



ECA DIGITAL NA ESCOLA





ECA DIGITAL NA ESCOLA





Prefeito Municipal

Zenildo Matos Oliveira

Dirigente Municipal de Educação

Ivanoilda Azevedo de Oliveira

Todos os direitos desta edição reservados a Secretaria Municipal de Educação de Itaeté-BA.

Dados de Catalogação

ITAETÉ, Secretaria Municipal de Educação. ECA Digital na Escola. Itaeté, BA. 2026

Itaeté-BA
2026

SUMÁRIO

Apresentação	7
O que é o ECA Digital?	8
Princípios do ECA Digital na Comunidade Escolar	9
Proteção Integral na Escola: Medidas Práticas	10
Responsabilidades na Construção de Uma Cultura Digital Segura	13
Conexão Segura: Orientações Práticas Para as Famílias	14
Riscos no Ambiente Escolar e Digital	16
O Papel da Escola e da Família	17
Riscos, Violências e Crimes Digitais	17
Desafios Contemporâneos: Os Novos Riscos Digitais	19
Protegendo a Identidade dos Estudantes: Uso de Imagens, Dados e Limites Legais	20
O Que Pode Ser Considerado Imagem?	21
Atenção Pais e Responsáveis	23
O Que Diz a Lei?	23
Cyberbullying: prevenção, identificação e resposta	24
O Que a Vítima e a Família Devem Fazer?.....	25
O Que A Escola Deve Fazer?	25
Alerta Legal: Cyberbullying é Crime	26
O Papel do Professor na Educação Preventiva	26
Responsabilidade Institucional: O Papel Legal da Escola	29
Dever de Comunicação: Ação Imediata e Integrada	29
Segurança Jurídica: A Escola e a Rede De Proteção Legal	30
Considerações Finais: Juntos Por Uma Escola Mais Segura	32
Contatos Úteis	32
Referências	33

APRESENTAÇÃO



As transformações sociais impulsionadas pelas tecnologias digitais trouxeram novos desafios para os sistemas educacionais, especialmente na garantia dos direitos de crianças e adolescentes na rede. Nesse cenário, torna-se fundamental fortalecer práticas pedagógicas e institucionais que promovam a cidadania digital, a proteção integral e o uso ético, crítico e responsável da tecnologia no ambiente escolar.

Esta cartilha foi elaborada para subsidiar escolas, gestores, professores, famílias e toda a comunidade educativa. O objetivo é conectar os direitos de crianças e adolescentes às suas vivências digitais contemporâneas, fundamentando-se nas principais normativas de proteção vigentes:

- **ECA Digital (Lei nº 15.211/2025):** Estatuto Digital da Criança e do Adolescente;
- **ECA (Lei nº 8.069/1990):** Estatuto da Criança e do Adolescente;
- **LGPD (Lei nº 13.709/2018):** Lei Geral de Proteção de Dados Pessoais;
- **Marco Civil da Internet (Lei nº 12.965/2014);**
- **Lei nº 14.811/2024:** Medidas de proteção contra a violência escolar e virtual.

A partir deste arcabouço, o documento apresenta orientações práticas e reflexões para construir ambientes digitais mais seguros, inclusivos e educativos.

Sabemos que a proteção no contexto digital exige ações articuladas e compartilhadas entre escolas, famílias, poder público, plataformas digitais e sociedade civil. Por isso, este documento busca fortalecer o compromisso coletivo com a garantia de direitos, a prevenção de violências digitais, a segurança de dados e a formação integral dos estudantes.

O que é o ECA Digital?

O termo refere-se à aplicação dos princípios e mecanismos de proteção do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) ao ambiente virtual. Não se trata de uma nova lei, mas sim da certeza de que os direitos fundamentais de crianças e adolescentes devem ser garantidos, com prioridade absoluta, também na internet.

surgiu diante de conflitos e fatos sociais, envolvendo crianças e adolescentes violentadas física, psicológica e/ou sexualmente, onde estabelece regras específicas para garantir a proteção prioritária de crianças e adolescentes em ambientes digitais, incluindo redes sociais, aplicativos, jogos eletrônicos, plataformas educacionais, sistemas operacionais e demais serviços online.

Seu eixo central é o melhor interesse da criança e do adolescente, assegurando:

- privacidade e proteção de dados
- segurança digital
- prevenção contra violências online
- acesso seguro e adequado à idade
- educação digital crítica e responsável
- proteção contra exploração comercial e publicidade abusiva.

A presença da tecnologia no cotidiano infanto-juvenil expande o acesso à informação e à aprendizagem. Contudo, exige barreiras de proteção contra ameaças frequentes, tais como:

- Exposição indevida de dados pessoais e imagem;
- *Cyberbullying* e violência virtual;
- Assédio online e desinformação;
- Uma Responsabilidade Compartilhada.

Garantir a cidadania digital de forma segura é um dever coletivo que envolve famílias, órgãos públicos, plataformas digitais e, essencialmente, a comunidade escolar. Cabe à escola promover ações pedagógicas focadas no uso ético, crítico e responsável das tecnologias.

Além do ECA, a proteção no ambiente digital é reforçada por outros marcos normativos brasileiros, como a Lei Geral de Proteção de Dados Pessoais (LGPD), o Marco Civil da Internet e as normativas voltadas à segurança, privacidade e proteção de direitos no

ambiente digital.

O ECA Digital é, portanto, o principal referencial para guiar a sociedade na construção de um ambiente conectado mais seguro e humano.



PRINCÍPIOS DO ECA DIGITAL NA COMUNIDADE ESCOLAR

A proteção do público infanto-juvenil nos ambientes digitais deve fundamentar-se nos princípios do Estatuto da Criança e do Adolescente (ECA) e nas normas de direitos digitais. No contexto escolar, essas diretrizes orientam decisões, práticas pedagógicas e procedimentos institucionais para promover um espaço seguro, respeitoso e inclusivo.

Proteção Integral: Crianças e adolescentes são sujeitos de direitos e devem ser protegidos em todos os espaços, inclusive no virtual. A escola deve adotar medidas preventivas que assegurem o desenvolvimento saudável dos estudantes no uso das tecnologias.

Interesse Superior do Aluno: Toda decisão sobre o uso de recursos tecnológicos, divulgação de informações, compartilhamento de imagens ou tratamento de dados deve priorizar o bem-estar, a dignidade e a segurança dos estudantes.

Privacidade e Proteção de Dados: As informações pessoais dos alunos devem ser tratadas com responsabilidade, observando a segurança e a confidencialidade. A coleta e o armazenamento de dados devem ocorrer estritamente para finalidades pedagógicas

legítimas, em conformidade com a LGPD.

Respeito à Imagem e à Dignidade: O uso de fotos, vídeos ou áudios que permitam identificar os menores deve respeitar o direito à privacidade. A publicação desses materiais exige rígidos critérios de autorização para evitar a exposição indevida.

Prevenção e Enfrentamento de Violências Digitais: A comunidade escolar deve agir ativamente contra o *cyberbullying*, discurso de ódio, assédio *online*, discriminação e exposição vexatória em ambiente virtual.

Educação para a Cidadania Digital: O uso das tecnologias deve ser indissociável de ações educativas que promovam ética, pensamento crítico e respeito aos direitos humanos, preparando os estudantes para uma navegação consciente.

Corresponsabilidade Coletiva: A segurança digital não é um dever isolado. Escola, famílias, órgãos públicos e plataformas digitais devem atuar de forma articulada para orientar e proteger os jovens no mundo conectado.

Escuta, Acolhimento e Proteção: Situações de risco ou violação de direitos exigem escuta qualificada e acolhimento imediato. A escola deve garantir protocolos para proteger as vítimas, preservar evidências e acionar a rede de proteção social sempre que necessário.

Esses princípios consolidam uma cultura digital baseada na responsabilidade, fortalecendo o compromisso da comunidade escolar com a formação cidadã e a garantia de direitos.

PROTEÇÃO INTEGRAL NA ESCOLA: MEDIDAS PRÁTICAS

A proteção integral de crianças e adolescentes no ambiente escolar exige medidas preventivas, educativas e protetivas que assegurem seus direitos tanto nos espaços físicos quanto nos digitais. Mais do que reagir a situações de risco, cabe à escola estruturar ações permanentes que promovam a segurança, a cidadania digital e o desenvolvimento saudável dos estudantes.

Para fortalecer a atuação institucional, cinco medidas são fundamentais:

1. Instituir Protocolo Formal de Prevenção e Resposta a Riscos Digitais

Toda unidade escolar deve dispor de procedimentos claros e formalizados no Regimento

Escolar ou em normativas institucionais específicas. Isso garante segurança jurídica e uniformidade na atuação da equipe, reduzindo improvisações diante de crises.



Escutar também é proteger. Crianças e adolescentes que se sentem ouvidos têm mais segurança para relatar situações de violência e buscar ajuda.

O protocolo deve normatizar:

- Estabelecer fluxos claros de comunicação e denúncia;
 - Definir os responsáveis pelo acolhimento e acompanhamento dos casos;
 - Padronizar os procedimentos para registro das ocorrências;
 - Orientar a equipe sobre como preservar evidências digitais (prints, links, arquivos);
- Articular os encaminhamentos aos órgãos da rede de proteção (Conselho Tutelar, Ministério Público, etc.);
 - Estruturar a comunicação imediata e adequada com as famílias;
 - Fixar responsabilidades e prazos rígidos para cada etapa do atendimento.

2. Implementar uma Cultura Permanente de Educação Digital

A proteção integral pressupõe ações pedagógicas contínuas que promovam o uso consciente, ético e seguro das tecnologias, integrando a cidadania digital à rotina escolar.

Para isso, a escola deve desenvolver:

- Projetos pedagógicos contínuos sobre direitos e deveres no ambiente virtual;
- Oficinas práticas sobre privacidade, proteção de dados e segurança *online*;
- Campanhas de prevenção contra o *cyberbullying* e o discurso de ódio;
- Rodas de conversa sobre ética, empatia e convivência saudável nas redes sociais;
- Análises de casos reais e textos de apoio que estimulem o pensamento crítico dos estudantes sobre o consumo de informação.

3. Criar Canais Seguros de Escuta, Acolhimento e Denúncia

O público infanto-juvenil precisa saber exatamente onde e como buscar ajuda ao enfrentar situações de violência, exposição indevida, ameaças ou assédio.

A escola deve estabelecer canais de comunicação acessíveis e confiáveis, assegurando:

- Espaços reservados que garantam a privacidade e o acolhimento livre de julgamentos;
- Sigilo e confidencialidade estrita das informações coletadas;
- Proteção integral da identidade dos envolvidos;
- Resposta institucional ágil, responsável e sem omissões;
- Parceria direta com profissionais da rede municipal (psicologia, assistência social e saúde).

4. Revisar e Fortalecer as Políticas de Uso de Imagem e Proteção de Dados

A utilização de registros audiovisuais e dados pessoais de estudantes exigem rigor técnico para evitar danos à privacidade e à segurança, além de mitigar responsabilidades civis e administrativas para a instituição.

A escola deve adotar fluxos internos que garantam:

- Coleta de autorização prévia, expressa e específica dos responsáveis legais;
- Delimitação clara das finalidades de uso de cada imagem ou dado coletado;
- Controle rigoroso das publicações em canais oficiais e materiais de divulgação;
- Armazenamento seguro de arquivos e descarte adequado de documentos com dados pessoais;
- Conformidade irrestrita com a Lei Geral de Proteção de Dados Pessoais (LGPD).

A construção de um ambiente conectado seguro demanda o compromisso permanente de toda a comunidade educativa. Quando prevenção, educação, acolhimento e proteção caminham juntos, a escola cumpre sua função social, garantindo o desenvolvimento pleno e saudável de seus estudantes dentro e fora das redes.

5. Formar Continuamente Toda a Equipe Escolar

A efetivação dessas barreiras de proteção depende da preparação técnica de diretores, coordenadores, professores e funcionários de apoio. Todos devem compreender suas responsabilidades legais e funcionais.

As formações continuadas devem abordar:

- Legislação aplicada: Direitos da criança, do adolescente e marcos regulatórios digitais;
- Sinais de alerta: Como identificar indícios de violência, abuso, automutilação ou exploração;
- Protocolos de ação: Como acolher a vítima e realizar os encaminhamentos institucionais;
- Limites da atuação: Direitos, deveres e o respaldo legal do profissional da educação.

RESPONSABILIDADES NA CONSTRUÇÃO DE UMA CULTURA DIGITAL SEGURA

A proteção de crianças e adolescentes no ambiente digital exige a atuação articulada de toda a comunidade escolar. Como espaço de formação e cuidado, a escola tem papel fundamental na promoção do uso ético, seguro e responsável das tecnologias.

Diretores, coordenadores pedagógicos, professores e familiares possuem responsabilidades específicas na prevenção de riscos, na orientação dos estudantes e na construção de práticas que fortaleçam a cidadania digital.

Público	O que fazer	O que evitar
Diretores (Gestão, Estrutura e Legalidade)	• Atualizar o Regimento Escolar e contratos da escola incluindo regras explícitas sobre cidadania digital, uso de dispositivos e conformidade com a LGPD. • Estruturar canais seguros e anônimos de denúncia interna para a comunidade escolar. • Mapear a rede de apoio externa, sabendo exatamente quando e como acionar o Conselho Tutelar ou delegacias especializadas.	• Ignorar os conflitos digitais sob a justificativa de que "aconteceram fora do horário escolar" ou em redes privadas. • Divulgar imagens, nomes ou dados de alunos em redes sociais da escola sem autorização expressa e assinada pelos responsáveis.
Coordenadores (Mediação, Prevenção e Formação)	• Promover formação continuada para o corpo docente identificar sinais de violência ou sofrimento online. • Mediar conflitos com escuta ativa, acolhendo tanto a família da vítima	• Aplicar medidas punitivas extremas (como expulsão imediata) sem antes entender o contexto e a intencionalidade do ato.

	quanto a do agressor de forma pedagógica. • Desenvolver ações de letramento digital e conscientização parental com as famílias.	• Deixar de registrar formalmente as ocorrências , perdendo o histórico e o respaldo legal da instituição.
Professores (Cotidiano, Manejo e Intervenção)	• Integrar debates sobre fake news , privacidade e empatia digital de forma natural em suas matérias. • Manter um olhar atento a mudanças bruscas de comportamento ou ansiedade ligada ao uso do celular em sala. • Documentar e reportar imediatamente o caso à coordenação assim que tomar conhecimento dele.	• Expor ou confrontar o aluno que cometeu o erro na frente da turma inteira. • Tentar investigar o caso por conta própria ou misturar canais de contato pessoais (redes privadas) com os estudantes fora do ambiente escolar. • Orientar a apagar as provas (mensagens/prints) antes do registro oficial.

CONEXÃO SEGURA: ORIENTAÇÕES PRÁTICAS PARA AS FAMÍLIAS

A proteção dos nossos filhos no mundo digital não acontece apenas na escola; ela começa em casa. A internet oferece um universo de aprendizado, mas exige supervisão, diálogo e limites claros. Veja passos práticos para construir uma rotina digital segura em seu lar:



1. Diálogo Aberto

- **Seja o porto seguro:** Converse com seus filhos sobre o que eles fazem na internet. Mostre que, se algo os deixar desconfortáveis, assustados ou tristes *online*, eles podem e devem procurar você sem medo de castigos.
- **Combine as regras:** Estabeleça horários e locais permitidos para o uso de telas. Evite o uso de celulares e tablets durante as refeições e antes de dormir.
- **Ensine o valor da privacidade:** Explique que o mundo virtual é um espaço público. Oriente-os a nunca compartilhar dados como endereço, telefone, nome da escola ou fotos com uniforme com desconhecidos.

2. Mediação Técnica (Ferramentas de Proteção)

- **Ative o Controle Parental:** Utilize aplicativos e ferramentas nativas dos sistemas operacionais (como *Google Family Link* ou ferramentas da *Apple*) para gerenciar o tempo de tela e filtrar conteúdos inadequados para a idade.
- **Configure filtros de busca:** Ative a opção de "Busca Segura" (*SafeSearch*) nos motores de pesquisa e configure as contas de *streaming* (YouTube, Netflix) no modo infantil/restrito.
- **Mantenha as telas à vista:** Especialmente para crianças menores, o ideal é que o uso da internet ocorra em espaços comuns da casa (como a sala), facilitando a supervisão natural dos pais.



A presença ativa da família no uso das tecnologias ajuda a prevenir golpes, aliciamentos, exposição indevida de informações e outras situações de risco.

3. Atenção à Exposição (*Sharenting*)

- **Pense antes de postar:** Evite publicar fotos dos seus filhos que revelem a rotina deles (uniforme escolar, fachada do condomínio, locais que frequentam rotineiramente).
- **Preserve a dignidade do menor:** Não poste imagens que possam causar constrangimento ao seu filho no futuro (momentos de birra, fotos sem roupa na praia/piscina). Lembre-se: a pegada digital que criamos para eles hoje permanece no futuro.



4. Fique Alerta aos Sinais de Mudança

Mudanças bruscas de comportamento podem indicar que algo não vai bem no ambiente virtual (como casos de *cyberbullying* ou assédio). Fique atento se o seu filho apresentar:

- Isolamento repentino ou recusa em ir à escola;
- Ansiedade, irritabilidade ou tristeza logo após usar o celular;
- Mudanças drásticas no padrão de sono ou apetite;
- Esconder a tela do celular ou fechar abas do computador rapidamente quando alguém se aproxima.

Parceria Escola e Família: Se notar qualquer comportamento suspeito ou se seu filho relatar alguma violência virtual envolvendo colegas, procure imediatamente a coordenação da escola. Juntos, podemos agir de forma rápida e protetiva.

RISCOS NO AMBIENTE ESCOLAR E DIGITAL



O avanço da tecnologia na educação abriu portas para o aprendizado e a conexão. No entanto, também trouxe desafios que exigem atenção para garantir o desenvolvimento seguro e saudável de crianças e adolescentes.

Abaixo, destacamos os principais pontos de atenção no dia a dia escolar e digital:

1. **Cyberbullying:** Agressões, humilhações e ameaças feitas por redes sociais, mensagens ou jogos online.



Impacto: Afeta a autoestima, o rendimento escolar e a saúde emocional.

2. **Exposição Excessiva (Oversharing):** Compartilhamento sem critérios de fotos, vídeos, rotinas e dados pessoais.



Impacto: Viola a privacidade e expõe o estudante a situações de vulnerabilidade física e digital.

3. **Contato com Desconhecidos e Aliciamento:** Aproximação de perfis falsos ou pessoas mal-intencionadas que tentam manipular, extorquir ou explorar os jovens.



Impacto: Riscos graves à segurança física e psicológica.

4. **Desinformação e Conteúdos Inadequados:** Acesso a fake news, discursos de ódio, conteúdos violentos ou impróprios para a idade.



Impacto: Distorção da realidade e influência negativa em comportamentos e opiniões.

5. **Dependência e Uso Excessivo:** Uso descontrolado de telas, celulares e videogames, muitas vezes de madrugada.

 **Impacto:** Prejudica o sono, a concentração, as relações familiares e a saúde física.

6. Golpes e Fraudes Virtuais: Links falsos com promessas de vantagens em jogos, roubo de contas de redes sociais ou clonagem de cartões dos pais.

 **Impacto:** Prejuízos financeiros e invasão de privacidade da família.

O PAPEL DA ESCOLA E DA FAMÍLIA

Proteger crianças e adolescentes na internet **não significa isolá-los da tecnologia**, mas ensiná-los a navegar com consciência e responsabilidade. Essa é uma missão conjunta:

- **Pela Família:** Estabelecer limites claros de tempo de tela, acompanhar os conteúdos consumidos e manter um canal aberto de diálogo, sem julgamentos.
- **Pela Escola:** Promover a cidadania digital, debater a ética na internet e oferecer um ambiente seguro para que o aluno possa relatar se algo der errado.



Se não faremos ou diremos algo no mundo real, não devemos fazer ou dizer no mundo digital. O respeito e a segurança começam na orientação.

RISCOS, VIOLÊNCIAS E CRIMES DIGITAIS

No ambiente virtual, a linha entre uma brincadeira de mau gosto, uma atitude violenta e um ato criminoso pode parecer sutil, mas as consequências são reais. Para proteger nossas crianças e adolescentes, precisamos aprender a identificar e diferenciar cada uma dessas situações.

1. Riscos Digitais (O que pode acontecer)

São situações de vulnerabilidade às quais os estudantes estão expostos ao navegar na internet. Muitas vezes ocorrem por falta de maturidade, distração ou desconhecimento das ferramentas de segurança. Com exemplos: Compartilhar a rotina de onde estuda, aceitar convites de desconhecidos em jogos online, clicar em links suspeitos que prometem "moedas virtuais" gratuitas ou passar tempo excessivo em frente às telas.

- **Como agir:** Com **prevenção e educação**. É o momento de ensinar sobre privacidade, configuração de contas e uso consciente da tecnologia.

2. Violências Digitais (O que fere e adocece)

Ocorre quando a tecnologia é utilizada intencionalmente para agredir, humilhar, isolar ou intimidar alguém. Mesmo quando não configuram um crime tipificado por lei, geram profundo sofrimento emocional e exclusão social.

- **Exemplos: Cyberbullying** (exclusão de grupos de mensagens, criação de figurinhas/memes para ridicularizar um colega), discursos de ódio e a propagação de fofocas ou boatos em páginas de "confissões" da escola.
- **Como agir:** Com **intervenção e acolhimento**. A escola e a família devem atuar aplicando o regimento escolar, conversando com os envolvidos e oferecendo apoio psicológico à vítima.

3. Crimes Digitais (O que viola a lei)

São condutas graves praticadas no ambiente virtual que violam as leis do país (como o Código Penal e o Estatuto da Criança e do Adolescente). Quando praticados por adultos, geram prisão; quando praticados por menores de idade, configuram **atos infracionais** sujeitos a medidas socioeducativas:

- **Calúnia, Difamação e Injúria:** Inventar crimes ou xingar alguém publicamente na internet.
- **Falsa Identidade:** Criar perfis fakes usando fotos e o nome de outra pessoa para prejudicá-la.
- **Ameaça:** Enviar mensagens afirmando que fará mal à integridade física do colega ou de sua família.
- **Crimes contra a Dignidade Sexual:** Aliciamento de menores, solicitação, produção ou compartilhamento de fotos íntimas (nudes) de crianças e adolescentes.

FIQUE DE OLHO:



O que mudou recentemente?

DESAFIOS CONTEMPORÂNEOS: OS NOVOS RISCOS DIGITAIS

O universo digital muda em um ritmo acelerado. Ferramentas que não existiam há poucos anos hoje fazem parte da rotina de crianças e adolescentes. Para proteger essa nova geração, precisamos estar atualizados sobre os desafios contemporâneos que surgiram com as novas tecnologias:

1. O Uso Indevido de Inteligência Artificial (IA)

A IA trouxe facilidades para os estudos, mas também abriu margem para novos tipos de violência digital que utilizam a imagem e a voz dos estudantes sem autorização.

- **Deepfakes e Montagens:** Uso de aplicativos para simular a voz de professores ou criar nudes falsos (montagens hiper-realistas) usando fotos do rosto de colegas colados em corpos nus.
- **Plágio Automatizado:** Dependência excessiva de ferramentas de IA para realizar tarefas escolares, prejudicando o pensamento crítico e o aprendizado real.



Sinal de Alerta: Isolamento do estudante ou surgimento de boatos na escola envolvendo fotos ou áudios estranhos de alunos e funcionários.

2. Algoritmos de Radicalização e "Tocas de Coelho" (Rabbit Holes)

As redes sociais usam algoritmos desenhados para reter a atenção do usuário. O problema ocorre quando o sistema percebe o interesse do jovem por temas sensíveis e passa a inundar seu feed com conteúdos cada vez mais extremos.

- **Conteúdos de Autolesão e Transtornos Alimentares:** Páginas que romantizam a automutilação ou dietas extremas e perigosas.
- **Discursos de Ódio e Extremismo:** Comunidades virtuais que cooptam jovens vulneráveis, incentivando a intolerância, o preconceito e a violência física no ambiente escolar.

Sinal de Alerta: Mudança repentina de vocabulário (uso de termos preconceituosos ou de nichos obscuros da internet), radicalização de opiniões e obsessão por fóruns fechados.



3. Cassinos Online e a Gamificação de Apostas (Bets)

A fronteira entre jogos eletrônicos (games) e jogos de azar (apostas) ficou muito tênue. Influenciadores digitais promovem plataformas de apostas disfarçadas de joguinhos divertidos, atraindo o público infantojuvenil.

- **Loot Boxes e Apostas:** Jogos que cobram dinheiro real por recompensas aleatórias e influenciadores que ensinam "estratégias" para ganhar dinheiro em plataformas de apostas proibidas para menores.
- **Compulsão Financeira:** Casos de adolescentes que gastam a mesada ou usam cartões dos pais escondidos para alimentar o vício nesses jogos.



Sinal de Alerta: Pedidos constantes de dinheiro, ansiedade extrema ao jogar no celular ou queda brusca no rendimento escolar por passar as noites jogando.

4. Desafios Virais Perigosos (Challenges)

Plataformas de vídeos curtos frequentemente viralizam "desafios" que estimulam crianças e adolescentes a realizarem ações perigosas contra si mesmos ou contra terceiros em busca de curtidas e validação social.

- **Riscos à Vida:** Desafios que envolvem asfixia, ingestão de substâncias perigosas ou invasão de propriedades.

Sinal de Alerta: Marcas roxas no pescoço/braços, sumiço de produtos de limpeza ou remédios de casa, ou relatos de "brincadeiras" estranhas na hora do intervalo na escola.



PROTEGENDO A IDENTIDADE DOS ESTUDANTES: USO DE IMAGENS, DADOS E LIMITES LEGAIS

Um dos direitos da personalidade assegurados pela Constituição Federal de 1988 e pelo Código Civil de 2002 é o direito à imagem, garantindo a todo cidadão o controle sobre o uso, a divulgação e a reprodução de sua imagem, protegendo sua identidade, dignidade, privacidade e honra.

A proteção da imagem acompanha o indivíduo ao longo de toda a vida e, em determinadas situações, pode ser resguardada mesmo após o falecimento. Além disso, a imagem é considerada um dado pessoal, estando também protegida pela Lei Geral de Proteção de Dados (LGPD), que estabelece regras para sua coleta, armazenamento, compartilhamento e utilização.

O QUE PODE SER CONSIDERADO IMAGEM?

A imagem de uma pessoa pode se manifestar de diferentes formas:

- a) Imagem-retrato** - Corresponde à representação física e visual da pessoa, por meio de fotografias, vídeos, pinturas, desenhos, caricaturas, ilustrações ou recursos de computação gráfica.
- b) Imagem-atributo** - Refere-se ao conjunto de características, qualidades, comportamentos e atributos pelos quais uma pessoa é reconhecida socialmente. Mesmo sem a exibição de sua aparência física, a reprodução desses elementos pode permitir sua identificação.
- c) Imagem-voz** - Abrange a voz humana registrada ou transmitida por meio de gravações, fonogramas, vídeos, radiodifusão, podcasts e outros recursos de comunicação sonora.

A violação do direito à imagem acontece quando a imagem de uma pessoa é utilizada, divulgada ou compartilhada sem autorização, causando exposição indevida, constrangimento ou prejuízo à sua dignidade.

Essa violação pode ocorrer quando:

- A imagem é utilizada de forma ofensiva, vexatória, humilhante ou degradante.
- Fotografias, vídeos ou gravações são captados, armazenados, reproduzidos, publicados ou compartilhados sem a autorização da pessoa retratada ou de seu responsável legal, quando necessário.
- A imagem é utilizada para fins diferentes daqueles para os quais houve consentimento.

NOTA: O compartilhamento de imagens íntimas de menores de 18 anos é crime hediondo previsto no ECA (Art. 241-A), o que ajuda a conscientizar os **próprios adolescentes sobre a gravidade de "repassar" fotos nos grupos de WhatsApp.**

- O compartilhamento da imagem gera exposição indevida, discriminação, intimidação ou outros danos à pessoa envolvida.



A divulgação não autorizada de imagens, vídeos ou registros contendo nudez, conteúdo sexual ou pornografia, a conduta pode configurar crime, sujeitando o responsável às sanções previstas na legislação brasileira, incluindo o artigo 218-C do Código Penal.

No ambiente escolar, a produção de fotos, vídeos e o registro de informações dos alunos são constantes. É necessário considerar que crianças e adolescentes possuem proteção legal prioritária no Brasil e seus dados e imagem não podem ser tratados como os de um adulto.

A escola é a guardiã dos dados dos alunos (histórico escolar, fichas médicas, fotos de eventos). Cada informação deve ser tratada com máxima segurança e para isso é importante entender os limites legais e as boas práticas para garantir o respeito aos direitos dos estudantes.

- **Autorização Obrigatória e Específica:** Não basta um termo genérico de "uso de imagem" na matrícula. Os pais precisam saber *onde* e *para que* a imagem será usada. Uma foto para o sistema interno da escola requer um cuidado; a postagem nas redes sociais públicas da instituição requer outro, por isso a autorização deve ser específica.
- **Foco no Pedagógico, Não no Comercial:** Ao postar fotos de atividades nas redes sociais da escola, o foco deve ser o projeto educativo, e não a exposição individual do aluno. Evite expor nomes completos associados às fotos.
- **Atenção a exposição da identidade:** Ao publicar imagens de estudantes, certifique-se de que detalhes como o nome do aluno no uniforme ou dados de crachás não estejam legíveis. Isso evita que pessoas mal-intencionadas descubram a rotina da criança.
- **Acesso Restrito a Dados Sensíveis:** Fichas de saúde, laudos psicológicos ou relatórios de desempenho e comportamento são dados sensíveis. Eles devem ser guardados em arquivos trancados ou sistemas digitais com senhas restritas.



PAIS E RESPONSÁVEIS

O cuidado com a imagem dos filhos começa em casa. Muitas vezes, na inocência de compartilhar o orgulho pelo desenvolvimento do filho, os pais criam o que os especialistas chamam de *Sharenting* (exposição excessiva das crianças na internet).

- **O Perigo do "Rastro Digital":** Cada foto postada cria uma identidade digital para a criança antes mesmo que ela tenha idade para decidir sobre sua própria privacidade. Fotos na praia, na hora do banho ou com trajes de natação nunca devem ser públicas.
- **A Rotina Escolar Exposta:** Evite postar fotos do seu filho no primeiro dia de aula onde apareça claramente o logotipo da escola, a fachada do local ou o horário das aulas. Essas informações facilitam a geolocalização por estranhos.
- **Respeito à Imagem dos Colegas:** Ao fotografar seu filho em uma festa de aniversário ou em uma apresentação da escola, lembre-se de que os outros alunos na foto também têm direito à privacidade. **Não publique fotos de filhos de terceiros nas suas redes sociais sem a autorização dos pais deles.**
- **Configurações de Privacidade:** Mantenha suas redes sociais em modo "privado", permitindo que apenas amigos e familiares reais vejam o crescimento dos seus filhos.

O QUE DIZ A LEI?



- **ECA (Art. 17):** Garante o direito ao respeito, que consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem e da identidade.
- **LGPD (Art. 14):** Determina que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu **melhor**

interesse e exige o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

CYBERBULLYING: PREVENÇÃO, IDENTIFICAÇÃO E RESPOSTA

O cyberbullying é a violência psicológica praticada de forma repetitiva no ambiente virtual (redes sociais, aplicativos de mensagens, jogos online). Diferente do bullying tradicional, ele não tem limites geográficos ou de horário: a agressão acompanha a vítima no bolso, através do celular, 24 horas por dia, e tem um poder de replicação devastador. Para combater esse problema, a comunidade escolar deve atuar em três frentes:



1. Prevenção: Construindo a Empatia Digital

Prevenir o *cyberbullying* significa educar crianças e adolescentes para que entendam o impacto de suas ações por trás das telas.

- **Educação Digital e Empatia:** Promover debates na escola e em casa sobre a ilusão de anonimato na internet. O que não temos coragem de dizer olhando nos olhos de alguém, não devemos digitar.
- **Cultura do Respeito:** Ensinar os estudantes a não serem "espectadores passivos". Curtir, comentar com risadas ou repassar um conteúdo humilhante em grupos de WhatsApp faz de quem compartilha um **coautor da agressão**.
- **Criação de Canais de Confiança:** Garantir que os jovens saibam que podem

relatar desconfortos virtuais sem o medo de serem punidos com a perda do celular ou da internet.

A melhor defesa contra a evolução dos riscos não é o monitoramento técnico rigoroso, mas sim o vínculo de confiança, permitindo que o jovem sinta que pode contar o que viu na internet sem medo.

2. Identificação: Como Perceber os Sinais Silenciosos

As vítimas de cyberbullying costumam se isolar por vergonha ou medo de piorar a situação. Pais e professores devem ficar atentos a mudanças repentinas de comportamento:

- **Sinais na Escola:** Queda brusca no rendimento escolar, isolamento na hora do intervalo, faltas frequentes ou desculpas para não ir à aula, além de uma postura defensiva ou triste quando

o assunto é o grupo de amigos.

- **Sinais em Casa:** Ansiedade ou irritabilidade extrema logo após usar o celular ou o computador; o hábito de esconder a tela quando alguém se aproxima; distúrbios de sono (insônia ou pesadelos) e abandono de atividades que antes davam prazer.
- **Sinais Físicos:** Dores de cabeça ou de estômago constantes sem causa médica aparente (sintomas psicossomáticos do estresse emocional).

3. Resposta: O que fazer quando acontece?

Se o cyberbullying foi identificado, a ação deve ser rápida, firme e acolhedora. **Nunca ignore ou trate como "brincadeira de criança".**

O QUE A VÍTIMA E A FAMÍLIA DEVEM FAZER?

1. **Acolha sem Julgar:** O jovem precisa se sentir seguro. Não o culpe pelo ocorrido.
2. **Não Apague Nada:** As mensagens, comentários, áudios e vídeos são **provas**. Tire capturas de tela (*prints*) legíveis, onde apareçam o número de telefone, o link do perfil do agressor, a data e a hora.
3. **Bloqueie o Agressor:** Após coletar as provas, corte o canal de comunicação bloqueando os perfis e denunciando a publicação na própria plataforma.
4. **Preserve juridicamente (se necessário):** Em casos graves, vá a um Cartório para registrar uma *Ata Notarial* dos prints ou utilize ferramentas digitais de auditoria de provas. Registre um Boletim de Ocorrência na Delegacia de Crimes Cibernéticos ou na delegacia mais próxima.

O QUE A ESCOLA DEVE FAZER?

1. **Intervenção Pedagógica:** Acione o protocolo de mediação de conflitos da instituição. Chame os responsáveis dos envolvidos (vítima e agressores) separadamente.
2. **Responsabilização e Apoio:** Aplique as medidas disciplinares previstas no regimento interno para os agressores, promovendo ações

Como agir com responsabilização jurídica?

É necessário registrar provas (prints, links, atas notariais) e acionar os órgãos competentes, como Conselhos Tutelares e Delegacias Especializadas em Crimes Cibernéticos.

de reparação do dano. Ofereça ou encaminhe suporte psicológico para a vítima.

3. **Ação Coletiva:** Trabalhe o tema com a turma inteira de forma reflexiva, sem expor os envolvidos diretamente, reforçando que a comunidade não tolera a violência.



ALERTA LEGAL: CYBERBULLYING É CRIME

Desde janeiro de 2024 (Lei nº 14.811), o **bullying e o cyberbullying foram incluídos no Código Penal**.

- A pena para o cyberbullying (praticado em ambiente virtual) pode chegar a **2 a 4 anos de reclusão**, além de multa.
- Quando praticado por menores de 18 anos, responde-se por **ato infracional equivalente**, aplicando-se medidas socioeducativas aos adolescentes e responsabilização civil (indenizações) aos pais.

O PAPEL DO PROFESSOR NA EDUCAÇÃO PREVENTIVA

Na linha de frente da comunidade escolar, o docente desempenha um papel estratégico na identificação precoce de vulnerabilidades e na mediação de conflitos. Para atuar de forma segura e eficaz, o professor deve adotar uma postura essencialmente preventiva. Este tópico reúne as orientações fundamentais sobre escuta ativa, uso ético das redes sociais, limites profissionais e os fluxos internos de encaminhamento que todo educador deve seguir.

O comportamento preventivo do professor baseia-se em quatro pilares fundamentais:

1. **Escuta Ativa e Observação de Sinais de Alerta** - Os professores são os profissionais que mais passam tempo com os estudantes e, por isso, os principais identificadores de mudanças.

- **Identificação de mudanças de comportamento:**
Orientar o docente a ficar atento a quedas abruptas no rendimento escolar, isolamento social físico, apatia excessiva, agressividade repentina ou sinais físicos (como marcas no corpo ou uso de roupas longas no calor inadequado).

**A escola segura
não é a que
reage melhor
aos conflitos, é
aquela que
constrói cultura
preventiva antes
que eles**

- **Acolhimento sem julgamento:** Quando um aluno trazer um desabafo ou uma denúncia (seja de violência em casa ou de *cyberbullying*), o professor deve ouvir de forma empática, sem interromper, sem minimizar a dor do aluno e sem emitir juízos de valor.
- **Não prometer segredo absoluto:** O professor deve ser acolhedor, mas honesto. Se o aluno disser "vou te contar uma coisa, mas você promete não contar para ninguém?", a resposta preventiva deve ser: *"Eu prometo te proteger e estar ao seu lado, mas se for algo que te coloque em risco, vou precisar pedir ajuda para as pessoas certas cuidarem de você"*.

2. Postura Ética e Fronteiras Profissionais no Ambiente Digital - Com as redes sociais e aplicativos de mensagens, a linha entre a vida pública e privada ficou tênue. O docente precisa agir com cautela para evitar mal-entendidos ou exposição desnecessária.

- **Canais oficiais de comunicação:** O professor deve utilizar estritamente os canais institucionais (e-mail da escola, plataformas oficiais ou números corporativos) para falar com alunos e responsáveis. Evitar conversas privadas e informais em redes sociais pessoais.
- **Horários de atendimento:** Estabelecer e respeitar limites de horário para responder mensagens, educando também os alunos e famílias sobre o direito ao descanso do professor.
- **Preservação da imagem própria e dos alunos:** Nunca publicar fotos ou vídeos de estudantes em suas redes sociais pessoais, mesmo que o momento seja pedagógico ou afetivo. A exposição de menores exige autorização legal e deve ser feita apenas nos perfis oficiais da escola.

Guia de ação rápida para a comunidade escolar

1. Identificou um Risco? Oriente e configure as barreiras de privacidade.

2. Identificou uma Violência? Acolha a vítima, dialogue e aplique as medidas pedagógicas da escola.

3. Identificou um Crime? Não apague as mensagens (elas são provas), tire prints e denuncie às autoridades responsáveis.

3. Gestão Preventiva da Sala de Aula (Física e Virtual) - O professor deve atuar como um mediador da cultura de paz no espaço de aprendizagem.

- **Intervenção imediata diante de conflitos:** Não tolerar "brincadeiras" de cunho discriminatório, piadas depreciativas, exclusão sistemática de colegas ou apelidos humilhantes. O silêncio do docente pode ser interpretado pelo agressor como validação e pela vítima como abandono.
- **Mediação no uso de tecnologias:** Ao propor atividades digitais, monitorar o uso dos dispositivos em sala. Criar combinados claros com a turma sobre o que é permitido e o que viola as regras de convivência naquele espaço.

4. Registro e Fluxo de Encaminhamento - Prevenir também significa documentar para resguardar direitos.

- **Cultura do registro formal:** Orientar o professor a relatar por escrito, de forma factual e objetiva (sem achismos), qualquer situação atípica, relato de vulnerabilidade ou conflito grave presenciado ou recebido.
- **Acionamento imediato da gestão:** O docente não deve tentar resolver problemas de alta complexidade sozinho (como suspeitas de abuso ou crimes virtuais). Seu comportamento preventivo consiste em acolher o estudante e repassar o caso imediatamente para a coordenação ou direção pedagógica, ativando o fluxo institucional.

Roteiro Prático de Conduta para o Professor

- 1. Acolher o Estudante imediato** - Escute o relato do aluno em um espaço reservado, demonstrando empatia e garantindo que ele está seguro em falar. Não faça perguntas indutivas ou interrogatórios.
- 2. Documentar o Fato no mesmo dia.** Escreva um relatório breve, descritivo e confidencial contendo apenas os fatos narrados pelo aluno ou observados por você, com datas e horários, evitando opiniões pessoais.
- 3. Encaminhar à Gestão imediatamente após o registro.** Entregue o relato à coordenação ou direção escolar. O papel de acionar a rede externa (como o Conselho Tutelar) ou convocar os pais é da liderança da instituição.
- 4. Manter Sigilo Absoluto Contínuo:** Não comente o caso com outros colegas de trabalho, alunos ou em ambientes comuns da escola. A privacidade do estudante deve ser integralmente preservada.

O comportamento preventivo do docente não exige que ele seja psicólogo, assistente social ou policial. Exige apenas que ele seja um educador atento, ético e uma ponte segura entre o estudante e a rede de proteção da escola.



RESPONSABILIDADE INSTITUCIONAL: O PAPEL LEGAL DA ESCOLA

A instituição de ensino tem o dever de garantir um ambiente seguro, tanto físico quanto digital. Falar sobre isso significa reforçar que a escola responde legal e pedagogicamente pelas omissões ou falhas na proteção dos alunos.

- **In loco parentis (Guarda e Vigilância):** Enquanto o estudante estiver sob os cuidados da escola (ou em atividades/plataformas coordenadas por ela), a responsabilidade pela sua integridade física e moral é da instituição.
- **Zelo pelo ambiente digital:** Se a escola utiliza ambientes virtuais de aprendizagem, grupos de comunicação ou permite o uso de dispositivos, ela tem a responsabilidade institucional de moderar, criar regras claras de uso e intervir imediatamente em casos de *cyberbullying* ou exposição indevida.
- **Políticas internas conhecidas:** A responsabilidade institucional se materializa em documentos. O Regimento Escolar e o Código de Conduta Digital precisam ser atualizados constantemente e amplamente divulgados para que ninguém alegue desconhecimento.

DEVER DE COMUNICAÇÃO: AÇÃO IMEDIATA E INTEGRADA

O dever de comunicação é a obrigação legal e ética de não silenciar diante de suspeitas ou confirmações de violações de direitos. A escola não deve tentar resolver "portas adentro" o que a lei exige que seja compartilhado.

- **Comunicação Interna (Acolhimento e Registro):** O professor ou funcionário que notar qualquer sinal de alerta (mudança abrupta de comportamento, indícios de automutilação, relatos de abuso ou vazamento de fotos) tem o dever de comunicar imediatamente a coordenação/direção. **Tudo deve ser formalmente registrado em relatórios internos confidenciais.**

Comunicar é acionar a rede necessária para que aquela criança ou adolescente receba o apoio que a escola, sozinha, não tem perna para dar.

- **Comunicação com as Famílias:** Os responsáveis devem ser notificados de forma sensível, ética e sem julgamentos. A escola comunica o fato ocorrido ou a preocupação pedagógica, oferecendo suporte e alinhando as condutas.
- **Comunicação Externa (Rede de Proteção):** Diante de casos graves (como violência doméstica, abuso, exploração ou crimes digitais), o Estatuto da Criança e do Adolescente (ECA) determina que a escola **deve notificar obrigatoriamente os órgãos competentes**, como o **Conselho Tutelar**, o Ministério Público ou a Delegacia de Proteção à Criança e ao Adolescente.

SEGURANÇA JURÍDICA: A ESCOLA E A REDE DE PROTEÇÃO LEGAL

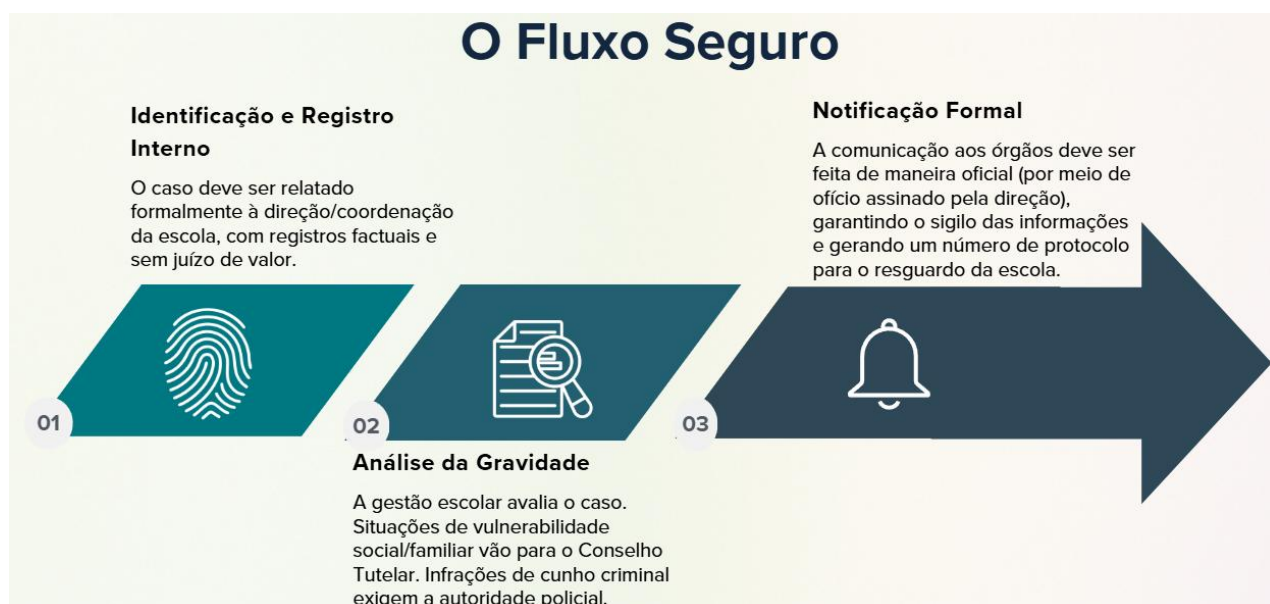
No ambiente escolar, o cuidado com os estudantes vai além do aspecto pedagógico; ele possui um sólido fundamento legal. Conhecer as responsabilidades jurídicas e saber como acionar a rede externa de proteção não é apenas um dever, mas a garantia de que a escola está agindo dentro da legalidade, resguardando a integridade dos alunos e a segurança institucional de seus profissionais.

1. Os Riscos Jurídicos da Omissão (O que a escola precisa evitar)

- **Responsabilidade Civil por Omissão:** Explicar de forma simples que se a escola souber de uma situação de violência (como um caso grave de cyberbullying entre alunos ou sinais de abuso doméstico) e não tomar providências, ela pode responder judicialmente por negligência ou omissão de socorro.
- **Violação de Privacidade (LGPD e Imagem):** Expor o risco jurídico de expor dados de menores de idade, divulgar imagens de conflitos ou expor a identidade de vítimas e agressores sem o devido sigilo.
- **Revitimização:** O risco de submeter o aluno a múltiplos interrogatórios informais dentro da escola, o que pode atrapalhar investigações oficiais e gerar processos por danos morais movidos pelas famílias.

Quem é Quem na Rede de Proteção? (A atuação dos órgãos)		
Órgão de Proteção	Quando a Escola Deve Acionar?	Qual é a Função Dele?
Conselho Tutelar	Em casos de suspeita ou confirmação de maus-tratos, abandono intelectual, evasão escolar crônica ou violação de	Zelar pelo cumprimento dos direitos da criança e do adolescente, aplicando medidas de proteção e

	direitos do menor.	encaminhando para a rede de assistência.
Delegacia de Polícia / DPCA	Diante de fatos que configurem crimes imediatos (como agressão física, ameaças graves, crimes digitais/vazamento de fotos íntimas ou abuso).	Registrar a ocorrência policial, colher provas e iniciar o inquérito para a investigação criminal do fato.
Ministério Público (Promotoria)	Situações graves e sistêmicas onde o Conselho Tutelar não conseguiu resolver ou quando há uma violação ampla de direitos difusos da infância.	Fiscalizar o cumprimento da lei, mover ações civis públicas e defender judicialmente os interesses e direitos dos menores.



A comunicação aos órgãos deve ser feita de maneira oficial (por meio de ofício assinado pela direção), garantindo o sigilo das informações e gerando um número de protocolo para o resguardo da escola.

A escola não tem o papel de investigar, julgar ou produzir provas periciais. Diante do risco ou indício de violação de direitos, o dever legal da instituição encerra-se no acolhimento e no encaminhamento imediato e formal aos órgãos competentes.



JUNTOS POR UMA ESCOLA MAIS SEGURA: CONSIDERAÇÕES FINAIS

A educação preventiva e a proteção integral de nossas crianças e adolescentes não são tarefas simples, nem obrigações que recaem sobre os ombros de um único profissional. Elas se consolidam na rotina, no detalhe de um olhar atento em sala de aula, no cumprimento rigoroso de um fluxo institucional e na coragem de acionar a rede de proteção quando necessário.

Mais do que listar regras e riscos jurídicos, o objetivo desta cartilha é oferecer um mapa de navegação seguro para que a equipe pedagógica e a gestão escolar possam agir com convicção, ética e amparo legal. Conhecer o nosso papel e os limites da nossa atuação nos fortalece.

Quando a escola exerce o seu dever de cuidado e se conecta de forma transparente com as famílias, o Conselho Tutelar e o Ministério Público, nós deixamos de apenas reagir aos problemas e passamos a construir, ativamente, uma cultura de paz, respeito e cidadania.

Contamos com o compromisso e a sensibilidade de cada educador nesta missão. Afinal, proteger o futuro dos nossos estudantes é o papel mais nobre do nosso presente.

CONTATOS ÚTEIS:



Ligue **100**;



Ligue **180** (Central de Atendimento à Mulher);



[Acesse e envie mensagem pelo Telegram](#) para o atendimento **Direitos Humanos Brasil**;



Mantenha [contato com o número \(61\) 99611 0100](#), via **WhatsApp**.



[Disque 100 Web](#)

REFERÊNCIAS:

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto Digital da Criança e do Adolescente. Diário Oficial da União, Brasília, DF, 18 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 19/06/2026.

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 ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente... Brasília, DF: Presidência da República, [2024]. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2024/lei-14811-12-janeiro-2024-795244-publicacaooriginal-170834-pl.html>. Acesso em: 19/06/2026



ECA DIGITAL NA ESCOLA

**SECRETARIA MUNICIPAL DE EDUCAÇÃO
DE ITAETÊ-BA**

