

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 08

Crianças e adolescentes na internet

Guia de proteção para pais e responsáveis



08

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Crianças e adolescentes na internet

Guia de proteção para pais e responsáveis

Como prevenir riscos, identificar situações de perigo e proteger crianças e adolescentes no ambiente digital.

Coleção Investigação e Proteção na Era Digital
Volume 08

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge

Material educativo de distribuição gratuita.

Coleção Investigação e Proteção na Era Digital, volume 08.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Crianças e adolescentes na internet : guia de proteção para pais e responsáveis [recurso eletrônico] / Higor Vinicius Nogueira Jorge. -- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (51 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 8)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências, apêndices e resumo para compartilhar.

Publicação de distribuição gratuita.

1. Crianças e adolescentes. 2. Segurança na internet. 3. Educação digital. 4. Proteção integral. 5. Mediação parental. 6. Cyberbullying. 7. Violência digital. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 A infância e a adolescência conectadas.....	7
2 Os principais riscos na internet.....	9
3 Pessoas podem apresentar identidades falsas.....	11
4 Jogos e ambientes de interação.....	13
5 Redes sociais e privacidade.....	15
6 Cyberbullying e violência entre colegas.....	17
7 Sextorsão e chantagem com imagens íntimas.....	19
8 Inteligência artificial e manipulação digital.....	21
9 Controle parental e configurações de segurança.....	23
10 Como conversar sobre segurança digital.....	25
11 Sinais de que algo pode estar errado.....	27
12 O que fazer diante de violência digital.....	29
13 A escola como parceira da proteção.....	31
14 Construindo um acordo familiar.....	33
Considerações finais.....	35
Apêndice A. Acordo familiar de segurança digital.....	36
Apêndice B. Recomendações por faixa etária.....	37
Apêndice C. Dez perguntas para conversar com os filhos.....	38
Apêndice D. Sinais de atenção e caminhos de apoio.....	39
Apêndice E. Roteiro de acolhimento e encaminhamento.....	40
Apêndice F. Página para pais e educadores.....	41
Apêndice G. Resumo para compartilhar.....	42
Referências.....	45
Minicurriculo do autor.....	48
Para aprofundar o estudo.....	50
A coleção.....	51

Apresentação

A internet participa da infância e da adolescência por meio da escola, das amizades, dos jogos e das descobertas. A proteção precisa acompanhar essas experiências, oferecendo orientação e condições para que uma criança ou um adolescente possa pedir ajuda quando algo o incomodar.

Muitas famílias conhecem os nomes dos aplicativos, mas não sabem com quem os filhos conversam ou como funcionam os espaços que frequentam. Aproximar-se desse cotidiano permite explicar riscos concretos, ajustar configurações e combinar decisões. O diálogo fica mais produtivo quando o adulto demonstra interesse e escuta antes de julgar.

Esta cartilha apresenta caminhos para prevenir a exposição indevida, reconhecer abordagens prejudiciais e responder à violência. Uma alteração de comportamento merece atenção, mas não comprova, sozinha, a ocorrência de crime. O acolhimento deve preservar a dignidade e evitar perguntas repetidas, exposição pública ou iniciativas particulares de investigação.

No meu livro *Investigação criminal tecnológica*, examino a importância de interpretar informações em seu contexto. Esse cuidado também orienta as famílias: a aparência de um perfil não confirma uma identidade, e uma suspeita exige providências de proteção sem conclusões precipitadas (Jorge, 2027).

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

O guia se destina a pais, mães, responsáveis, educadores e profissionais que acompanham crianças e adolescentes. Pode ser utilizado em reuniões escolares, palestras e atividades de prevenção. A linguagem dispensa conhecimentos de informática ou de Direito.

A leitura ajuda a compreender riscos, estabelecer acompanhamento adequado ao desenvolvimento e organizar a resposta a uma possível violência. As orientações consideram o melhor interesse, a proteção integral, a privacidade e a autonomia progressiva. Famílias, escolas, empresas e poder público têm responsabilidades nesse cuidado.

Como utilizar a cartilha

Os capítulos iniciais explicam os ambientes e as situações de risco. Os capítulos 9, 10 e 14 apoiam a organização da rotina familiar. Diante de violência ou ameaça, procure o capítulo 12 e o Apêndice E. Se houver perigo imediato, priorize a segurança e a ajuda emergencial.

Ao final, há acordo familiar, recomendações por faixa etária, perguntas para conversar, sinais de atenção, roteiro de acolhimento e página para pais e educadores. O Apêndice G reúne um resumo de duas páginas para compartilhar.

Não registre senhas, imagens íntimas ou detalhes desnecessários da violência nos instrumentos. Eles servem para combinar cuidados e organizar providências, preservando a intimidade de quem precisa de proteção.

CAPÍTULO 1

A infância e a adolescência conectadas

1.1 Participação com orientação

Uma criança pode utilizar a internet para aprender uma música, conversar com familiares ou participar de uma atividade escolar. Um adolescente pode produzir conteúdo, encontrar colegas com interesses semelhantes e exercer sua criatividade. Essas experiências fazem parte de sua vida e precisam ser compreendidas pelo adulto responsável.

A avaliação do uso considera o conteúdo, os contatos, o contexto e os efeitos sobre a rotina. Duas atividades com a mesma duração podem ter características muito diferentes. Importa observar se há acompanhamento, se o ambiente é adequado e se continuam preservados o sono, a convivência, o estudo e as atividades fora das telas.

O adulto pode começar pedindo que o filho apresente um jogo ou explique uma comunidade de que participa. Demonstrar interesse abre espaço para conversar sobre dúvidas reais. A pergunta sobre o que ele gosta costuma produzir uma conversa mais esclarecedora do que uma fiscalização iniciada com acusações.

Exemplo hipotético. Uma adolescente utiliza um grupo para estudar e também recebe mensagens incômodas de um integrante. Proibir toda comunicação escolar pode afastá-la dos colegas sem resolver a abordagem. Ouvir, identificar o problema e ajustar o contato permite uma proteção mais precisa.

O acesso à tecnologia deve ser acompanhado de educação, condições de segurança e respeito às necessidades de desenvolvimento de cada pessoa (Secom, 2025).

1.2 Direitos e responsabilidades continuam na internet

Crianças e adolescentes têm direito à dignidade, ao respeito, à imagem e à proteção contra violência. Esses direitos permanecem quando estudam, jogam ou conversam pela internet. A Constituição e o Estatuto da Criança e do

Adolescente, o ECA, orientam uma proteção prioritária e compartilhada (Brasil, 1988, art. 227; 1990, arts. 4º, 5º e 17).

O Estatuto Digital da Criança e do Adolescente, conhecido como ECA Digital, estabelece deveres para produtos e serviços destinados a esse público ou de acesso provável por ele. A legislação exige prevenção de riscos, privacidade mais protetiva por padrão e recursos de supervisão parental, observadas a idade e a autonomia progressiva (Brasil, 2025b; 2026).

Para a família, isso significa procurar configurações adequadas e cobrar canais de proteção compreensíveis. Para as plataformas, significa desenvolver medidas de segurança e cumprir seus próprios deveres. O cuidado familiar não elimina a responsabilidade das empresas ou do poder público.

O acompanhamento precisa ser explicado e revisto conforme o desenvolvimento. Uma criança pequena exige presença próxima; um adolescente precisa participar das decisões e aprender a avaliar consequências. A autonomia se constrói com orientação e oportunidades de demonstrar responsabilidade.

Quando surgir uma situação de violência, a prioridade é proteger. Uma regra familiar descumprida não justifica humilhação nem retira o direito de receber ajuda.

CAPÍTULO 2

Os principais riscos na internet

2.1 Entender a situação antes de escolher o cuidado

Os riscos podem chegar pelo conteúdo apresentado, pelas pessoas com quem se interage e pelas escolhas feitas durante o uso. Uma recomendação automática pode exibir material inadequado. Um contato pode pressionar por uma fotografia. Uma oferta de vantagem pode solicitar dinheiro ou dados da família.

Também há riscos relacionados à exposição e ao consumo. Publicações podem revelar escola e rotina; compras em jogos podem ultrapassar o combinado; anúncios podem misturar entretenimento e publicidade. Cada situação pede uma orientação específica, além do simples controle do tempo de uso.

Exemplo hipotético. Um vídeo adequado termina e a reprodução automática apresenta outro, com violência. A resposta pode envolver interromper a exibição, conversar sobre o que foi visto e revisar o serviço. Não se deve presumir que a criança procurou aquele conteúdo nem exigir que o reproduza para explicar o ocorrido.

Observe como o aplicativo recomenda materiais, permite contatos, solicita permissões e oferece compras. A classificação indicativa ajuda a escolher, mas não descreve todas as interações possíveis. Um jogo adequado quanto ao conteúdo pode ter conversas abertas e transações que exigem configuração adicional.

Converse sobre o que fazer quando aparecer algo perturbador. Ensine a fechar o conteúdo e procurar ajuda, sem precisar investigar, compartilhar ou continuar assistindo para ter certeza do que é (Secom, 2025).

2.2 Atenção sem conclusões precipitadas

Encontrar um risco não significa que uma violência já aconteceu. Receber uma mensagem desconhecida, por exemplo, exige avaliar o contexto e configurar a proteção. Uma ameaça concreta ou uma exigência de imagem íntima demanda resposta imediata, mesmo que o remetente não esteja identificado.

A família deve distinguir o relato da criança, o material que está disponível e as interpretações feitas pelos adultos. Dizer que alguém pediu uma fotografia é diferente de concluir quem controla o perfil ou o que pretendia fazer. Essa distinção melhora a comunicação com os serviços de atendimento.

Não é necessário descobrir o nome verdadeiro de um suspeito para buscar proteção. Evite criar conta falsa, abordar o contato ou manter a criança na conversa com a finalidade de obter mais informações. Essas iniciativas podem ampliar a exposição e interferir no atendimento adequado.

Também não se deve tratar toda discordância entre colegas como crime. A análise considera o comportamento, a gravidade e as circunstâncias. Ao mesmo tempo, uma agressão isolada pode exigir intervenção, ainda que não tenha a repetição associada ao bullying.

O melhor interesse da criança orienta a decisão: interromper o risco, ouvir o necessário e procurar a rede competente. A investigação de possíveis crimes deve seguir os procedimentos próprios, com respeito aos direitos de todos os envolvidos (Brasil, 1990; 2017; Jorge, 2027).

CAPÍTULO 3

Pessoas podem apresentar identidades falsas

3.1 A aparência do perfil não confirma a pessoa

Nome, idade, fotografia e voz podem ser inventados ou manipulados. Uma conta também pode ter sido tomada de outra pessoa. Estar no mesmo jogo ou conhecer assuntos de interesse do grupo não comprova que o interlocutor é quem afirma ser.

Explique esse cuidado sem ensinar que toda pessoa desconhecida é perigosa. O objetivo é reconhecer limites para a interação: não enviar informações íntimas, não aceitar pressão e não combinar encontro sem conhecimento e acompanhamento responsáveis. Os mesmos limites são importantes quando o contato parece conhecido.

Uma aproximação prejudicial pode apresentar pedidos de segredo, presentes condicionados a favores, insistência em conversar a sós ou tentativa de afastar a criança de quem a protege. Nenhum sinal isolado identifica um agressor, mas esses pedidos justificam interromper a situação e buscar ajuda.

Exemplo hipotético. Um perfil diz ter a mesma idade, conversa sobre um jogo e pede que o contato continue em outro aplicativo sem que os pais saibam. O responsável pode acolher o relato, orientar a interrupção e utilizar os canais de denúncia. Não precisa provar a idade do remetente antes de proteger o filho.

A verificação não deve exigir novos vídeos, fotografias ou mensagens da criança. Uma chamada de vídeo também pode ser manipulada e não substitui a avaliação do contexto (Secom, 2025; CERT.br, 2026).

3.2 Ensine limites que possam ser lembrados

Converse sobre o direito de recusar uma solicitação e interromper uma conversa. Ninguém pode exigir imagem íntima, dinheiro, encontro ou segredo

sobre algo que cause medo. Afeto, amizade, presentes e participação em um grupo não criam obrigação de atender a esses pedidos.

O aliciamento é uma aproximação voltada a facilitar abuso ou exploração. Pode ocorrer gradualmente e também envolver pessoas conhecidas. Por isso, o cuidado precisa considerar o comportamento, sem se limitar à ideia de um desconhecido com aparência suspeita (Secom, 2025).

A criança deve saber quem pode procurar se não conseguir falar com os pais. Escolha outros adultos confiáveis e acessíveis. Se a pessoa envolvida na violência estiver na própria família, a ajuda precisa vir de alguém e de serviços capazes de protegê-la, sem expô-la ao possível agressor.

Uma conversa possível. Explique que ela pode contar algo mesmo depois de ter respondido, aceitado presente ou descumprido um combinado. A prioridade será ajudá-la. Evite prometer que guardará segredo absoluto, pois pode ser necessário acionar profissionais de proteção.

Quando houver revelação, ouça sem exigir detalhes repetidos e não organize confronto. A família oferece segurança e encaminha; a escuta especializada e a produção de prova têm finalidades e procedimentos próprios (Brasil, 1990, arts. 17 e 18; 2017).

CAPÍTULO 4

Jogos e ambientes de interação

4.1 Conheça as funções que acompanham o jogo

Um jogo pode permitir mensagens privadas, voz, transmissão ao vivo e participação em grupos. Essas funções têm riscos diferentes dos desafios e imagens da partida. Antes de autorizar o uso, confira a classificação, as regras do serviço e quem poderá conversar com a criança.

Sempre que possível, experimente o ambiente junto com ela. Pergunte como adiciona colegas, recebe convites e pede ajuda. Configure interações de forma restrita e reveja periodicamente os contatos. A aprovação de uma amizade virtual não precisa ser permanente nem abranger todos os meios de comunicação.

Exemplo hipotético. Uma criança conhece um jogador que oferece um item raro e solicita um código de acesso. O presente pode ser uma tentativa de tomar a conta. Oriente a não entregar o código, interrompa a interação e procure a recuperação oficial se o acesso já tiver sido afetado.

Explique que senhas e códigos não devem ser enviados a jogadores ou supostos moderadores. Proteja a conta com os recursos oficiais e prepare a recuperação antes de precisar dela. Não instale modificações ou programas indicados por contatos para conseguir vantagens.

O ECA Digital prevê salvaguardas para jogos com comunicação entre usuários e atuação dos responsáveis sobre esses recursos. Procure as configurações disponíveis e não aceite uma conta com idade falsa para contornar a proteção (Brasil, 2025b, art. 21; CERT.br, 2022).

4.2 Combine gastos e formas de encerrar a atividade

Compras podem aparecer como itens, moedas virtuais ou ofertas por tempo limitado. A criança nem sempre percebe com clareza o valor em dinheiro ou a repetição das cobranças. Exija autorização para transações, revise os meios de pagamento e não deixe compras liberadas por conveniência.

O ECA Digital veda caixas de recompensa pagas e aleatórias, conhecidas como loot boxes, em jogos dirigidos a crianças e adolescentes ou de acesso provável por eles, nos termos da classificação indicativa. Essa regra não transforma toda compra de item virtual em caixa de recompensa, mas exige atenção às funcionalidades oferecidas (Brasil, 2025b, art. 20).

Converse também sobre a pressão de continuar conectado. Um grupo pode exigir presença diária ou ameaçar excluir quem não participa. Combine pausas e um modo de terminar a partida que respeite o descanso e os compromissos familiares. A organização deve considerar a atividade e o desenvolvimento, sem reduzir todo problema a um cronômetro.

Exemplo hipotético. Um adolescente quer pagar para não perder sua posição no grupo. Ouça o motivo, confira a cobrança e retome o combinado financeiro. Vergonha ou ameaça de exclusão são razões para avaliar a convivência naquele espaço.

Se aparecerem ofertas de apostas, dinheiro fácil ou tarefas perigosas, interrompa a participação e procure orientação. Não envie valor para testar a promessa nem mantenha o contato para descobrir quem está por trás dela (Secom, 2025).

CAPÍTULO 5

Redes sociais e privacidade

5.1 A exposição também depende dos adultos

Uma fotografia pode revelar uniforme, endereço, localização ou informações que aparecem ao fundo. O conjunto das publicações permite conhecer hábitos da família, mesmo quando cada postagem parece pouco relevante. Antes de publicar, avalie o conteúdo, o público e a necessidade da exposição.

Crianças e adolescentes têm direito à preservação da imagem, da identidade e de seus espaços pessoais. A responsabilidade dos adultos deve considerar esses direitos, inclusive quando a publicação parece uma homenagem ou um registro familiar. Ouça a opinião dos filhos de forma adequada à idade e respeite o desconforto manifestado (Brasil, 1990, art. 17).

Exemplo hipotético. Um responsável quer divulgar um boletim para comemorar uma conquista. O documento mostra nome completo, escola e outros dados. É possível celebrar sem publicar a identificação detalhada, preservando também aquilo que o filho prefere manter reservado.

Não publique imagens de banho, intimidade, sofrimento, atendimento de saúde ou situações que possam constranger. Pedir autorização não resolve toda exposição inadequada: o adulto continua responsável por avaliar a proteção de quem está em desenvolvimento.

Perfis restritos reduzem a circulação inicial, mas não impedem cópias. Revise o público, a localização e as publicações antigas. O cuidado com o que os adultos compartilham deve acompanhar as orientações dadas às crianças (CERT.br, 2023).

5.2 Proteja as contas sem falsear a idade

Confira as condições de uso e a classificação do serviço antes de criar uma conta. Não informe idade falsa para liberar um recurso. A existência de colegas naquele ambiente não demonstra que ele seja adequado nem elimina os deveres de proteção.

Nas redes sociais, o ECA Digital determina a vinculação de usuários ou contas de crianças e adolescentes de até 16 anos à conta de um responsável legal. Essa exigência não funciona como autorização geral para acessar qualquer serviço antes dessa idade. As demais restrições e salvaguardas continuam aplicáveis (Brasil, 2025b, art. 24).

Explique por que informações como escola, localização e documentos precisam de cuidado. A proteção de dados de crianças e adolescentes deve atender ao seu melhor interesse. Uma autorização de cadastro não deve ser tratada como permissão irrestrita para coletar, divulgar ou explorar informações (Brasil, 2018, art. 14).

Na prática. Revise com o filho quem pode ver o perfil, enviar mensagens, marcar publicações e utilizar a localização. Examine também aplicativos conectados e formas de recuperação. Use senhas diferentes e a verificação adicional oferecida pelo serviço.

Se alguém copiar o perfil ou utilizar a conta indevidamente, proteja os acessos, denuncie na plataforma e avise contatos por outro meio. Não procure invadir a conta falsa ou confrontar seu responsável (CERT.br, 2022; 2023).

CAPÍTULO 6

Cyberbullying e violência entre colegas

6.1 A agressão pode continuar fora da escola

Cyberbullying é a intimidação sistemática praticada por meios digitais. A repetição e a intenção de intimidar, humilhar ou discriminar ajudam a compreender esse comportamento. Ele pode envolver mensagens, perfis falsos, publicações e grupos que mantêm a agressão em circulação (Brasil, 2024).

Uma publicação pode alcançar muitas pessoas e continuar disponível depois do horário escolar. Isso dificulta encontrar um espaço de descanso. A alegação de que era apenas brincadeira não encerra a avaliação do dano nem dispensa a intervenção de adultos responsáveis.

Exemplo hipotético. Um grupo passa a publicar montagens para ridicularizar uma estudante e incentiva novas mensagens sobre ela. O responsável pode ouvir o relato, reunir as informações já disponíveis e procurar a escola, solicitando providências de proteção e acompanhamento. Não deve responder com exposição dos envolvidos em grupos de pais.

Uma agressão isolada também pode ser grave e exigir ajuda. Não espere que se repita para interromper uma ameaça ou proteger quem está sofrendo. O enquadramento jurídico deve ser avaliado pelos profissionais competentes, conforme os fatos e as regras aplicáveis.

Pergunte à criança como a situação está afetando sua rotina e de quem ela gostaria de receber apoio. A proteção precisa alcançar a convivência e o bem-estar, além da retirada de uma publicação (Unicef, [2026?]).

6.2 Quem presencia pode ajudar sem ampliar a exposição

Quem recebe uma publicação ofensiva pode deixar de compartilhar, procurar um adulto e apoiar a pessoa atingida. Não é necessário comentar para defender a vítima se isso aumentar a circulação do ataque. Um contato privado e respeitoso pode ser mais útil do que uma discussão pública.

A família deve guardar registros disponíveis que não envolvam conteúdo sexual de crianças e adolescentes, preservar o contexto e utilizar a denúncia da plataforma. Se houver esse tipo de conteúdo sexual, não copie nem redistribua; procure imediatamente orientação das autoridades para a preservação adequada.

Peça à escola um canal reservado e um responsável pelo acompanhamento. Relate o que foi observado, identifique necessidades de segurança e combine uma data de retorno. Medidas preventivas não devem depender de a família descobrir sozinha a autoria de cada mensagem.

Quando o próprio filho participa da agressão, interrompa a conduta e explique o dano. Preserve sua dignidade, acompanhe a mudança de comportamento e coopere com as providências adequadas. Responsabilização educativa não se confunde com humilhação, ameaça ou exposição pública de uma criança.

A mediação não deve impor contato ou reconciliação à pessoa que sofreu violência. Casos graves, ameaças e outras violações exigem encaminhamento à rede de proteção e às autoridades competentes. A escola deve articular prevenção, acolhimento e acompanhamento, sem substituir a investigação criminal (Brasil, 2017; 2024; Unicef, [2026?]).

CAPÍTULO 7

Sextorsão e chantagem com imagens íntimas

7.1 A ameaça não cria obrigação de obedecer

Sextorsão é a ameaça de divulgar conteúdo íntimo para exigir dinheiro, novas imagens, atos ou outras vantagens. O agressor pode utilizar material real, uma montagem ou apenas afirmar que possui uma imagem. A incerteza pode ser explorada para provocar medo e impedir que a vítima procure ajuda (SaferNet Brasil, [2026?]).

Uma criança ou um adolescente pode temer a reação da família mais do que a própria ameaça. Por isso, diga antecipadamente que haverá apoio mesmo se alguma regra tiver sido descumprida. A violência é responsabilidade de quem ameaça, explora ou divulga, e a vítima conserva seu direito à proteção.

Exemplo hipotético. Um adolescente recebe uma montagem com seu rosto e uma cobrança para impedir a publicação. O responsável deve acolhê-lo, orientar a interrupção dos envios e procurar ajuda competente. Pagar ou enviar outra imagem não oferece garantia de que a ameaça terminará.

Não exija que ele prove a chantagem repetindo uma conversa ou mostrando o material a várias pessoas. Procure saber o necessário para a segurança imediata: se há ameaça atual, possibilidade de encontro ou alguém em condição de alcançá-lo presencialmente.

Preserve informações já disponíveis sobre perfis, endereços e horários, sem reproduzir conteúdo sexual. A comunicação às autoridades e o atendimento de proteção devem acontecer sem investigação particular (Brasil, 1990; 2017).

7.2 Acolha e interrompa novas exigências

Afaste a criança ou o adolescente da pressão para responder. Oriente a não pagar, não enviar mais conteúdo e não aceitar encontro. Não faça ameaças ao interlocutor nem anuncie uma tentativa particular de identificá-lo. Utilize os canais adequados de proteção e denúncia.

Se houver risco imediato à integridade, procure ajuda emergencial. Quando o perigo envolver crime em andamento ou ameaça concreta à segurança, acione a Polícia Militar pelo 190. O registro da ocorrência e os demais encaminhamentos devem observar a situação e os serviços disponíveis.

A família não precisa baixar uma imagem para comunicar a violência. Identificadores do perfil, endereço da publicação, data, horário e descrição objetiva do que já foi percebido ajudam a indicar onde buscar as informações. Não reabra o conteúdo sexual para completar um registro e não o envie em grupos, e-mails ou formulários comuns.

Se o material já estiver no aparelho, evite manuseios, novas cópias e alterações precipitadas. Procure orientação imediata da autoridade competente sobre a preservação e a apresentação adequada. Solicitar ajuda não exige criar um arquivo de investigação doméstica.

Utilize a denúncia da plataforma para pedir as providências cabíveis, sem adiar a comunicação às autoridades. O cuidado continua depois da primeira medida, com acompanhamento emocional e atenção à rotina, sem responsabilizar a vítima pelo que aconteceu (Brasil, 1990; 2017; MDHC, 2026).

CAPÍTULO 8

Inteligência artificial e manipulação digital

8.1 Uma montagem também pode causar violência

Ferramentas de inteligência artificial podem produzir textos, imitar vozes e alterar imagens ou vídeos. Um conteúdo pode parecer registrar algo que nunca aconteceu. Para quem sofre uma montagem íntima, porém, a humilhação, a ameaça e a circulação do material são problemas que exigem proteção.

Não atribua à criança a responsabilidade de demonstrar que a imagem é falsa. A análise técnica e a investigação pertencem aos profissionais competentes. A família pode acolher, indicar onde a publicação foi encontrada e procurar os canais de proteção sem ampliar sua circulação.

O ECA contempla a simulação da participação de criança ou adolescente em conteúdo de violência sexual por recursos tecnológicos, inclusive inteligência artificial, e considera formas de representação geradas ou manipuladas digitalmente. A análise jurídica depende do conteúdo e das circunstâncias; não se confunde toda edição de fotografia com essa hipótese (Brasil, 1990, arts. 241-C e 241-E).

Exemplo hipotético. Colegas divulgam uma montagem sexual com o rosto de uma adolescente e dizem que não há problema porque a imagem é artificial. O responsável deve procurar proteção e encaminhamento, sem encaminhar o arquivo a outros pais para discutir sua autenticidade.

Não envie conteúdo íntimo a sites ou ferramentas de IA para verificar se é verdadeiro. Isso pode criar novas cópias e expor dados. Preserve apenas as informações disponíveis de forma juridicamente adequada, com orientação da autoridade competente (CERT.br, 2026).

8.2 Converse sobre limites ao utilizar uma IA

Uma ferramenta que conversa de forma convincente pode oferecer respostas incorretas, inventar referências ou sugerir ações inadequadas. Explique que ela

não conhece toda a situação do usuário e que sua linguagem acolhedora não substitui pessoas e serviços responsáveis pelo cuidado.

Evite inserir documentos, senhas, informações de saúde e detalhes íntimos da família em serviços sem necessidade e sem compreender o tratamento dos dados. Também não utilize uma ferramenta para expor relatos identificáveis de violência ou pedir que interprete imagens sexuais de crianças e adolescentes.

Quando o uso for adequado à idade e às condições do serviço, acompanhe as primeiras experiências. Mostre como conferir uma informação e como recusar solicitações desnecessárias. Se uma resposta causar medo ou sugerir algo perigoso, interrompa a interação e procure ajuda humana confiável.

Exemplo hipotético. Um adolescente recebe de um assistente uma orientação para resolver um conflito com um colega. Antes de agir, pode conversar com um adulto e avaliar consequências. A resposta organizada da ferramenta não comprova que aquela solução seja segura ou apropriada.

O cuidado deve alcançar também serviços que utilizam IA sem se apresentarem como chat, como recomendações de conteúdo e filtros de imagem. Revise configurações e ensine a reconhecer o que o sistema está sugerindo ou pedindo, sem exigir conhecimentos técnicos especializados (CERT.br, 2026; Secom, 2025).

CAPÍTULO 9

Controle parental e configurações de segurança

9.1 Configure com uma finalidade compreensível

Controle parental é o conjunto de recursos que ajuda a acompanhar e limitar o uso de serviços digitais. Pode restringir compras, contatos, conteúdos e horários, conforme a ferramenta. Sua configuração deve ter finalidade de proteção e ser adequada à idade, ao desenvolvimento e às necessidades da criança ou do adolescente.

Comece pela conta do sistema do aparelho e pelos serviços mais utilizados. Confira se a idade foi informada corretamente, quais responsáveis estão vinculados e como funciona a recuperação. Proteja o acesso administrativo para impedir alterações indevidas, sem deixar a família dependente de uma única pessoa ou aparelho.

Depois, examine as opções de privacidade e contato. Restrinja mensagens de pessoas não autorizadas, localização e compras. Reveja recomendações, reprodução automática e notificações quando essas funções dificultarem pausas ou apresentarem conteúdo inadequado.

O ECA Digital prevê ferramentas acessíveis, informações compreensíveis e aviso sobre os controles aplicados. O uso desses recursos deve considerar o melhor interesse e o desenvolvimento progressivo das capacidades. A transparência ajuda a criança a compreender os cuidados, em vez de descobrir um acompanhamento que nunca lhe foi explicado (Brasil, 2025b, arts. 17 a 19).

Na prática. Escolha uma configuração, explique o efeito e confira seu funcionamento com material adequado. Não use conteúdo violento ou sexual para testar filtros. Procure a ajuda oficial se o resultado não corresponder ao esperado.

9.2 Revise a proteção sem transformar tudo em vigilância

Uma ferramenta não garante que todos os conteúdos e contatos serão identificados. A comunicação pode ocorrer em outro aparelho ou ambiente, e um filtro pode falhar. Por isso, o acompanhamento precisa combinar configurações, presença e oportunidades de conversar.

Estabeleça o que será acompanhado e por quê. Um limite de compra pode ser explicado de forma simples. O acesso a conversas e informações pessoais exige avaliar a necessidade concreta de proteção, a idade e a intensidade da medida. A privacidade também é um direito de quem está em desenvolvimento (Brasil, 1990, art. 17; 2025b).

Não utilize programas clandestinos, não exponha conversas para constranger e não compartilhe dados de localização com pessoas sem necessidade. Quando uma situação exigir proteção mais intensa, procure orientação da rede competente e reveja a medida depois de enfrentar o risco.

Exemplo hipotético. Uma família combina limites de compras e mensagens para uma criança. Com o crescimento, pode ampliar escolhas e revisar contatos autorizados, mantendo a possibilidade de pedir ajuda. O acompanhamento deve considerar o que ela já compreende e as dificuldades que ainda apresenta.

Inclua a segurança das contas dos adultos na revisão. Se a conta do responsável for comprometida, as configurações vinculadas também podem ser afetadas. Atualize aparelhos, utilize senhas diferentes e prepare meios de recuperação seguros (CERT.br, 2022; Secom, 2025).

CAPÍTULO 10

Como conversar sobre segurança digital

10.1 Faça da conversa parte da rotina

É mais fácil falar sobre um problema quando a família já conversa sobre o cotidiano digital. Pergunte quais atividades são interessantes, o que incomoda e como os colegas lidam com situações difíceis. Escute a resposta sem converter toda informação em motivo de proibição.

Use exemplos compatíveis com a idade. Para uma criança, explique que ninguém pode exigir segredo sobre algo que a assuste. Com adolescentes, converse também sobre pressão do grupo, intimidade, consentimento e consequências de compartilhar material de outra pessoa. A orientação precisa incluir respeito a quem está do outro lado da tela.

Uma conversa possível. Pergunte o que o filho faria se alguém pedisse um código ou ameaçasse divulgar uma fotografia. Ouça sua ideia e ajude a encontrar uma alternativa segura. Não é necessário apresentar imagens perturbadoras para tornar a conversa séria.

Evite começar com ameaças de retirada definitiva do aparelho. Se pedir ajuda parecer trazer apenas punição, a criança pode esconder um problema. Regras e consequências educativas podem ser discutidas depois de assegurar proteção e compreender o ocorrido.

Os adultos também devem observar o próprio comportamento. Publicar imagens sem ouvir os filhos ou utilizar o telefone durante toda conversa enfraquece o combinado. Uma rotina coerente oferece referências que a criança consegue compreender e praticar (Secom, 2025).

10.2 Adapte a explicação e respeite o modo de comunicar

Idade, linguagem, deficiência e experiências anteriores influenciam como cada pessoa compreende uma orientação. Use frases claras, recursos de acessibilidade e exemplos concretos. Não presuma que a dificuldade de explicar algo significa ausência de problema ou falta de credibilidade.

Uma criança pode contar parte do ocorrido, mudar de assunto ou precisar de tempo. Ofereça presença e evite preencher as lacunas com perguntas que sugere respostas. Em situação de possível violência, procure profissionais preparados para o atendimento e para a comunicação adequada às suas necessidades (Brasil, 2017, arts. 5º e 7º).

Exemplo hipotético. Uma criança que utiliza recursos visuais de comunicação demonstra desconforto com determinado contato. O responsável pode acolher a manifestação e buscar apoio qualificado, sem interpretar um gesto isolado como confirmação de crime ou treinar uma narrativa para apresentar às autoridades.

Ao receber uma revelação, agradeça por ter contado e explique que buscará ajuda para protegê-la. Não prometa resultado, segredo absoluto ou punição imediata de alguém. Informe, de modo compreensível, quem precisará ser procurado e por qual motivo.

O objetivo da conversa familiar é oferecer segurança e identificar a necessidade de proteção. Ela não substitui escuta especializada ou depoimento especial. Evite gravar uma entrevista doméstica, pedir repetição para familiares ou exigir uma demonstração do que aconteceu (Brasil, 2017).

CAPÍTULO 11

Sinais de que algo pode estar errado

11.1 Observe mudanças sem produzir um diagnóstico

Medo de receber mensagens, afastamento de colegas, dificuldade de dormir ou resistência em frequentar a escola podem merecer atenção. Essas mudanças têm diversas causas e não comprovam, isoladamente, violência digital, uso problemático de tecnologia ou ocorrência de crime.

Observe o contexto, a duração e os efeitos sobre a vida cotidiana. Uma situação pontual pode ser resolvida com diálogo; um sofrimento persistente pode exigir avaliação de saúde e apoio escolar. A família não precisa escolher sozinha uma explicação definitiva para procurar ajuda.

Exemplo hipotético. Um adolescente deixa de participar de um grupo e fica irritado ao receber notificações. Pode haver um conflito, uma cobrança excessiva, violência ou outra dificuldade. Em vez de afirmar que sabe o que ocorreu, o responsável pode perguntar como ele está e se alguém o está pressionando.

Leve o relato a sério, sem exigir que a criança apresente provas para merecer cuidado. Ao mesmo tempo, preserve a distinção entre o que ela contou, o que foi observado e o que ainda precisa ser esclarecido. Isso permite encaminhar a situação com maior precisão.

Se houver sofrimento intenso ou risco concreto à integridade, busque atendimento imediato. O acolhimento não deve esperar que a família descubra quem está por trás de uma conta ou consiga reconstruir toda a conversa (Brasil, 1990; 2017; MDHC, 2026).

11.2 Registre necessidades e procure apoio adequado

Anote apenas o necessário para organizar a ajuda: o que mudou, quando foi percebido e quais providências foram tomadas. Não monte um dossiê de intimidades nem compartilhe suspeitas em grupos. Um registro de

acompanhamento deve servir à proteção, com acesso restrito às pessoas que precisam atuar.

Converse com a escola quando a dificuldade envolver colegas, aprendizagem ou frequência. Procure serviços de saúde diante de sofrimento persistente ou intenso. O Conselho Tutelar pode orientar e articular medidas de proteção quando houver ameaça ou violação de direitos. Suspeitas de crime devem ser comunicadas à autoridade policial competente.

Esses caminhos podem ser acionados em conjunto. Uma providência de saúde não depende da identificação do possível agressor, e a proteção escolar não precisa aguardar a conclusão da investigação. Cada serviço atua conforme sua função e o fluxo de atendimento local.

Exemplo hipotético. Após uma ameaça em grupo, uma estudante teme voltar à escola. A família pode procurar atendimento, comunicar o fato e combinar proteção na rotina escolar. O retorno deve ser acompanhado, sem tratar a retirada de uma mensagem como encerramento automático do problema.

Não use os sinais de atenção para vigiar permanentemente toda expressão de tristeza ou reserva. A proximidade respeitosa ajuda a perceber mudanças e facilita que a criança procure apoio por iniciativa própria (Brasil, 1990, art. 136; 2017).

CAPÍTULO 12**O que fazer diante de violência digital**

12.1 Proteja primeiro e comunique o ocorrido

Ao tomar conhecimento de possível violência, afaste a criança da pressão para continuar o contato e avalie sua segurança imediata. Não organize confronto, não peça novas mensagens ao suspeito e não a mantenha exposta para obter material. Em perigo imediato ou crime em andamento, acione o 190.

Ouçá a revelação espontânea com calma. Pergunte apenas o necessário para saber se há risco atual e qual ajuda precisa ser acionada. A Lei nº 13.431/2017 protege a intimidade e limita intervenções que possam produzir sofrimento adicional. Qualquer pessoa que conheça ou presencie violência tem dever de comunicá-la pelos canais previstos em seu art. 13 (Brasil, 2017).

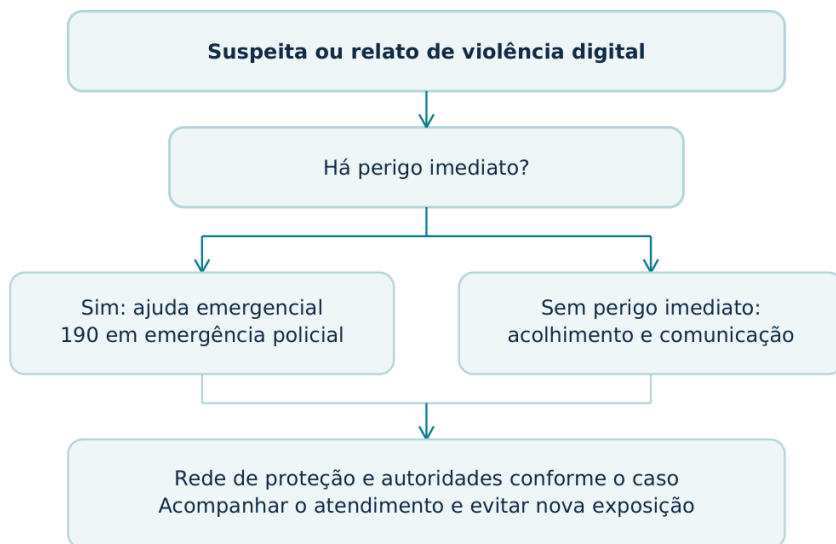
Procure a Polícia Civil para comunicar indícios de crime. O Conselho Tutelar atua na proteção de direitos e na articulação da rede. O Disque 100 recebe e encaminha denúncias de violações de direitos humanos, gratuitamente e durante 24 horas. Ele não substitui o atendimento emergencial pelo 190.

Utilize também os mecanismos da plataforma para denunciar o contato ou o conteúdo e solicitar as providências cabíveis. Guarde o protocolo e identifique a publicação sem redistribuí-la. A comunicação à plataforma não substitui os demais encaminhamentos.

Se o possível agressor estiver no convívio familiar, busque ajuda externa capaz de proteger a criança. Não a entregue a uma situação de confronto ou de nova exposição (Brasil, 1990; 2017; MDHC, [2026?]).

12.2 Organize a resposta conforme a necessidade

A proteção pode exigir providências simultâneas. O fluxo abaixo ajuda a identificar a prioridade, sem impor uma sequência rígida entre atendimento de saúde, comunicação às autoridades e proteção escolar.

Figura 1. Encaminhamento diante de possível violência digital

Fonte: elaboração própria, com base no ECA e na Lei nº 13.431/2017. Perigo imediato exige ajuda emergencial; os demais cuidados continuam depois da primeira intervenção.

Não copie nem redistribua imagens de abuso sexual. Se o conteúdo já estiver no aparelho, evite novas manipulações e procure orientação imediata da autoridade competente. Registre apenas informações disponíveis e seguras, como perfil, endereço, data e horário, sem reabrir o material para completar o relato.

Combine quem acompanhará o atendimento e quais providências terão retorno. A criança precisa saber, em linguagem compreensível, que continuará recebendo apoio (Brasil, 1990; 2017).

CAPÍTULO 13

A escola como parceira da proteção

13.1 Combine um canal reservado de atendimento

A escola pode perceber mudanças de convivência e receber uma revelação antes da família. Por isso, precisa ter um canal acessível, pessoas de referência e um fluxo para acolher, registrar o necessário e acionar a rede de proteção. O atendimento não deve depender de exposição em grupo ou de confronto entre estudantes.

Ao procurar a instituição, relate as informações disponíveis e as necessidades de segurança. Pergunte quem acompanhará o caso, como será preservada a intimidade e quando haverá retorno. A comunicação deve permitir acompanhar as providências sem exigir acesso a dados de outras crianças.

Exemplo hipotético. Um estudante recebe ameaças após a circulação de uma montagem. A escola pode organizar acolhimento e medidas para impedir nova exposição, comunicar os canais competentes e acompanhar a convivência. Não deve projetar a imagem para a turma nem exigir que o estudante repita o relato a cada professor.

A Lei nº 14.811/2024 prevê medidas de proteção contra violência em estabelecimentos educacionais. A Lei nº 13.431/2017 orienta o atendimento de crianças e adolescentes vítimas ou testemunhas, inclusive quanto à proteção da intimidade e à prevenção de sofrimento adicional (Brasil, 2017; 2024).

Quando houver indícios de crime, as autoridades devem ser acionadas pelos canais adequados. Uma solução disciplinar ou uma conversa entre responsáveis não substitui a comunicação e as medidas de proteção cabíveis.

13.2 Desenvolva prevenção durante o ano

A educação digital pode abordar privacidade, respeito às diferenças, pedidos de ajuda, publicidade e verificação de informações. Atividades devem utilizar exemplos adequados à idade, sem imagens de violência sexual nem situações

que exponham estudantes. A prevenção é mais útil quando permite praticar decisões e conhecer os canais de apoio.

A Lei nº 15.100/2025 restringe o uso de aparelhos eletrônicos pessoais por estudantes durante aulas, recreios e intervalos na educação básica, com usos pedagógicos orientados e exceções legais. Entre elas estão acessibilidade, inclusão, condições de saúde e garantia de direitos fundamentais. As regras da escola precisam considerar essas situações (Brasil, 2025a).

A restrição do aparelho não elimina experiências digitais fora da escola. Família e instituição devem combinar como tratar conflitos que repercutem na convivência, sem presumir que todo problema ocorrido na internet seja responsabilidade exclusiva de uma delas.

Revise também os serviços utilizados para atividades escolares. Considere adequação etária, proteção de dados, acessibilidade e alternativa para quem não dispõe de equipamento ou conexão. Uma atividade educativa não deve induzir a falsificar idade para criar uma conta.

Ao divulgar projetos e fotografias, preserve documentos, localização e informações dos estudantes. A instituição precisa aplicar à própria comunicação o cuidado que ensina à comunidade (Brasil, 1990; 2018; Secom, 2025).

CAPÍTULO 14

Construindo um acordo familiar

14.1 Transforme cuidados em combinações possíveis

Um acordo familiar organiza expectativas sobre aparelhos, jogos, contatos, publicações e pedidos de ajuda. Ele funciona melhor quando a criança ou o adolescente compreende o motivo das regras e participa de decisões adequadas ao seu desenvolvimento. A assinatura não substitui presença e acompanhamento.

Comece pelos ambientes realmente utilizados. Combine quais serviços podem ser acessados, como compras serão autorizadas e quem poderá ajudar se houver dificuldade. Defina momentos de descanso e convivência, levando em conta estudo, necessidades de saúde e atividades fora das telas.

Inclua compromissos dos adultos. Respeitar a intimidade, explicar a supervisão e ouvir um pedido de ajuda são partes do acordo. As decisões também devem alcançar o que os responsáveis publicam sobre os filhos e como protegem as próprias contas.

Exemplo hipotético. Uma criança quer participar de um jogo usado pelos colegas. A família pode conferir as condições, experimentar o ambiente e combinar contatos e compras antes de autorizar. Se o serviço não for adequado, deve explicar a decisão e procurar uma alternativa, sem criar idade falsa.

Use frases concretas, que possam ser revistas: pedir autorização antes de uma compra, consultar um adulto diante de ameaça e conferir contatos novos. Evite promessas impossíveis de ausência total de risco ou regras que ninguém consegue cumprir na rotina (Brasil, 2025b; Secom, 2025).

14.2 Reveja o acordo quando as necessidades mudarem

O acordo deve acompanhar mudanças de idade, aparelho, serviço e circunstância familiar. Reserve uma data para rever o que funcionou, o que gerou dificuldade e qual apoio ainda é necessário. O objetivo é desenvolver capacidade de decisão, mantendo proteção adequada.

Descumprir uma combinação pode exigir conversa e consequência educativa proporcional. Se houver violência, porém, o acolhimento vem primeiro. Não retire o acesso à ajuda como punição nem utilize relatos íntimos para constranger. O fato de ter respondido a uma mensagem não autoriza a violência praticada por outra pessoa.

Quando os responsáveis vivem em casas diferentes, procure manter orientações coerentes e canais de contato conhecidos. Não use o acompanhamento digital para vigiar ou disputar a relação da criança com outro adulto. Situações de conflito ou risco devem ser tratadas pelos meios competentes.

Uma revisão útil. Pergunte se o filho sabe a quem recorrer, consegue identificar uma solicitação inadequada e compreende os controles aplicados. Uma resposta incerta indica tema a ser explicado, sem humilhação. Refaça a configuração ou o combinado quando necessário.

O formulário do Apêndice A serve de ponto de partida. Adapte-o à realidade da família e às necessidades de acessibilidade. Não registre senhas ou detalhes de incidentes no acordo. A proteção depende de apoio contínuo e de acesso à rede de atendimento quando necessário (Brasil, 1990; 2017; 2025b).

Considerações finais

Proteger crianças e adolescentes na internet exige conhecer suas experiências e manter um caminho de ajuda acessível. Conversas sobre jogos, amizades e publicações permitem orientar escolhas e compreender situações que talvez não apareçam em uma simples revisão do aparelho.

As configurações de segurança ajudam, mas precisam de acompanhamento e revisão. O crescimento traz novas necessidades, e a autonomia se desenvolve com informação, participação e oportunidade de decidir dentro de condições de proteção. Privacidade e dignidade continuam presentes nesse processo.

Diante de uma possível violência, leve o relato a sério e avalie a segurança imediata. Evite perguntas repetidas, confronto e circulação do material. A família não precisa produzir uma investigação para procurar a rede de proteção, os serviços de saúde ou as autoridades competentes.

O cuidado também depende das escolas, das plataformas e do poder público. Cada um deve cumprir suas funções, com comunicação suficiente para que o atendimento continue depois da primeira denúncia. O desaparecimento de uma publicação não significa, sozinho, que a criança deixou de precisar de apoio.

Utilize os materiais seguintes para organizar combinações, identificar dúvidas e conhecer os caminhos de encaminhamento. Uma rotina em que seja possível pedir ajuda sem medo de humilhação torna a proteção mais próxima das necessidades de quem está em desenvolvimento.

APÊNDICE A

Acordo familiar de segurança digital

Preencha com participação da criança ou do adolescente, conforme seu desenvolvimento. Combine cuidados possíveis e uma data para revisar. Não anote senhas nem relatos de violência neste instrumento.

Ambientes que podemos utilizar e condições de acesso

Como vamos combinar tempo, descanso e atividades

Quem pode autorizar compras e novos contatos

O que vamos conferir antes de publicar imagens

Como o acompanhamento será explicado e revisto

A quem procurar diante de medo, ameaça ou dúvida

Compromissos dos adultos. Ouvir sem humilhar, respeitar a intimidade, explicar as medidas e procurar ajuda competente quando necessário.

Participantes e data da revisão

Fonte: instrumento próprio, com base nos capítulos 9, 10 e 14. O acordo não afasta direitos nem substitui os deveres de proteção.

APÊNDICE B

Recomendações por faixa etária

Estas faixas organizam orientações educativas. Não são autorização para acessar serviços nem substituem avaliação individual, condições de uso ou restrições legais.

Faixa etária	Acompanhamento a priorizar
Até 5 anos	Priorize convivência, brincadeiras e experiências fora das telas. Quando houver uso adequado, acompanhe de perto e ajude a compreender. Evite navegação autônoma, compras e interação livre. Considere necessidades de desenvolvimento e orientação de saúde.
6 a 9 anos	Escolha ambientes e configurações junto com a criança. Ensine a pedir ajuda diante de segredo, cobrança ou contato incômodo. Restrinja compras e mensagens, com presença próxima e explicação das regras.
10 a 12 anos	Converse sobre pressão do grupo, dados pessoais, imagens e identidade dos contatos. Amplie decisões acompanhadas, sem falsear idade. Revise recursos de segurança e combine como encerrar uma interação prejudicial.
13 a 17 anos	Aprofunde privacidade, intimidade, publicidade, manipulação e apoio entre colegas. Negocie responsabilidades e revise a supervisão, respeitando autonomia progressiva. Observe exigências legais de vinculação de contas e as condições de cada serviço.

Necessidades de comunicação, acessibilidade e proteção podem exigir apoio adicional em qualquer idade. A passagem de faixa não libera automaticamente um recurso.

Fonte: síntese educativa própria, orientada pelo ECA, pelo ECA Digital e pelas seções pertinentes do guia da Secom (2025). Não estabelece prescrição clínica de tempo de tela.

APÊNDICE C

Dez perguntas para conversar com os filhos

Escolha um momento tranquilo. As perguntas ajudam a conhecer o cotidiano digital; não são roteiro para investigar uma revelação de violência.

1. O que você mais gosta de fazer quando está conectado?
2. Quem costuma participar dessas atividades com você?
3. O que torna uma conversa agradável ou desconfortável?
4. Como você percebe quando alguém está pressionando?
5. O que faria se alguém pedisse segredo sobre algo assustador?
6. Como podemos conferir um pedido de dinheiro ou de código?
7. O que precisamos pensar antes de publicar uma fotografia?
8. O que ajudaria você a procurar apoio para um amigo?
9. Quais configurações e regras precisamos entender melhor?
10. A quem você pode pedir ajuda se não conseguir falar comigo?

Ouçã sem interromper para corrigir cada resposta. Identifique uma dúvida e retome o assunto em outro momento. Diante de relato de violência, acolha, avalie a segurança e procure os serviços competentes, sem aplicar este questionário.

Fonte: instrumento próprio, com base nos capítulos 3, 5 e 10 e na Lei nº 13.431/2017.

APÊNDICE D

Sinais de atenção e caminhos de apoio

Uma mudança isolada não comprova violência ou crime. Considere contexto, duração e efeitos sobre a rotina; não use o quadro como teste diagnóstico.

O que merece atenção	Como oferecer apoio
Medo de mensagens ou de um contato	Pergunte como a pessoa está e se precisa de proteção. Não a obrigue a retomar a conversa.
Afastamento de colegas ou da escola	Ouçá e procure a escola por canal reservado, sem exposição em grupos.
Alterações persistentes de sono ou rotina	Observe o contexto e busque avaliação de saúde quando necessário.
Cobranças, ameaças ou pedidos de segredo	Interrompa a pressão, avalie o risco atual e procure os canais competentes.
Sofrimento intenso ou perigo imediato	Priorize atendimento urgente. Acione o 190 em emergência policial.

Providência de proteção e pessoa que acompanhará

Não registre imagens íntimas, senhas ou detalhes desnecessários. A orientação deve acolher e facilitar o atendimento, sem atribuir culpa à vítima.

Fonte: capítulos 11 e 12; ECA; Lei nº 13.431/2017; orientação do MDHC (2026).

APÊNDICE E

Roteiro de acolhimento e encaminhamento

1 Proteja a integridade

Afastar da pressão para responder. Em perigo imediato ou crime em andamento, acione o 190. Procure atendimento de saúde quando necessário.

2 Ouça o necessário

Acolha sem culpar e sem perguntas repetidas. Não prometa segredo absoluto. Explique que buscará ajuda para proteger.

3 Evite novas exposições

Não confronte o suspeito, não peça novas mensagens e não faça investigação particular. Não pague nem envie mais material para atender a ameaças.

4 Preserve sem redistribuir

Não copie, baixe ou encaminhe imagens de abuso sexual. Se já estiverem no aparelho, procure orientação imediata da autoridade sobre a preservação. Registre apenas informações disponíveis e seguras.

5 Acione os canais adequados

Polícia Civil para indícios de crime; Conselho Tutelar para proteção de direitos; Disque 100 para denúncia e encaminhamento de violações. O Disque 100 é gratuito, funciona 24 horas e não substitui emergência policial.

6 Acompanhe as providências

Use também a denúncia da plataforma. Guarde protocolos, combine retorno e mantenha o apoio. Não exponha o relato a quem não precisa atuar.

Fonte: capítulos 7 e 12; ECA; Lei nº 13.431/2017; serviço oficial Disque 100. As medidas podem ocorrer simultaneamente.

APÊNDICE F

Página para pais e educadores

Antes de surgir um problema

Conheça os ambientes utilizados, converse sobre contatos e escolha configurações adequadas. Respeite idade, desenvolvimento, privacidade e acessibilidade. Não crie idade falsa para liberar um serviço.

Ensine a pedir ajuda

Ninguém deve exigir dinheiro, código, imagem íntima ou segredo sobre algo assustador. A criança pode procurar apoio mesmo depois de ter respondido ou descumprido uma regra.

Se houver revelação

Ouça com calma, leve o relato a sério e avalie a segurança. Não interrogue, não peça demonstrações e não confronte o possível agressor. Encaminhe à rede competente.

Cuide das informações

Não copie nem redistribua imagens de abuso sexual. Procure orientação imediata das autoridades sobre material já disponível. Não publique relatos ou suspeitas em grupos.

Conheça os caminhos

Perigo imediato ou crime em andamento: 190. Indícios de crime: Polícia Civil. Proteção de direitos: Conselho Tutelar. Denúncias de violações de direitos humanos: Disque 100, gratuito e disponível 24 horas. Acione saúde e escola conforme a necessidade.

Referência de apoio da família ou da escola

Fonte: síntese da cartilha. Material gratuito para compartilhar. O resumo de duas páginas está no Apêndice G.

APÊNDICE G

Resumo para compartilhar

Orientações para famílias e educadores

Conheça o cotidiano digital

Pergunte o que a criança ou o adolescente gosta de fazer, com quem conversa e como pede ajuda. Experimente os ambientes juntos, quando adequado. Considere conteúdo, contatos e efeitos sobre sono, estudo, convivência e atividades fora das telas.

Configure e explique a proteção

Respeite idade, condições do serviço e restrições legais. Não crie uma idade falsa para liberar acesso. Revise privacidade, contatos, compras, localização e recuperação de contas. Use senhas diferentes e verificação adicional. Explique o acompanhamento e reveja as medidas conforme o desenvolvimento.

Converse sobre pedidos inadequados

Nome, fotografia, voz e vídeo não confirmam uma identidade. Ninguém deve exigir dinheiro, código, imagem íntima ou segredo sobre algo assustador. A criança pode recusar, interromper a conversa e procurar apoio, mesmo depois de ter respondido ou descumprido uma regra.

Proteja imagens e informações

Antes de publicar, observe uniforme, endereço, documentos e localização. Respeite a intimidade e o desconforto dos filhos. Perfis restritos não impedem cópias. Não compartilhe ataques, montagens íntimas ou relatos de vítimas para tentar alertar um grupo.

Mantenha um caminho de ajuda

Combine uma pessoa de referência e outra alternativa acessível. A escola deve oferecer um canal reservado e conhecer o fluxo de proteção. Mudanças de

comportamento merecem atenção, mas não comprovam, sozinhas, violência ou crime.

Pessoas de confiança e como procurá-las

Acolhimento não depende de prova apresentada pela criança. Este resumo acompanha a cartilha completa, que contém capítulos, referências, acordo familiar e outros materiais para impressão. Não anote senhas ou detalhes de violência nesta folha.

Se houver ameaça ou violência

Proteja e procure os canais adequados

Leve o relato a sério, avalie a segurança e explique que buscará ajuda. As providências podem ocorrer simultaneamente, conforme a necessidade.

Interrompa a pressão

Não mantenha a criança em contato para obter material. Não confronte o possível agressor, não organize encontro e não pague nem envie mais imagens para atender a chantagem. Em perigo imediato ou crime em andamento, acione o 190.

Acolha sem interrogar

Ouçã com calma e pergunte apenas o necessário para a segurança imediata. Não exija demonstrações, gravações ou repetição do relato a várias pessoas. Não prometa segredo absoluto, pois pode ser necessário acionar profissionais de proteção. A violência não é justificada por uma regra descumprida.

Não copie nem redistribua imagens de abuso sexual

Não baixe o material, não o envie a grupos e não o submeta a sites ou ferramentas de inteligência artificial. Se já estiver no aparelho, evite novas manipulações e procure orientação imediata da autoridade competente sobre a preservação e a apresentação adequada.

Registre somente informações disponíveis e seguras, como perfil, endereço da publicação, data e horário. Não reabra conteúdo sexual para completar um registro e não faça investigação particular.

Acione a rede conforme o caso

Polícia Civil: comunicação de indícios de crime e providências de investigação. Conselho Tutelar: proteção de direitos e articulação da rede. Disque 100: denúncia e encaminhamento de violações de direitos humanos, gratuitamente e durante 24 horas. O Disque 100 não substitui emergência policial.

Procure atendimento de saúde quando necessário e combine proteção na escola. Utilize também a denúncia da plataforma e guarde protocolos. Se o possível agressor estiver no convívio familiar, procure ajuda externa capaz de proteger a criança.

Continue acompanhando

Combine quem acompanhará o atendimento e quando haverá retorno. A retirada de uma publicação não encerra automaticamente a necessidade de apoio. Preserve a intimidade e evite circular suspeitas em grupos.

Serviço procurado, protocolo e próxima providência

Fonte: capítulos 7, 10, 11 e 12 e referências do Volume 08, especialmente ECA, Lei nº 13.431/2017 e serviço oficial Disque 100. Distribuição gratuita. Cartilha completa e canais do autor: www.higorjorge.com.br.

Referências

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Câmara dos Deputados, 1988. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-normaatualizada-pl.html>. Acesso em: 24 jun. 2026.

BRASIL. **Decreto nº 12.880, de 18 de março de 2026**. Regulamenta a Lei nº 15.211/2025 e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: Câmara dos Deputados, 2026. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2026/decreto-12880-18-marco-2026-798813-publicacaooriginal-178481-pe.html>. Acesso em: 20 ago. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Brasília, DF: Câmara dos Deputados, 1990. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1990/lei-8069-13-julho-1990-372211-normaatualizada-pl.html>. Acesso em: 22 ago. 2026.

BRASIL. **Lei nº 13.431, de 4 de abril de 2017**. Estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência. Brasília, DF: Câmara dos Deputados, 2017. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2017/lei-13431-4-abril-2017-784569-normaatualizada-pl.pdf>. Acesso em: 13 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Câmara dos Deputados, 2018. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html>. Acesso em: 11 set. 2026.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais e altera a legislação penal. Brasília, DF: Câmara dos Deputados, 2024. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2024/lei-14811-12-janeiro-2024-795244-publicacaooriginal-170834-pl.html>. Acesso em: 20 jul. 2026.

BRASIL. **Lei nº 15.100, de 13 de janeiro de 2025**. Dispõe sobre a utilização de aparelhos eletrônicos portáteis pessoais por estudantes na educação básica. Brasília, DF: Câmara dos Deputados, 2025a. Disponível em:

<https://www2.camara.leg.br/legin/fed/lei/2025/lei-15100-13-janeiro-2025-796892-publicacaooriginal-174094-pl.html>. Acesso em: 20 set. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Estatuto Digital da Criança e do Adolescente. Brasília, DF: Câmara dos Deputados, 2025b. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2025/lei-15211-17-setembro-2025-797997-normaatuallizada-pl.pdf>. Acesso em: 25 jun. 2026.

CERT.br. **Autenticação**. [S. l.]: NIC.br, nov. 2022. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf>. Acesso em: 19 set. 2026.

CERT.br. **Inteligência artificial**. [S. l.]: NIC.br, set. 2026. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/ia/fasciculo-ia.pdf>. Acesso em: 1 out. 2026.

CERT.br. **Privacidade**. [S. l.]: NIC.br, ago. 2023. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/privacidade/fasciculo-privacidade.pdf>. Acesso em: 13 jun. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais**. 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

MINISTÉRIO DOS DIREITOS HUMANOS E DA CIDADANIA (Brasil) (MDHC). **Denunciar violação de direitos humanos**. Brasília, DF: MDHC, [2026?]. Serviço Disque 100, versão corrente. Disponível em: <https://www.gov.br/pt-br/servicos/denunciar-violacao-de-direitos-humanos>. Acesso em: 25 out. 2026.

MINISTÉRIO DOS DIREITOS HUMANOS E DA CIDADANIA (Brasil) (MDHC). **Segurança digital: como proteger crianças e adolescentes no ambiente online**. Brasília, DF: MDHC, 16 set. 2026. Disponível em: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2026/defeso-eleitoral/setembro/seguranca-digital-como-proteger-criancas-e-adolescentes-no-ambiente-online>. Acesso em: 5 out. 2026.

SAFERNET BRASIL. **O que é sextorsão?** [S. l.]: SaferNet Brasil, [2026?]. Versão eletrônica corrente, sem data editorial identificada. Disponível em: <https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o>. Acesso em: 3 ago. 2026.

SECRETARIA DE COMUNICAÇÃO SOCIAL (Brasil) (Secom). **Crianças, adolescentes e telas: guia sobre usos de dispositivos digitais**. Brasília, DF: Secom, 2025.

Consultados capítulos pertinentes e resumo executivo no portal institucional.

Disponível em: <https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia>. Acesso em: 29 jun. 2026.

UNICEF. **Cyberbullying: o que é e como pará-lo**. [S. l.]: Unicef, [2026?]. Versão eletrônica corrente, sem data editorial identificada. Disponível em:

<https://www.unicef.org/brazil/cyberbullying-o-que-eh-e-como-para-lo>. Acesso em: 9 out. 2026.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne oito cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

- Vol. 01** **Investigação Criminal Tecnológica.** Fundamentos, métodos e aplicações práticas
- Vol. 02** **Provas digitais e cadeia de custódia.** Da coleta à valoração jurídica
- Vol. 03** **Inteligência artificial na investigação criminal.** Aplicações, limites e boas práticas
- Vol. 04** **Golpes digitais e fraudes eletrônicas.** Prevenção, identificação e investigação
- Vol. 05** **Investigação de crimes na internet.** Dados, registros, sigilos e medidas judiciais
- Vol. 06** **Raciocínio investigativo e decisão fundamentada.** Do indício ao relatório final
- Vol. 07** **Internet segura.** Guia prático para proteger você e sua família
- Vol. 08** **Crianças e adolescentes na internet.** Guia de proteção para pais e responsáveis (este volume)

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge