a **pensar antes de publicar** e avaliar o que compartilham, com quem e quais podem ser as consequências.
- ▶ Oriente-os a **não inserir informações pessoais, fotos ou outros conteúdos privados em ferramentas de IA** sem entender como podem ser usados.
- ▶ Reforce a importância de **respeitar a privacidade e os dados de outras pessoas** e de pedir autorização antes de divulgar conteúdos que as envolvam.

REFORCE OS CUIDADOS AO INTERAGIR COM DESCONHECIDOS

Orientar seus filhos sobre como interagir com desconhecidos ajuda a protegê-los de situações potencialmente prejudiciais.

- ▶ **Configure as permissões de interação nos aplicativos e jogos.** Quando disponível, restrinja o contato com desconhecidos ou limite as possibilidades de interação.
- ▶ **Orientar seus filhos a ter cuidado ao interagir com pessoas que conhecem apenas no ambiente digital** e a nunca marcar encontros presenciais sem o conhecimento e a autorização de um responsável.



FIQUE ATENTO AOS SINAIS DE CYBERBULLYING

Vítimas de *cyberbullying* podem apresentar sinais como tristeza persistente, baixa autoestima, ansiedade, agressividade ou medo, além de queda no rendimento escolar e de evitar a escola.

- ▶ Caso perceba esses sinais, **converse com seus filhos e, se necessário, também com a escola.**
- ▶ Incentive-os a procurar você ou outro adulto de confiança sempre que sofrerem ou presenciarem situações de *cyberbullying*.

INCENTIVE O RESPEITO E A EMPATIA

- ▶ Converse sobre respeito, empatia e comportamento adequado nas interações pela Internet.
- ▶ Oriente-os a não criar nem compartilhar conteúdos que exponham ou humilhem crianças, professores e outras pessoas.
- ▶ Explique que **ofender ou prejudicar alguém pela Internet pode causar sofrimento e gerar consequências na escola e até mesmo na Justiça.**

CONVERSE SOBRE GOLPES

Reconhecer golpes pode ser difícil para crianças, principalmente quando os golpistas usam estratégias para chamar atenção, despertar curiosidade ou criar um senso de urgência.

- ▶ Oriente seus filhos a **desconfiar de promoções, sorteios e ofertas que pareçam boas demais** e a verificar as informações antes de acreditar.
- ▶ Explique que **não devem acessar links, instalar aplicativos fora das lojas oficiais** nem abrir arquivos enviados por desconhecidos.
- ▶ Oriente-os a **não realizar compras ou fornecer informações de pagamento sem sua autorização.**
- ▶ Incentive-os a procurar um adulto de confiança se receberem mensagens suspeitas, sofrerem pressão ou tiverem dúvidas.



USE MECANISMOS DE SUPERVISÃO PARENTAL

Os mecanismos de supervisão parental, ou **controle parental**, ajudam a criar um ambiente digital mais seguro e adequado às necessidades de cada criança.

- ▶ Explique aos seus filhos como esses mecanismos ajudam a protegê-los.
- ▶ Configure as funcionalidades de acordo com os combinados feitos em família.
- ▶ Revise periodicamente as configurações e ajuste o nível de supervisão conforme seus filhos crescem e amadurecem.
- ▶ Para evitar alterações indevidas, mantenha em sigilo as senhas de administração dos dispositivos e dos próprios mecanismos de supervisão.



SAIBA MAIS

Os mecanismos de supervisão parental ajudam a gerenciar o uso de dispositivos e acompanhar as atividades *online* das crianças.

Suas funcionalidades variam conforme o serviço e podem incluir restrições a conteúdos, aplicativos e *sites*; definição de horários e limites de uso; gerenciamento de configurações de privacidade, contatos e compras; e acompanhamento do tempo de uso.



**OS MECANISMOS DE SUPERVISÃO
COMPLEMENTAM, MAS NÃO SUBSTITUEM,
O DIÁLOGO, A ORIENTAÇÃO E O
ACOMPANHAMENTO DA FAMÍLIA.**

PROTEJA AS CONTAS

Contas próprias e protegidas ajudam a evitar acessos indevidos a informações e serviços.

- ▶ Ao criar uma conta para a criança, **use a opção de conta infantil ou de supervisão** oferecida pelo próprio serviço.
- ▶ Quando disponível, **vincule a conta da criança à conta de um familiar ou adulto responsável**. Isso facilita o gerenciamento das configurações de segurança e supervisão.
- ▶ Incentive seus filhos a criar senhas longas e difíceis de adivinhar e a **ativar a verificação em duas etapas**.
- ▶ Considere usar um gerenciador de senhas para facilitar os acessos.
- ▶ Ensine-os a não compartilhar senhas nem códigos de verificação.
- ▶ Oriente-os a sair das contas (encerrar a sessão) ao usar dispositivos de outras pessoas ou de uso compartilhado.



PROTEJA OS DISPOSITIVOS

Dispositivos seguros e atualizados ajudam a proteger os dados e as contas.

- ▶ Configure atualizações automáticas do sistema e dos aplicativos.
- ▶ Use mecanismos de segurança, como antivírus e *firewall* pessoal, para reduzir os riscos de infecção por *malware*.
- ▶ Habilite *backups* automáticos para facilitar a recuperação de fotos, vídeos e outros arquivos importantes.
- ▶ Ao repassar um dispositivo antigo aos seus filhos, **verifique se ele ainda recebe atualizações**, restaure as configurações de fábrica e apague os dados anteriores.
- ▶ Em dispositivos compartilhados, se possível, crie um perfil ou uma conta própria para a criança e use configurações de proteção adequadas.
- ▶ Vai emprestar seu celular para a criança? **Restrinja o acesso a um único aplicativo**. No Android, use “Fixação de tela”; no iOS, “Acesso Guiado”.

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.



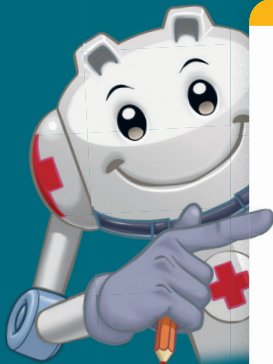
ONDE DENUNCIAR

- **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**

MANTENHA-SE INFORMADO



No Portal Internet Segura você encontra, além deste material, também o guia criado especialmente para seus filhos.



<https://internetsegura.br/>

Confira ainda a **Cartilha de Segurança para Internet**.



<https://cartilha.cert.br/>

