Ofício DIR 012/2026

Curitiba/PR, 14 de junho de 2026

À Autoridade Nacional de Proteção de Dados (ANPD)
GABINETE DA PRESIDÊNCIA DA REPÚBLICA
Conselho Diretor

Esplanada dos Ministérios, Ministério da Economia, Bloco C, 2º andar, Brasília - DF, 70297-400.

Ao Conselho Diretor da Agência Nacional de Proteção de Dados – ANPD A/C Waldemar Gonçalves Ortunho Junior, Diretor-Presidente,

Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos direitos fundamentais de privacidade e proteção de dados, bem como colaborar com o desenvolvimento de políticas públicas relacionadas a proteção de dados pessoais, o INPD vêm, respeitosamente, apresentar suas observações e recomendações quanto à Consulta **Pública** relacionada ao **Guia Orientativo de Fornecedores do Eca Digital**, conforme exposto abaixo.

Atenciosamente,

MARTHA IBANEZ LEAL:47902400025

Assinado de forma digital por MARTHA IBANEZ LEAL:47902400025
Dados: 2026.06.15 11:14:40 -03'00'

Instituto Nacional de Proteção de Dados

MARTHA LEAL

(PRESIDENTE)

Classificação: INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (x)

OFÍCIO DE CONTRIBUIÇÃO INSTITUCIONAL

Contribuições do INPD ao Guia Orientativo de Fornecedores do ECA Digital

Interessado	Instituto Nacional de Proteção de Dados – INPD
Assunto	Contribuições consolidadas à consulta pública do Guia Orientativo de Fornecedores do ECA digital
Origem	Grupo de trabalho e contribuições consolidadas em formulário interno do INPD
Forma de apresentação	Documento único com o apontamento das melhorias e sugestão de redação

Documento consolidado - Questionamentos “i” e “ii” da Tomada de Subsídios (ANPD)

Objetivo. Este documento consolida, em peça única, as contribuições de membros do Instituto Nacional de Proteção de Dados (INPD) à Minuta de Guia Orientativo “Fornecedores de produtos ou serviços de tecnologia da informação: escopo e obrigações gerais do ECA Digital” (SEI 00261.004723/2025-73, doc. 0274640). As contribuições respondem às duas questões centrais do Guia: (i) a quem se aplica o ECA Digital, com foco em soluções SaaS e aplicações equivalentes e no conceito de acesso provável; e (ii) qual o significado e as implicações dos deveres de prevenção, proteção, informação e segurança (art. 5º da Lei nº 15.211/2025). O propósito comum é aperfeiçoar a clareza, a proporcionalidade e a aplicabilidade do Guia, assegurando a proteção integral e prioritária de crianças e adolescentes sem inviabilizar a adequação dos agentes regulados.

Premissas normativas consideradas. Constituição Federal (arts. 5º, II, LIV e LV; 170; 227); Convenção sobre os Direitos da Criança (art. 3.1); Código Civil; Estatuto da Criança e do Adolescente (Lei nº 8.069/1990, arts. 6º, 17, 18, 70 e 100, parágrafo único, II); Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015); Código de Defesa do Consumidor (Lei nº 8.078/1990, arts. 4º, I; 6º, I; 8º; e 37); LGPD (Lei nº 13.709/2018, arts. 6º, VIII e X, e 14); Lei nº 15.211/2025 (ECA Digital, arts. 1º, 4º, 5º, 7º, 8º, 22 e 39); Decreto nº 12.880/2026 (arts. 19, §2º, e 47); a Minuta de Guia Orientativo e o Relatório de Análise de Impacto Regulatório (RAIR) submetidos à consulta.

Nota metodológica. O documento organiza-se em duas partes, correspondentes às questões “i” e “ii”. Cada contribuição indica o ponto principal em que o problema aparece, com identificação do documento, da seção e da página, e mantém a

estrutura de “problema identificado”, “redação sugerida” e “justificativa da proposta”. A autoria é indicada ao final do documento. As contribuições do Bloco C, originalmente apresentadas em formato discursivo, foram convertidas a este mesmo padrão e tiveram suas referências normativas complementadas. As sugestões têm natureza interpretativa e preservam a estrutura legal do ECA Digital.

Quadro executivo consolidado das contribuições

Bloco A - Fornecedores, SaaS e aplicações equivalentes (Questão “i”).

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
1. Inclusão de seção própria para SaaS, aplicações e soluções digitais equivalentes	Guia Orientativo, Sumário e Seção 2 - “Fornecedores de produto ou serviço de tecnologia da informação”, p. 3-6; RAIR, Seção 6, p. 26-27.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
2. Distinção entre SaaS restrito e rede social	Guia Orientativo, Seção “Rede Social”, p. 8-10; Anexo I, p. 32.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
3. Tratamento de soluções SaaS B2B, B2B2C, B2G ou institucionais com usuários finais crianças/adolescentes	Guia Orientativo, Seção 2, p. 4-6; Seção 3 - “Acesso provável”, p. 15-18; RAIR, Seção 5, p. 24-25.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
4. Separação entre acessibilidade/usabilidade e facilidade de acesso por crianças	Guia Orientativo, Seção “Facilidade de acesso e utilização”, p. 19-20; RAIR, Seção 4, p. 21; Lei nº 15.211/2025, art. 4º, VII, p. 2-3.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Média/Alta
5. Critérios para aplicações com múltiplos perfis de usuário	Guia Orientativo, Seção 4 - “Dever de Prevenção”, p. 23-25; Anexo III, p. 35.	Inclusão/ajuste redacional interpretativo para SaaS e	Média/Alta

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
		aplicações equivalentes	
6. Governança de APIs, webhooks, SDKs, conectores e integrações	Guia Orientativo, Seção 2 - produto/serviço de tecnologia da informação, p. 6-8; Seção “Dever de Segurança”, p. 30-31; RAIR, Seção 6, p. 26-32.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
7. Cadeia tecnológica, cloud, suboperadores e transferência internacional	Guia Orientativo, Seção 2, p. 5; Seção “Loja de aplicações”, p. 11; Seção “Sistemas operacionais”, p. 12-13.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
8. Gratuidade, freemium e monetização indireta em SaaS	Guia Orientativo, Seção “Produto ou serviço de tecnologia da informação”, p. 7-8; RAIR, Seção 6, p. 30-31.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
9. Uso de IA em SaaS: distinção entre uso protetivo, funcional e exploratório	Guia Orientativo, Seção “Serviços com controle editorial”, p. 14-15; Seção “Significativo grau de risco”, p. 21-22; RAIR, Seção 4, p. 22-23.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
10. Design persuasivo, gamificação, notificações e uso compulsivo em SaaS	Guia Orientativo, Seção “Probabilidade de uso e atratividade”, p. 18-19; Seção “Significativo grau de risco”, p. 21-22; RAIR, Seção 4, p. 22-23.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
11. Registros, logs e evidências de conformidade sem coleta excessiva	Guia Orientativo, Seção “Dever de Prevenção”, p. 23-25; Seção “Dever de Segurança”, p. 30-31; RAIR, Seção 8, p. 61-69.	Inclusão/ajuste redacional interpretativo para SaaS e	Média/Alta

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
		aplicações equivalentes	
12. Aferição de idade, sinal etário e minimização de dados	Guia Orientativo, Seção “Loja de aplicações”, p. 11; Seção “Sistemas operacionais”, p. 12-13; Lei nº 15.211/2025, Capítulo IV, p. 5.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
13. Compras, assinaturas, upgrades e atos contratuais praticados por menores em SaaS	Guia Orientativo, Seção “Loja de aplicações”, p. 11; Seção “Produto ou serviço de tecnologia da informação”, p. 7-8; Lei nº 15.211/2025, arts. 20-21, p. 7-8.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
14. Transparência material, contextual e acessível em SaaS	Guia Orientativo, Seção “Dever de Informação”, p. 28-29; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
15. Moderação, denúncias e interação em SaaS sem equiparação automática a rede social	Guia Orientativo, Seção “Rede Social”, p. 8-10; Seção “Significativo grau de risco”, p. 21-22; Seção “Dever de Proteção”, p. 26-27.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
16. SaaS que trata dados de crianças/adolescentes sem acesso direto por elas	Guia Orientativo, Seção 3 - “Acesso provável”, p. 15-18; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Alta
17. Definição de papéis LGPD em SaaS: operador, controlador independente,	Guia Orientativo, Seção 2, p. 4-6; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.	Inclusão/ajuste redacional interpretativo para SaaS e	Alta

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
controlador conjunto e suboperador		aplicações equivalentes	
18. Encerramento seguro, exportação, portabilidade, exclusão e revogação de integrações	Guia Orientativo, Seção “Dever de Segurança”, p. 30-31; Seção “Dever de Prevenção”, p. 23-25.	Inclusão/ajuste redacional interpretativo para SaaS e aplicações equivalentes	Média/Alta

Bloco B - Acesso provável: cumulatividade e melhor interesse (Questão “i”).

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
19. Articulação entre a cumulatividade e o princípio do melhor interesse	Guia Orientativo, Seção 3, “Acesso provável”, p. 16-17.	Ajuste interpretativo (clareza e previsibilidade)	Alta
20. Aferição autônoma do requisito de risco	Guia Orientativo, Seção 3, “Acesso provável”, p. 16 e p. 18-22.	Ajuste interpretativo (proteção sem sobreinclusão)	Alta
21. Proporcionalidade do ônus e da avaliação de impacto	Guia Orientativo, Seção 3, p. 17; art. 39 do ECA Digital; art. 47 do Decreto nº 12.880/2026.	Inclusão de critério de proporcionalidade e contraditório	Alta
22. Presunções relativas e valorização das medidas de mitigação	Guia Orientativo, Seção 3, “Acesso provável”, p. 16-17.	Ajuste interpretativo (incentivo à proteção)	Média/Alta

Bloco C - Deveres de prevenção, proteção, informação e segurança (Questão “ii”).

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
23. Continuidade normativa do dever de prevenção (LGPD, CDC e ECA)	Guia Orientativo, Seção 4, “Dever de Prevenção”, p. 23-25.	Ajuste redacional interpretativo (continuidade normativa)	Alta
24. Aproveitamento das obrigações da LGPD sobre dados de crianças (art. 14)	Guia Orientativo, Seção 4, “Dever de Prevenção”, p. 23-25; Seção “Dever de Informação”, p. 28-29.	Ajuste redacional interpretativo (remissão e complementaridade)	Alta
25. Modulação do esforço de prevenção conforme risco e maturidade do agente	Guia Orientativo, Seção 4, “Dever de Prevenção”, p. 23-25; art. 39 do ECA Digital.	Ajuste interpretativo (proporcionalidade)	Média/Alta

Bloco D - Publicidade, perfilamento e parâmetros de auditoria (Questão “ii”).

Tema	Ponto principal do problema	Tipo de ajuste sugerido	Prioridade
26. Parâmetros de auditoria para perfilamento e publicidade direcionada a crianças e adolescentes	Guia Orientativo, Seção “Dever de Proteção”, p. 26-27; art. 22 do ECA Digital; art. 37 do CDC.	Inclusão de subseção (parâmetros de auditoria)	Alta

PARTE I - A quem se aplica o ECA Digital (Questionamento "i")

Bloco A - Fornecedores, SaaS e aplicações equivalentes

1. INCLUSÃO DE SEÇÃO PRÓPRIA PARA SAAS, APLICAÇÕES E SOLUÇÕES DIGITAIS EQUIVALENTES

Ponto principal em que o problema aparece: Guia Orientativo, Sumário e Seção 2 - "Fornecedores de produto ou serviço de tecnologia da informação", p. 4-8; RAIR, Seção 6, p. 26-27.

Problema identificado: O Guia trabalha o conceito geral de fornecedor e depois aprofunda redes sociais, lojas de aplicações, sistemas operacionais e serviços com controle editorial, mas não abre uma subseção específica para aplicações SaaS, plataformas web, APIs, integrações, sistemas educacionais, CRMs, ERPs em nuvem, plataformas corporativas, assistivas ou de IA.

Essa lacuna pode levar fornecedores SaaS a alegar que não se enquadram nas subcategorias tratadas, ou levar agentes regulados a aplicar indevidamente critérios de redes sociais ou lojas de aplicações a qualquer aplicação SaaS.

Redação sugerida. Inserir subseção após "Produto ou serviço de tecnologia da informação":

"Soluções, aplicações e serviços digitais em modelo SaaS ou equivalente compreendem produtos ou serviços de tecnologia da informação fornecidos à distância, por meio eletrônico e mediante requisição individual do usuário, disponibilizados por aplicações web, aplicativos, plataformas em nuvem, APIs, integrações, ambientes de colaboração, sistemas de gestão, ferramentas educacionais, profissionais, corporativas, assistivas, de comunicação, automação ou inteligência artificial.

O enquadramento dessas soluções no ECA Digital não depende da denominação comercial adotada pelo fornecedor, tampouco do modelo de licenciamento, hospedagem, remuneração ou contratação. A análise deverá considerar as funcionalidades efetivamente disponibilizadas, o público alcançado, as condições reais de acesso, o tratamento de dados realizado, a existência de interação entre usuários, a presença de mecanismos de engajamento, recomendação ou personalização, bem como os riscos à privacidade, à segurança e ao desenvolvimento biopsicossocial de crianças e adolescentes.

Soluções SaaS de uso restrito, corporativo, institucional, educacional ou profissional não devem ser automaticamente equiparadas a redes sociais, lojas de aplicações ou sistemas operacionais. Contudo, poderão estar sujeitas às obrigações gerais do ECA Digital quando forem direcionadas a crianças e adolescentes ou de acesso

provável por esse público, observados os critérios legais e a proporcionalidade das medidas exigíveis."

Justificativa da proposta: A proposta concretiza a neutralidade tecnológica já afirmada no Guia, sem criar categoria legal nova. O acréscimo melhora a segurança jurídica para o mercado SaaS e reduz o risco de enquadramentos por analogia inadequada. Também se harmoniza com CDC, Código Civil e ECA, pois preserva a análise funcional da relação de fornecimento, do usuário afetado e da vulnerabilidade concreta.

2. DISTINÇÃO ENTRE SAAS RESTRITO E REDE SOCIAL

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Rede Social", p. 8-10; Anexo I, p. 32.

Problema identificado: O Guia acerta ao afirmar que uma plataforma escolar com fórum incidental não é rede social, mas a redação ainda pode ser insuficiente para plataformas SaaS que possuem chat, fórum, comentários, mural, feed educacional, mensagens, tickets ou colaboração em documentos. A mera existência de interação não deve gerar equiparação automática a rede social.

Redação sugerida. Inserir ao final da Seção "Rede Social":

"A existência de funcionalidades de comunicação, colaboração, comentários, fóruns, chats, murais, canais internos ou compartilhamento limitado de informações em uma solução SaaS, educacional, corporativa, institucional ou profissional não caracteriza, por si só, o serviço como rede social.

O enquadramento como rede social exige que a finalidade principal da aplicação seja a interação social aberta, a conexão entre usuários e a disseminação de conteúdos, opiniões ou informações em larga escala, por meio de contas conectadas ou acessíveis de forma articulada.

Quando as funcionalidades de comunicação forem acessórias, restritas a usuários previamente determinados, vinculadas à finalidade educacional, institucional, profissional, assistiva ou operacional da solução, e não voltadas à circulação aberta ou massiva de conteúdo, o fornecedor não deverá ser enquadrado automaticamente como rede social, sem prejuízo da incidência das obrigações gerais do ECA Digital quando presentes os requisitos de direcionamento ou acesso provável por crianças e adolescentes."

Justificativa da proposta: A redação preserva a proteção do público infantojuvenil, mas evita enquadramento excessivo de ambientes fechados, educacionais, corporativos ou institucionais. Isso reduz insegurança jurídica, evita sobrecarga regulatória e preserva proporcionalidade, sem afastar os deveres gerais quando houver risco real a crianças e adolescentes.

3. TRATAMENTO DE SOLUÇÕES SAAS B2B, B2B2C, B2G OU INSTITUCIONAIS COM USUÁRIOS FINAIS CRIANÇAS/ADOLESCENTES

Ponto principal em que o problema aparece: Guia Orientativo, Seção 2, p. 4-6; Seção 3 - "Acesso provável", p. 15-18; RAIR, Seção 5, p. 24-25.

Problema identificado: O Guia não explicita que, em SaaS contratado por escola, empresa, associação, clínica, órgão público ou outra pessoa jurídica, a análise deve considerar os usuários finais efetivos ou previsíveis, e não apenas o contratante formal.

Isso pode permitir interpretação defensiva de que a solução é B2B e, por isso, fora do escopo protetivo, mesmo quando crianças ou adolescentes são destinatários funcionais do serviço.

Redação sugerida. Inserir na Seção "Acesso provável" ou na nova subseção sobre SaaS:

"Nas soluções SaaS ou equivalentes contratadas por pessoa jurídica, instituição de ensino, entidade pública, organização privada, associação, clínica, plataforma intermediária ou outro agente institucional, a análise de acesso provável deve considerar não apenas o contratante formal do serviço, mas também os usuários finais efetivos ou previsíveis.

O fato de o serviço ser contratado em modelo B2B[1], B2B2C[2], B2G[3], licenciamento institucional ou contratação por intermediário não afasta, por si só, a incidência do ECA Digital quando crianças ou adolescentes forem usuários finais, destinatários funcionais, beneficiários diretos ou pessoas afetadas pelas funcionalidades do produto ou serviço.

Nesses casos, a avaliação deverá considerar o papel do fornecedor na definição das funcionalidades, no desenho da experiência, no tratamento de dados, na gestão de acessos, na comunicação com usuários, na configuração de controles, na segurança do ambiente e na mitigação de riscos."

---

[1] Business to Business: modelo em que uma empresa fornece produto ou serviço para outra empresa. Ex.: uma escola contrata um SaaS de gestão escolar.

[2] Business to Business to Consumer: modelo em que uma empresa contrata outra empresa, mas o serviço chega ao consumidor ou usuário final. Ex.: uma escola contrata uma plataforma educacional usada por alunos e responsáveis.

[3] Business to Government: modelo em que uma empresa fornece produto ou serviço para o governo ou entidade pública. Ex.: uma empresa de tecnologia fornece plataforma SaaS para uma secretaria municipal de educação.

Justificativa da proposta: A proposta elimina lacuna recorrente em SaaS educacional, saúde digital, gestão escolar, plataformas de aprendizagem e soluções contratadas por instituições. Ela reforça a proteção integral e evita que o modelo contratual formal neutralize a avaliação de risco sobre o usuário final vulnerável.

4. SEPARAÇÃO ENTRE ACESSIBILIDADE/USABILIDADE E FACILIDADE DE ACESSO POR CRIANÇAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Facilidade de acesso e utilização", p. 19-21; RAIR, Seção 4, p. 21; Lei nº 15.211/2025, art. 4º, VII.

Problema identificado: A facilidade de acesso é descrita como interface simples, fluxos reduzidos e baixa barreira de uso. Em SaaS, isso pode ser confundido com boas práticas de usabilidade, acessibilidade, desenho universal e compatibilidade com tecnologias assistivas. Essa leitura criaria incentivo indesejado a interfaces menos acessíveis e poderia colidir com o Estatuto da Pessoa com Deficiência.

Redação sugerida. Inserir na Seção "Facilidade de acesso e utilização":

"A facilidade de acesso e utilização não deve ser confundida, isoladamente, com boas práticas de usabilidade, acessibilidade, desenho universal, compatibilidade com tecnologias assistivas ou simplificação legítima da experiência do usuário.

Interfaces claras, intuitivas e acessíveis, inclusive aquelas desenvolvidas para atender pessoas com deficiência, pessoas com baixa alfabetização digital, idosos ou usuários com diferentes níveis de letramento tecnológico, não caracterizam, por si só, acesso provável por crianças e adolescentes.

Para fins de caracterização da facilidade de acesso por crianças e adolescentes, devem ser considerados elementos adicionais, como ausência de barreiras proporcionais de idade, configurações padrão permissivas, acesso irrestrito a funcionalidades sensíveis, linguagem ou recursos especialmente atrativos ao público infantojuvenil, possibilidade de uso autônomo por menores em contexto previsível e inexistência de mecanismos adequados de supervisão, restrição ou proteção."

Justificativa da proposta: A proposta compatibiliza proteção infantojuvenil e inclusão digital. Evita que acessibilidade seja tratada como risco em si e preserva os deveres de desenho universal e não discriminação previstos no Estatuto da Pessoa com Deficiência, sem impedir a análise contextual de acesso provável.

5. CRITÉRIOS PARA APLICAÇÕES COM MÚLTIPLOS PERFIS DE USUÁRIO

Ponto principal em que o problema aparece: Guia Orientativo, Seção 4 - "Dever de Prevenção", p. 23-25; Anexo III, p. 35.

Problema identificado: Soluções SaaS costumam ter perfis distintos: administrador institucional, aluno, responsável, professor, moderador, suporte, operador interno, integrador, conta técnica e usuário convidado. O Guia não explicita que a avaliação de riscos e a distribuição de controles devem variar conforme permissões, capacidades e riscos de cada perfil.

Redação sugerida. Inserir na Seção "Dever de prevenção em sentido estrito":

"Em soluções SaaS ou equivalentes com múltiplos perfis de usuário, o fornecedor deverá considerar, na avaliação de riscos e na implementação das medidas de prevenção, proteção, informação e segurança, as permissões, capacidades e riscos associados a cada perfil.

Devem ser avaliados, no mínimo, os perfis de usuários finais crianças ou adolescentes, responsáveis legais, administradores institucionais, profissionais autorizados, moderadores, operadores internos, equipes de suporte, integradores, usuários convidados e contas técnicas ou automatizadas.

Os controles aplicáveis deverão observar o princípio do menor privilégio, a segregação de funções, a proteção por padrão, a rastreabilidade de acessos relevantes e a limitação de funcionalidades incompatíveis com a idade, a capacidade civil, a finalidade do serviço ou o melhor interesse da criança e do adolescente."

Adicionalmente, a distribuição de controles deve considerar a segregação de ambientes e a arquitetura sistêmica da aplicação, avaliando de forma isolada e independente os diferentes compartimentos ou módulos funcionais (por exemplo, distinguindo um portal institucional ou canal de atendimento comercial de livre acesso de um ambiente logado transacional de alta criticidade), de modo que obrigações regulatórias estritas associadas a uma funcionalidade de alto risco não onerem desproporcionalmente outros módulos/aplicações puramente informativos ou administrativos da mesma solução."

Justificativa da proposta: A proposta torna operacional o dever de prevenção em ambientes SaaS complexos. Também reduz riscos de acesso indevido, escalonamento de privilégios, exposição de dados, atos contratuais inválidos e falhas de supervisão parental ou institucional.

6. GOVERNANÇA DE APIS, WEBHOOKS, SDKS, CONECTORES E INTEGRAÇÕES

Ponto principal em que o problema aparece: Guia Orientativo, Seção 2 - produto/serviço de tecnologia da informação, p. 6-8; Seção "Dever de Segurança", p. 30-31; RAIR, Seção 6, p. 26-32.

Problema identificado: O Guia reconhece aplicações de internet e serviços digitais, mas não trata de forma explícita APIs, webhooks, SDKs, conectores, plugins, analytics, autenticação terceirizada, gateways, integrações e automações.

Em SaaS, a circulação de dados e o risco operacional frequentemente decorrem dessas integrações.

Redação sugerida. Inserir na nova subseção sobre SaaS ou no dever de segurança:

"Quando a solução SaaS ou equivalente disponibilizar ou consumir APIs, webhooks, conectores, SDKs, plugins, ferramentas de analytics, serviços de autenticação, gateways de pagamento, provedores de notificação, automações ou componentes de terceiros, o fornecedor deverá considerar tais elementos na avaliação de riscos e nas medidas de prevenção, proteção, informação e segurança.

As integrações que envolvam dados pessoais, dados de crianças e adolescentes, credenciais, identificadores, logs, sinais de idade, dados de uso, dados comportamentais ou informações de responsáveis legais deverão observar controles proporcionais, incluindo autenticação segura, gestão de chaves, limitação de escopo, registro de eventos relevantes, revogação de acessos, minimização de dados, finalidade determinada e governança sobre terceiros integrados.

O fornecedor deverá informar, de forma clara e acessível, quando integrações relevantes impactarem o tratamento de dados pessoais, a segurança, a experiência do usuário, a supervisão parental ou o compartilhamento de informações com terceiros."

Justificativa da proposta: A redação fecha lacuna relevante em arquiteturas SaaS modernas e reforça segurança por design, accountability, minimização e rastreabilidade. Sem esse ponto, a proteção pode ficar restrita à interface principal, ignorando a cadeia técnica que efetivamente trata dados e influencia riscos.

7. CADEIA TECNOLÓGICA, CLOUD, SUBOPERADORES E TRANSFERÊNCIA INTERNACIONAL

Ponto principal em que o problema aparece: Guia Orientativo, Seção 2, p. 5; Seção "Loja de aplicações", p. 10/11; Seção "Sistemas operacionais", p. 12-13.

Problema identificado: O Guia afirma que a incidência independe da localização do fornecedor, mas não detalha como soluções SaaS devem tratar provedores de cloud, CDN[4], observabilidade, suporte internacional, IA de terceiros, analytics, mensagens, backups, pagamentos e suboperadores. Isso pode gerar invisibilidade da cadeia tecnológica.

[4] CDN (Content Delivery Network): rede de distribuição de conteúdo, infraestrutura usada para entregar sites, imagens, vídeos, scripts e arquivos de forma mais rápida e segura, com servidores distribuídos em várias localidades. Ex.: Cloudflare, Akamai, AWS CloudFront.

Redação sugerida. Inserir na nova subseção sobre SaaS:

"Em soluções SaaS ou equivalentes, o fornecedor deverá considerar, na sua governança de conformidade, a cadeia tecnológica envolvida na prestação do serviço, incluindo provedores de nuvem, hospedagem, armazenamento, CDN, autenticação, monitoramento, analytics, inteligência artificial, suporte técnico, mensageria, pagamentos, atendimento, processamento de logs, backup, segurança e demais terceiros que possam tratar dados, operar funcionalidades ou influenciar a segurança do produto ou serviço.

A utilização de subcontratados, suboperadores ou componentes tecnológicos de terceiros não afasta os deveres do fornecedor perante o ECA Digital, devendo ser observadas medidas proporcionais de diligência, transparência, segurança, limitação de finalidade, minimização de dados, retenção adequada e responsabilização compatível com o grau de controle e influência de cada agente na cadeia.

Quando houver tratamento de dados pessoais fora do Brasil, acesso remoto internacional, suporte global, replicação, backup ou armazenamento em infraestrutura localizada no exterior, o fornecedor deverá avaliar e documentar os impactos jurídicos e técnicos correspondentes, inclusive sob a perspectiva da proteção de crianças e adolescentes."

Justificativa da proposta: A proposta alinha o Guia à realidade operacional de SaaS e à LGPD, especialmente quanto a operadores, suboperadores e transferências internacionais. Também preserva a lógica de responsabilidade proporcional na cadeia tecnológica, sem transferir integralmente o risco ao usuário final ou ao contratante institucional.

8. GRATUIDADE, FREEMIUM E MONETIZAÇÃO INDIRETA EM SAAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Produto ou serviço de tecnologia da informação", p. 7-8; RAIR, Seção 6, p. 30-31.

Problema identificado: O Guia corretamente afirma que a ausência de pagamento direto não afasta a incidência do ECA Digital, mas convém evitar interpretação de que todo SaaS gratuito implica exploração comercial de dados ou atenção. Há serviços gratuitos institucionais, educacionais, assistivos, cívicos ou comunitários que não adotam publicidade, perfilamento ou monetização comportamental.

Redação sugerida. Inserir após o trecho sobre ausência de pagamento direto:

"A ausência de pagamento direto pelo usuário não afasta, por si só, a incidência do ECA Digital, especialmente quando o serviço for sustentado por publicidade, monetização de dados, perfilamento, venda de funcionalidades, compras internas, subsídios cruzados, exploração de atenção ou outros mecanismos de remuneração direta ou indireta.

Todavia, a gratuidade do serviço não deve ser interpretada, isoladamente, como indício de exploração comercial, perfilamento ou risco significativo. A análise deverá considerar o modelo de negócio concreto, a natureza dos dados tratados, as finalidades de uso, a existência de publicidade, compras internas, monetização por engajamento, compartilhamento com terceiros, uso para treinamento de modelos, analytics comercial ou outras formas de obtenção de vantagem econômica.

Serviços gratuitos de natureza institucional, educacional, assistiva, pública, cívica ou comunitária deverão ser avaliados conforme suas funcionalidades, riscos, alcance, público efetivo e práticas de tratamento de dados, observada a proporcionalidade."

Justificativa da proposta: A redação mantém a interpretação ampliativa compatível com o CDC, mas impede presunções absolutas. Isso evita onerar projetos de baixo risco e concentra a análise nos elementos realmente relevantes: dados, publicidade, compras, engajamento, perfilamento e impacto sobre crianças e adolescentes.

9. USO DE IA EM SAAS: DISTINÇÃO ENTRE USO PROTETIVO, FUNCIONAL E EXPLORATÓRIO

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Serviços com controle editorial", p. 14-15; Seção "Significativo grau de risco", p. 21-22; RAIR, Seção 4, p. 22-23.

Problema identificado: O Guia menciona IA em exemplo de controle editorial, mas não estabelece parâmetros gerais para IA em SaaS. IA pode ser usada em chatbots, recomendação, moderação, triagem, avaliação educacional, transcrição, tradução, sumarização, classificação de risco, detecção de fraude, suporte, agentes automatizados e análise comportamental.

Sem distinções, usos protetivos podem ser confundidos com perfilamento comercial, ou usos exploratórios podem ser apresentados como meramente funcionais.

Redação sugerida. Inserir subseção específica sobre IA em soluções digitais:

"O uso de sistemas de inteligência artificial, modelos generativos, sistemas de recomendação, personalização, classificação, moderação, análise comportamental, análise emocional, chatbots, agentes automatizados ou funcionalidades equivalentes em soluções SaaS deverá ser avaliado conforme sua finalidade, grau de autonomia, dados utilizados, impacto sobre crianças e adolescentes, possibilidade de erro, viés, indução comportamental, exposição a conteúdo inadequado e existência de supervisão humana proporcional ao risco.

O uso de IA para finalidades protetivas, como detecção de abuso, classificação etária, prevenção de fraude, moderação de conteúdo, identificação de padrões de assédio ou reforço de segurança, não deve ser confundido com perfilamento

comercial ou exploração comportamental, desde que observados os princípios da necessidade, proporcionalidade, transparência, segurança, revisão adequada e limitação de finalidade.

O uso de dados de crianças e adolescentes para treinamento, ajuste, avaliação, melhoria genérica de modelos ou desenvolvimento de produtos deverá ser objeto de avaliação específica de conformidade, com vedação de usos incompatíveis com o melhor interesse da criança e do adolescente, especialmente quando envolver dados sensíveis, interações privadas, imagem, voz, geolocalização, dados comportamentais ou conteúdo gerado por usuários menores de idade."

Justificativa da proposta: A proposta reduz ambiguidade em um dos pontos mais sensíveis do mercado. A distinção entre IA protetiva e IA exploratória é necessária para preservar segurança, privacidade, inovação responsável e proteção contra manipulação, discriminação, recomendação nociva ou uso secundário incompatível.

10. DESIGN PERSUASIVO, GAMIFICAÇÃO, NOTIFICAÇÕES E USO COMPULSIVO EM SAAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Probabilidade de uso e atratividade", p. 18-19; Seção "Significativo grau de risco", p. 21-22; RAIR, Seção 4, p. 22-23.

Problema identificado: O Guia menciona gamificação, recompensas, rankings, personalização, notificações e mecanismos de engajamento, mas poderia diferenciar uso legítimo em edtechs, saúde, acessibilidade ou produtividade de mecanismos desenhados para maximizar permanência, consumo, publicidade, compras ou exposição ao risco.

Redação sugerida. Inserir na Seção "Probabilidade de uso e atratividade" ou "Significativo grau de risco":

"Em soluções SaaS ou equivalentes, funcionalidades de engajamento, gamificação, notificações, recompensas, rankings, pontuação, sequências de uso, reprodução automática, rolagem contínua, recomendações personalizadas, desafios, convites, mensagens automatizadas ou estímulos de retorno deverão ser avaliadas conforme sua finalidade, intensidade, público afetado, possibilidade de desativação, impacto sobre tempo de uso, autonomia do usuário, supervisão parental e risco de indução a comportamento compulsivo.

Funcionalidades desenhadas para apoiar aprendizagem, acessibilidade, continuidade de tratamento, segurança, organização de tarefas, orientação pedagógica ou uso funcional do serviço não devem ser presumidas como nocivas. Contudo, quando tais mecanismos forem utilizados para maximizar permanência, consumo, compras, exposição publicitária, compartilhamento de dados ou interações de risco por crianças e adolescentes, deverão ser adotadas medidas proporcionais de limitação, transparência, controle, supervisão e proteção por padrão."

Justificativa da proposta: A redação evita tanto a demonização de toda gamificação quanto a normalização de arquitetura persuasiva prejudicial. Em termos de CDC e ECA, preserva a proteção contra exploração comercial e práticas abusivas, mas admite finalidades pedagógicas, assistivas, terapêuticas ou funcionais legítimas.

11. REGISTROS, LOGS E EVIDÊNCIAS DE CONFORMIDADE SEM COLETA EXCESSIVA

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Dever de Prevenção", p. 23-25; Seção "Dever de Segurança", p. 30-31; RAIR, Seção 8, p. 61-69.

Problema identificado: O Guia fala em capacidade demonstrável de proteção, gestão de riscos e medidas técnicas, organizacionais e de governança, mas não explicita exemplos de evidências adequadas para SaaS. Sem isso, a conformidade pode se tornar meramente declaratória ou, no extremo oposto, induzir coleta excessiva de dados para provar conformidade.

Redação sugerida. Inserir no dever de prevenção ou segurança:

"Para demonstrar o cumprimento dos deveres de prevenção, proteção, informação e segurança, fornecedores de soluções SaaS ou equivalentes deverão manter evidências proporcionais ao risco do serviço, tais como registros de avaliação de risco, decisões de configuração padrão, critérios de controle parental, políticas de retenção e exclusão, registros de alterações relevantes, logs de acesso administrativo, registros de incidentes, evidências de testes, documentação de integrações, critérios de moderação, registros de revisão humana quando aplicável e documentação de medidas adotadas para mitigação de riscos.

A exigência de registros e evidências deverá observar a minimização de dados, a segurança da informação, o sigilo, a proporcionalidade e a finalidade de prestação de contas, não podendo justificar coleta excessiva ou retenção indefinida de dados de crianças e adolescentes."

Justificativa da proposta: A proposta transforma accountability em prática auditável, mas impede que a prestação de contas gere vigilância desproporcional. É especialmente relevante para LGPD, CDC e responsabilidade civil, pois permite evidenciar diligência sem ampliar indevidamente o risco ao titular vulnerável.

12. AFERIÇÃO DE IDADE, SINAL ETÁRIO E MINIMIZAÇÃO DE DADOS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Loja de aplicações", p. 10/11; Seção "Sistemas operacionais", p. 12-13; Lei nº 15.211/2025, Capítulo IV.

Problema identificado: O Guia menciona aferição de idade e sinal de idade principalmente para lojas de aplicações e sistemas operacionais, mas em SaaS a

aferição etária pode induzir coleta excessiva de documento, biometria, imagem, dados sensíveis, dados de responsáveis e identificadores desnecessários.

Redação sugerida. Inserir em seção sobre aferição de idade ou SaaS:

"Em soluções SaaS ou equivalentes, mecanismos de aferição de idade, sinalização etária, vinculação a responsável legal ou supervisão parental deverão ser proporcionais ao risco do serviço, à natureza das funcionalidades, ao público efetivo ou previsível, aos dados tratados e ao potencial impacto sobre crianças e adolescentes.

Sempre que possível, o fornecedor deverá priorizar métodos menos intrusivos, sinais etários, faixas etárias, configurações por perfil, validações contextuais ou mecanismos intermediados por responsáveis, evitando coleta excessiva de documentos, biometria, imagem, dados sensíveis ou identificadores desnecessários.

Dados coletados para aferição de idade ou supervisão parental deverão ser utilizados apenas para finalidades compatíveis com a proteção de crianças e adolescentes, com retenção limitada, segurança reforçada, transparência adequada e vedação de uso para publicidade, perfilamento comercial, treinamento de modelos ou finalidades incompatíveis."

Justificativa da proposta: A proposta equilibra proteção e minimização. Ela evita que um mecanismo protetivo gere base de dados sensível desnecessária, com risco de vazamento, discriminação, uso secundário ou vigilância. Também reforça a compatibilidade com LGPD e com a proteção integral.

13. COMPRAS, ASSINATURAS, UPGRADES E ATOS CONTRATUAIS PRATICADOS POR MENORES EM SAAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Loja de aplicações", p. 10/11; Seção "Produto ou serviço de tecnologia da informação", p. 7-8; Lei nº 15.211/2025, arts. 20-21.

Problema identificado: O Guia trata de operações financeiras em lojas de aplicações, mas SaaS também pode envolver assinatura, upgrade, créditos, compra de recursos, marketplace interno, microtransações, contratação de aulas/serviços, doações e funcionalidades pagas. O risco não se limita a lojas de aplicações.

Redação sugerida. Inserir na nova seção de SaaS ou após o trecho sobre operações contratuais/financeiras:

"Soluções SaaS ou equivalentes que permitam contratação, assinatura, upgrade de plano, compra de créditos, aquisição de recursos, transações internas, contratação de serviços, compras in-app, doações, marketplace interno ou qualquer operação com impacto patrimonial deverão implementar barreiras proporcionais para impedir que crianças e adolescentes realizem atos contratuais ou financeiros incompatíveis

com sua idade, capacidade civil ou ausência de representação ou assistência adequada.

As informações sobre preço, cobrança recorrente, renovação automática, cancelamento, reembolso, compras adicionais, funcionalidades pagas e consequências da contratação deverão ser apresentadas de forma clara, acessível e adequada aos responsáveis legais e, quando cabível, aos próprios adolescentes, observada sua autonomia progressiva."

Justificativa da proposta: A proposta integra Código Civil, CDC e ECA Digital. Evita que cliques, aceites e microtransações sejam tratados como atos plenamente válidos sem considerar capacidade civil, representação, assistência, hiper vulnerabilidade e transparência de consumo.

14. TRANSPARÊNCIA MATERIAL, CONTEXTUAL E ACESSÍVEL EM SAAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Dever de Informação", p. 28-29; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.

Problema identificado: O Guia reforça o dever de informação, mas em SaaS as informações costumam ficar dispersas em Termos de Uso, Política de Privacidade, contrato B2B, DPA, central de ajuda, painel administrativo e notificações internas. Isso pode ser formalmente suficiente, mas materialmente inútil para crianças, adolescentes, responsáveis e usuários com deficiência.

Redação sugerida. Inserir na Seção "Dever de Informação":

"Em soluções SaaS ou equivalentes, o dever de informação deverá ser cumprido por meio de comunicação clara, acessível, contextual e adequada aos diferentes públicos envolvidos, incluindo usuários crianças ou adolescentes, responsáveis legais, contratantes institucionais, administradores da plataforma e profissionais autorizados.

Informações essenciais sobre tratamento de dados, perfis de usuário, configurações de privacidade, supervisão parental, riscos, interações, uso de IA, publicidade, compras, compartilhamento com terceiros, incidentes, canais de denúncia, critérios de moderação e direitos dos usuários não devem ficar restritas a documentos extensos, genéricos ou de difícil compreensão.

Sempre que compatível com a natureza do serviço, o fornecedor deverá adotar avisos em camadas, linguagem simples, recursos visuais, elementos audiovisuais, formatos acessíveis, informações contextuais no momento da ação e painéis de controle que permitam compreensão e gestão efetiva das escolhas relevantes."

Justificativa da proposta: A redação concretiza transparência substancial, compatível com CDC, LGPD, ECA e Estatuto da Pessoa com Deficiência. Evita que a informação seja apenas defensiva e reforça compreensão por responsáveis e titulares, inclusive em ambientes institucionais.

15. MODERAÇÃO, DENÚNCIAS E INTERAÇÃO EM SAAS SEM EQUIPARAÇÃO AUTOMÁTICA A REDE SOCIAL

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Rede Social", p. 8-11; Seção "Significativo grau de risco", p. 21-22; Seção "Dever de Proteção", p. 26-27.

Problema identificado: SaaS pode conter chat, fóruns, comentários, upload de arquivos, colaboração em tempo real ou mensagens privadas sem ser rede social. O Guia poderia esclarecer quando tais funcionalidades exigem mecanismos proporcionais de denúncia, moderação, bloqueio, limitação de contato e preservação de evidências.

Redação sugerida. Inserir na seção de SaaS ou no dever de proteção:

"Soluções SaaS ou equivalentes que disponibilizem funcionalidades de interação entre usuários, publicação de conteúdo, comentários, fóruns, chats, mensagens privadas, upload de arquivos, comunidades, salas virtuais ou colaboração em tempo real deverão avaliar a necessidade de mecanismos proporcionais de denúncia, moderação, bloqueio, limitação de contato, preservação de evidências, resposta a abuso e proteção contrarretaliação.

A intensidade desses mecanismos deverá considerar o grau de abertura da interação, a presença de crianças e adolescentes, a possibilidade de contato com adultos, o alcance do conteúdo, a existência de comunicação privada, a escala da plataforma, a finalidade do serviço e o risco de assédio, aliciamento, intimidação, exposição indevida ou outras formas de violação de direitos.

Quando forem adotadas medidas automatizadas de moderação, o fornecedor deverá assegurar critérios documentados, possibilidade de revisão proporcional ao impacto da decisão, transparência adequada e preservação de registros necessários à apuração de abusos."

Justificativa da proposta: A proposta evita aplicar o regime de rede social a todo SaaS, mas impede omissão em plataformas interativas. A solução é proporcional e baseada em risco, compatível com proteção integral, dever de segurança, dever de informação e responsabilidade civil por falhas previsíveis.

16. SAAS QUE TRATA DADOS DE CRIANÇAS/ADOLESCENTES SEM ACESSO DIRETO POR ELAS

Ponto principal em que o problema aparece: Guia Orientativo, Seção 3 - "Acesso provável", p. 15-18; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.

Problema identificado: O Guia é centrado no acesso provável ao produto ou serviço, mas algumas aplicações SaaS tratam dados de crianças/adolescentes sem que eles acessem diretamente a interface: gestão escolar, prontuário, transporte escolar, avaliação, controle de presença, CRM educacional, benefícios, segurança, atendimento ou backoffice institucional.

Redação sugerida. Inserir na seção de SaaS ou em nota na Seção "Acesso provável":

"Soluções SaaS ou equivalentes que não sejam acessadas diretamente por crianças ou adolescentes, mas que tratem seus dados pessoais, imagem, voz, registros educacionais, dados de saúde, localização, comportamento, desempenho, presença, comunicação, perfil, documentos ou outras informações relacionadas a esse público, deverão observar medidas proporcionais de privacidade, segurança, prevenção e proteção, ainda que a análise de acesso provável não se configure nos mesmos termos de serviços utilizados diretamente pelo público infantojuvenil.

Nesses casos, a avaliação deverá considerar os riscos decorrentes do tratamento de dados, da finalidade do sistema, dos acessos concedidos, da cadeia de operadores, da retenção, do compartilhamento, da segurança, da transparência ao controlador ou contratante institucional e dos impactos potenciais aos direitos de crianças e adolescentes."

Justificativa da proposta: A proteção de crianças e adolescentes não depende apenas do uso direto da interface. A proposta preserva a centralidade dos direitos do titular vulnerável e evita lacuna em sistemas de backoffice que podem gerar danos relevantes por vazamento, uso indevido, perfilamento, retenção excessiva ou compartilhamento irregular.

17. DEFINIÇÃO DE PAPÉIS LGPD EM SAAS: OPERADOR, CONTROLADOR INDEPENDENTE, CONTROLADOR CONJUNTO E SUBOPERADOR

Ponto principal em que o problema aparece: Guia Orientativo, Seção 2, p. 4-6; RAIR, Seção 3 - Tratamento de dados pessoais, p. 12-13.

Problema identificado: O Guia analisa fornecedores como sujeitos obrigados pelo ECA Digital, mas não explicita que, em SaaS, o mesmo fornecedor pode exercer papéis diferentes em operações distintas: operador do contratante, controlador independente para conta/segurança/billing, controlador para melhoria do produto, suboperador ou controlador conjunto. A falta dessa distinção pode gerar alocação incorreta de responsabilidades.

Redação sugerida. Inserir na seção sobre SaaS:

"A qualificação do fornecedor como sujeito obrigado pelo ECA Digital não elimina a necessidade de identificar, para fins de proteção de dados pessoais, os papéis desempenhados no tratamento de dados, inclusive como controlador, operador, controlador conjunto, controlador independente ou suboperador, conforme as finalidades, decisões e instruções aplicáveis a cada operação.

Em soluções SaaS ou equivalentes, o fornecedor poderá desempenhar papéis distintos em relação a diferentes tratamentos, como prestação do serviço ao contratante, gestão de conta, segurança, suporte, cobrança, prevenção a fraudes,

melhoria do produto, analytics, treinamento de modelos, comunicação com usuários ou cumprimento de obrigações legais.

A definição desses papéis deverá ser compatível com a realidade operacional, documentada nos instrumentos contratuais e considerada na distribuição de responsabilidades, no atendimento a direitos dos titulares, na comunicação de incidentes, na transparência e na prestação de contas."

Justificativa da proposta: A proposta evita que rótulos contratuais simplifiquem indevidamente a realidade do tratamento de dados. Isso é essencial para LGPD, resposta a incidentes, direitos dos titulares, suboperação, transferência internacional e governança contratual.

18. ENCERRAMENTO SEGURO, EXPORTAÇÃO, PORTABILIDADE, EXCLUSÃO E REVOGAÇÃO DE INTEGRAÇÕES

Ponto principal em que o problema aparece: Guia Orientativo, Seção "Dever de Segurança", p. 30-31; Seção "Dever de Prevenção", p. 23-25.

Problema identificado: O Guia aborda segurança e prevenção, mas não especifica procedimentos de encerramento em SaaS. Ao término do contrato ou da conta, podem permanecer dados em backups, logs, ambientes de suporte, integrações, tokens, contas órfãs, APIs e ambientes temporários.

Redação sugerida. Inserir na Seção "Dever de Segurança":

"Fornecedores de soluções SaaS ou equivalentes deverão prever procedimentos proporcionais para encerramento seguro da relação, incluindo exportação ou devolução de dados, exclusão ou anonimização quando aplicável, revogação de acessos, encerramento de contas, invalidação de tokens, desativação de integrações, limitação de retenção em backups, tratamento de logs, eliminação de ambientes temporários e confirmação das medidas adotadas ao contratante ou responsável competente.

A retenção posterior ao encerramento deverá ser limitada ao necessário para cumprimento de obrigação legal, exercício regular de direitos, segurança, prevenção a fraudes ou finalidade legítima documentada, observados minimização, segurança, segregação e prazo compatível."

Justificativa da proposta: A proposta completa o ciclo de vida da conformidade. Em SaaS, a proteção não termina com o encerramento comercial. A ausência de controles de saída pode gerar vazamento, retenção excessiva, acesso indevido, cobranças indevidas e falhas de portabilidade ou exclusão.

Bloco B - Acesso provável: cumulatividade e melhor interesse

19. ARTICULAÇÃO ENTRE A CUMULATIVIDADE E O PRINCÍPIO DO MELHOR INTERESSE

Ponto principal em que o problema aparece: Guia Orientativo, Seção 3, "Acesso provável por crianças e adolescentes", p. 16-17.

Problema identificado: O Guia afirma a necessidade de presença concomitante dos três requisitos do art. 1º, parágrafo único, e, em seguida, ressalva que essa leitura não pode restringir injustificadamente o âmbito de incidência, devendo ser aplicada em consonância com o princípio do melhor interesse (art. 5º, §2º). Ambos os comandos são legítimos e voltados à proteção de crianças e adolescentes. Postos lado a lado sem critério expresso de articulação, contudo, podem gerar dúvida quanto ao enquadramento e dificultar o planejamento das medidas protetivas pelo agente regulado. A definição clara da relação entre a regra da cumulatividade e o princípio do melhor interesse favorece tanto a proteção efetiva quanto a segurança jurídica.

Redação sugerida. Complementar o parágrafo de ressalva (p. 16), de modo a explicitar a relação entre os comandos:

Os três requisitos do art. 1º, parágrafo único, são cumulativos e devem estar concretamente presentes para a caracterização do acesso provável. O princípio do melhor interesse da criança e do adolescente orienta a interpretação e a valoração de cada requisito, em especial o padrão de aferição do significativo grau de risco, e deve prevalecer sempre que a análise contextual indicar a presença dos três requisitos.

Essa articulação assegura a proteção integral e, ao mesmo tempo, confere previsibilidade ao agente regulado quanto ao seu enquadramento e às medidas de proteção que deve adotar.

Justificativa da proposta: A redação preserva a proteção orientada pelo melhor interesse e, simultaneamente, oferece ao agente regulado a clareza necessária para identificar suas obrigações e implementá-las adequadamente. A previsibilidade do enquadramento estimula a adoção tempestiva de salvaguardas, em benefício direto de crianças e adolescentes. Harmoniza-se com a regra interpretativa do art. 100, parágrafo único, II, do ECA[5], e com o art. 6º do mesmo Estatuto, que

[5] Art. 100, parágrafo único, II, do ECA: as normas de proteção devem ser interpretadas e aplicadas tendo em vista a proteção integral e prioritária dos direitos de crianças e adolescentes, regra reforçada pelo art. 6º do mesmo Estatuto e pelo art. 227 da Constituição Federal.

determinam a interpretação orientada à proteção integral e à condição peculiar de pessoa em desenvolvimento.

20. AFERIÇÃO AUTÔNOMA DO REQUISITO DE RISCO

Ponto principal em que o problema aparece: Guia Orientativo, Seção 3, "Acesso provável", p. 16 e p. 18-22.

Problema identificado: A descrição da cumulatividade pode sugerir que a presença dos requisitos de atratividade e de facilidade de acesso seja suficiente, por si só, para caracterizar o significativo grau de risco. Embora atratividade e facilidade de acesso possam, de fato, contribuir para a exposição de crianças e adolescentes, como o próprio Guia reconhece nas páginas 18 a 22, convém que o requisito de risco seja aferido de modo próprio, para que a análise permaneça consistente e previsível. Esse cuidado evita que boas práticas de usabilidade, acessibilidade e desenho universal, inclusive aquelas voltadas a pessoas com deficiência, sejam interpretadas, isoladamente, como indicativas de risco, o que poderia desestimular a sua adoção.

Redação sugerida. Inserir na sequência do parágrafo sobre a presença concomitante dos requisitos (p. 16):

A atratividade e a facilidade de acesso podem constituir elementos relevantes para a avaliação do risco, mas não dispensam a aferição autônoma do significativo grau de risco, que deve considerar a natureza do serviço, os dados tratados, as funcionalidades disponíveis e os efeitos concretos sobre crianças e adolescentes.

Boas práticas de usabilidade, acessibilidade e desenho universal não devem ser interpretadas, isoladamente, como indício de risco significativo.

Justificativa da proposta: A redação preserva a análise integrada dos requisitos e mantém a clareza da aferição, evitando enquadramentos excessivos. Favorece a inclusão digital e a acessibilidade, valores convergentes com o melhor interesse da criança e do adolescente, sem afastar a proteção quando o risco estiver efetivamente presente.

21. PROPORCIONALIDADE DO ÔNUS E DA AVALIAÇÃO DE IMPACTO

Ponto principal em que o problema aparece: Guia Orientativo, Seção 3, "Acesso provável", p. 17; art. 39 do ECA Digital; art. 47 do Decreto nº 12.880/2026.

Problema identificado: O Guia estabelece, com acerto, que a presunção de acesso provável somente pode ser afastada de forma motivada e excepcional e que a autoavaliação do fornecedor não vincula a ANPD. Convém, todavia, esclarecer o modo de distribuição do ônus de demonstração e a proporcionalidade da avaliação de impacto (art. 47), de forma que a exigência seja exequível para agentes de diferentes portes, inclusive pequenas e médias empresas e iniciativas educacionais e assistivas. A previsão de um caminho proporcional e factível para a demonstração

estimula que esses agentes realizem a avaliação de riscos e adotem medidas de proteção, em vez de recorrerem a soluções apenas formais.

Redação sugerida. Inserir após o parágrafo que trata do afastamento da presunção (p. 17):

A aferição do acesso provável e a eventual elaboração da avaliação de impacto (art. 47 do Decreto nº 12.880/2026) devem observar a proporcionalidade e a modulação prevista no art. 39 do ECA Digital, considerados o porte do fornecedor, o número de usuários e o grau de interferência sobre conteúdos e interações.

Ao questionar o enquadramento, a Autoridade indicará os elementos concretos que sustentam a presença dos três requisitos, assegurando-se ao fornecedor o contraditório e via adequada de demonstração, proporcional ao risco identificado.

Justificativa da proposta: A proposta torna o ônus razoável e exequível, em consonância com o devido processo (art. 5º, LIV e LV, da CF) e com a modulação do art. 39[6]. Ao tornar a conformidade factível, especialmente para agentes de menor porte, incentiva a adoção efetiva de medidas de proteção e evita tanto a conformidade meramente formal quanto a coleta excessiva de dados, preservando a minimização exigida pela LGPD.

22. PRESUNÇÕES RELATIVAS E VALORIZAÇÃO DAS MEDIDAS DE MITIGAÇÃO

Ponto principal em que o problema aparece: Guia Orientativo, Seção 3, “Acesso provável”, p. 16-17 (rol de categorias presumidas e condições de afastamento).

Problema identificado: As presunções de acesso provável cumprem relevante função protetiva. Para que mantenham a sua natureza relativa e estimulem a melhoria contínua, é conveniente que o Guia explicite critérios objetivos e um caminho viável para a demonstração de não incidência ou de redução de obrigações quando o agente adotar medidas eficazes de proteção, tais como aferição etária proporcional, segregação de público, restrição de funcionalidades sensíveis e evidências de uso efetivo. O reconhecimento do efeito jurídico dessas medidas reforça o incentivo à sua adoção, em benefício direto de crianças e adolescentes.

Redação sugerida. Inserir após o rol de categorias presumidas (p. 17):

As presunções de acesso provável têm natureza relativa e admitem afastamento ou redução de obrigações mediante demonstração motivada e documentada, considerada a adoção de medidas técnicas e organizacionais eficazes, tais como

---

[6] Art. 39 do ECA Digital: as obrigações devem ser moduladas conforme o grau de interferência do fornecedor sobre os conteúdos, o número de usuários e o porte do fornecedor, e aplicadas de forma proporcional à sua capacidade de influenciar, moderar ou intervir na disponibilização e no alcance dos conteúdos.

mecanismos proporcionais de aferição etária, segregação ou restrição de público, limitação de funcionalidades sensíveis e evidências de uso efetivo.

A adoção de salvaguardas proporcionais deve ser considerada na modulação das obrigações exigíveis (art. 39 do ECA Digital), de modo a incentivar a mitigação de riscos e a preservar a proporcionalidade entre o risco concreto e o ônus de conformidade.

Justificativa da proposta: A redação mantém a presunção como instrumento protetivo e, ao reconhecer efeito jurídico às medidas de mitigação, cria incentivo concreto à adoção de boas práticas de proteção. O resultado é convergente com o melhor interesse de crianças e adolescentes e, ao mesmo tempo, com a previsibilidade e a viabilidade da adequação pelos agentes regulados.

PARTE II - Deveres de prevenção, proteção, informação e segurança (Questionamento "ii")

Bloco C - A prevenção como princípio já incorporado ao ordenamento jurídico

Contribuições originalmente apresentadas em formato discursivo, aqui convertidas ao padrão das demais e com as referências normativas complementadas. A Lei nº 15.211/2025 e o Decreto nº 12.880/2026 visam prevenir riscos e conferir proteção integral a crianças e adolescentes no ambiente digital, diante de sua vulnerabilidade agravada e graduada conforme o estágio de desenvolvimento humano, principalmente por meio do estabelecimento de obrigações gerais e de obrigações específicas a determinados agentes regulados, como a aferição de idade, os mecanismos de supervisão parental e a moderação de conteúdo. Essas obrigações inovam o ordenamento jurídico brasileiro, mas derivam de um princípio já consolidado no texto legal: a prevenção. As contribuições a seguir buscam tornar explícita essa continuidade normativa, de modo a reduzir a insegurança jurídica e o custo de adequação, sem prejuízo da proteção integral.

23. CONTINUIDADE NORMATIVA DO DEVER DE PREVENÇÃO (LGPD, CDC E ECA)

Ponto principal em que o problema aparece: Guia Orientativo, Seção 4, "Dever de Prevenção", p. 23-25.

Problema identificado: O Guia apresenta o dever de prevenção como núcleo do modelo regulatório do ECA Digital, o que é correto, mas não explicita que o princípio da prevenção já integra o ordenamento jurídico brasileiro. A prevenção consta expressamente do art. 6º, inciso VIII, da LGPD, que impõe ao controlador e ao operador conduta proativa para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais. O dever também encontra fundamento no Código de Defesa do Consumidor, especialmente no dever de segurança (art. 8º), e no

Estatuto da Criança e do Adolescente, que estabelece o dever de todos de prevenir a ocorrência de ameaça ou violação a direitos (art. 70). A ausência de menção a essa continuidade pode transmitir a impressão de obrigação inteiramente nova e onerar de forma desnecessária os programas de privacidade já existentes.

Redação sugerida. Inserir, na introdução da Seção 4 (p. 23-25), parágrafo que reconheça a continuidade normativa:

O dever de prevenção previsto no art. 5º do ECA Digital dialoga e se complementa com o princípio da prevenção da Lei Geral de Proteção de Dados Pessoais (art. 6º, VIII), com o dever de segurança do Código de Defesa do Consumidor (art. 8º) e com o dever geral de prevenção do Estatuto da Criança e do Adolescente (art. 70), interpretados à luz da proteção integral e prioritária (art. 100, parágrafo único, II, do ECA).

A adequação ao ECA Digital pode e deve aproveitar as estruturas de governança e os controles já implementados em razão dessas normas, evitando duplicação de esforços e priorizando a complementação proporcional ao risco do produto ou serviço.

Justificativa da proposta: Tornar explícita a continuidade normativa reduz a insegurança jurídica e o receio de obrigações inéditas, favorece a adequação proporcional e valoriza a maturidade dos programas de conformidade à LGPD já existentes. A medida reforça a proteção efetiva, pois agentes que já operam sob a lógica preventiva tendem a internalizar mais rapidamente os deveres do ECA Digital.

24. APROVEITAMENTO DAS OBRIGAÇÕES DA LGPD SOBRE DADOS DE CRIANÇAS E ADOLESCENTES (ART. 14)

Ponto principal em que o problema aparece: Guia Orientativo, Seção 4, “Dever de Prevenção”, p. 23-25; Seção “Dever de Informação”, p. 28-29.

Problema identificado: O Guia trata dos deveres de prevenção e de informação sem remeter, de forma sistematizada, ao art. 14 da LGPD, que já disciplina o tratamento de dados de crianças e adolescentes e impõe obrigações diretamente úteis ao cumprimento do ECA Digital. Desde a entrada em vigor da LGPD, os agentes de tratamento já devem observar, em especial: (i) a vedação de condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações além das estritamente necessárias (§4º), em consonância com a minimização; (ii) a disponibilização de informações sobre os tipos de dados coletados, a forma de utilização e os procedimentos de exercício de direitos, de maneira simples, clara e acessível, com uso de recursos audiovisuais quando adequado e de forma a proporcionar informação aos pais ou responsável legal e adequada ao entendimento da criança (§§ 2º e 6º); e (iii) o emprego de esforços razoáveis para verificar que o consentimento foi efetivamente dado pelo responsável legal, consideradas as tecnologias disponíveis (§5º). A ausência de remissão expressa pode levar à interpretação de que se tratam de obrigações inteiramente novas.

Redação sugerida. Inserir, na Seção "Dever de Informação" e em remissão na Seção 4, parágrafo de articulação com a LGPD:

Os deveres de prevenção e de informação previstos no ECA Digital articulam-se com o art. 14 da LGPD, que já impõe, no tratamento de dados de crianças e adolescentes, a minimização (art. 14, §4º), a informação clara, acessível e adaptada às características do público infantil, inclusive com recursos audiovisuais e comunicação ao responsável legal (art. 14, §§ 2º e 6º), e os esforços razoáveis de verificação do consentimento parental (art. 14, §5º).

Práticas já consolidadas em atenção a esses dispositivos, como avisos de privacidade construídos com técnicas de comunicação acessível (legal design)[7] *e mecanismos de verificação de consentimento parental, atendem parcialmente aos deveres do ECA Digital e devem ser complementadas conforme o risco do produto ou serviço.*

Justificativa da proposta: A remissão expressa ao art. 14 da LGPD confere coerência sistêmica e previsibilidade, evita a percepção de obrigações redundantes e reaproveita controles já existentes. A referência à comunicação acessível concretiza a transparência substancial exigida tanto pela LGPD quanto pelo ECA Digital, beneficiando crianças, adolescentes e seus responsáveis.

25. MODULAÇÃO DO ESFORÇO DE PREVENÇÃO CONFORME O RISCO E A MATURIDADE DO AGENTE

Ponto principal em que o problema aparece: Guia Orientativo, Seção 4, "Dever de Prevenção", p. 23-25; art. 39 do ECA Digital.

Problema identificado: A implementação do princípio da prevenção não deveria implicar peso adicional desproporcional para agentes que já cumprem os deveres correlatos previstos no Código de Defesa do Consumidor e no Estatuto da Criança e do Adolescente. O Código de Defesa do Consumidor já reconhece a vulnerabilidade do consumidor (art. 4º, I), assegura a proteção da vida, saúde e segurança contra riscos (art. 6º, I) e veda produtos e serviços que acarretem riscos à saúde e à segurança, salvo os normais e previsíveis, com dever de informação (art. 8º). O Estatuto da Criança e do Adolescente, por sua vez, assegura o direito ao respeito e à integridade (art. 17), o dever de velar pela dignidade e de colocar a criança a salvo de tratamento vexatório ou constrangedor (art. 18) e o dever de todos de prevenir ameaça ou violação a direitos (art. 70). Convém que o Guia

[7] Exemplos meramente ilustrativos, sem qualquer vinculação: https://www.mercadopago.com.br/c/contamenoridade e https://www.ubisoft.com/legal/privacy/pt-BR. Referem-se a avisos de privacidade construídos com técnicas de comunicação acessível (legal design).

explicite a complementaridade entre essas normas e o ECA Digital e a necessidade de modulação do esforço de adequação conforme o risco e o porte do agente.

Redação sugerida. Inserir, ao final da Seção 4, parágrafo sobre complementaridade e proporcionalidade:

O dever de prevenção do ECA Digital soma-se e harmoniza-se com o Código de Defesa do Consumidor (arts. 4º, I; 6º, I; e 8º) e com o Estatuto da Criança e do Adolescente (arts. 17, 18, 70 e 100, parágrafo único, II), de modo que o esforço de adequação deve observar a modulação prevista no art. 39 do ECA Digital, considerados o porte do fornecedor, o número de usuários, o grau de interferência sobre conteúdos e a maturidade dos programas de conformidade já existentes.

A implementação das medidas preventivas deve ser proporcional ao risco concreto do produto ou serviço, aproveitando controles previamente adotados em razão da legislação consumerista, da proteção da infância e da proteção de dados pessoais.

Justificativa da proposta: A explicitação da complementaridade e da proporcionalidade confere segurança jurídica, evita a duplicação de exigências e reconhece que a prevenção é dever já difundido no ordenamento. A modulação conforme risco e porte torna a adequação viável para agentes de diferentes capacidades, sem reduzir a proteção nos contextos de maior risco, em coerência com a abordagem baseada em risco adotada pelo Guia.

Bloco D - Publicidade, perfilamento e parâmetros de auditoria

Contribuição originalmente apresentada em formato de tabela analítica, aqui convertida ao padrão das demais.

26. PARÂMETROS DE AUDITORIA PARA PERFILAMENTO E PUBLICIDADE DIRECIONADA A CRIANÇAS E ADOLESCENTES

Ponto principal em que o problema aparece: Guia Orientativo, Seção “Dever de Proteção”, p. 26-27 (vedação ao perfilamento para publicidade); art. 22 do ECA Digital; art. 37 do Código de Defesa do Consumidor (publicidade abusiva).

Problema identificado: O ECA Digital veda a utilização de técnicas de perfilamento para o direcionamento de publicidade comercial a crianças e adolescentes, bem como o emprego de análise emocional e de realidade aumentada, estendida ou virtual para esse fim (art. 22), e o ordenamento já coíbe a publicidade abusiva, especialmente aquela que se aproveita da deficiência de julgamento e experiência da criança (art. 37, §2º, do Código de Defesa do Consumidor). O Guia, contudo, ainda não oferece parâmetros de auditoria para práticas de segmentação, recomendação algorítmica de conteúdo e uso de padrões enganosos de interface (dark patterns), o que dificulta a verificação concreta do cumprimento dessas vedações pelos órgãos de fiscalização e pelos próprios fornecedores.

Redação sugerida. Incluir, na Seção “Dever de Proteção”, subseção “Parâmetros de auditoria de publicidade e perfilamento”, prevendo:

A verificação do cumprimento das vedações ao perfilamento e à publicidade direcionada a crianças e adolescentes deve considerar: (a) a identificação de práticas de alto risco, como segmentação baseada em dados comportamentais, recomendação algorítmica de conteúdo publicitário e emprego de padrões enganosos de interface (dark patterns); (b) perguntas de auditoria que permitam avaliar o modelo de negócio e o desenho do produto, e não apenas os termos de uso; e (c) remissão expressa às vedações de publicidade abusiva do Código de Defesa do Consumidor (art. 37) e às normas do Estatuto da Criança e do Adolescente e do ECA Digital.

Justificativa da proposta: A definição de parâmetros de auditoria em matéria de perfilamento e publicidade torna o Guia instrumento central para a tutela do consumidor infantil em ambientes digitais, permitindo que os órgãos de fiscalização avaliem modelos de negócio e o desenho do produto, e não apenas a conformidade formal dos termos de uso. A medida concretiza a proteção contra a exploração comercial (art. 4º do ECA Digital), reforça o regime do Código de Defesa do Consumidor contra a publicidade abusiva e confere efetividade às vedações legais.

RESUMO E RECOMENDAÇÃO

Reconhece-se a relevância técnica, institucional e regulatória da iniciativa da ANPD na elaboração do Guia Orientativo, instrumento essencial para a consolidação de parâmetros interpretativos claros, proporcionais e aplicáveis à proteção integral e prioritária de crianças e adolescentes no ambiente digital. As contribuições reunidas neste documento, embora abranjam aspectos distintos, convergem para uma mesma diretriz: assegurar proteção efetiva por meio de normas claras, proporcionais e exequíveis, capazes de orientar a adequação dos agentes regulados e de reduzir a insegurança jurídica.

Quanto à Questão “i” (a quem se aplica o ECA Digital), recomenda-se: (a) explicitar o tratamento das soluções SaaS e aplicações equivalentes, da cadeia tecnológica, do uso de inteligência artificial, da aferição etária com minimização de dados e dos atos contratuais praticados por menores, conforme o Bloco A; e (b) aperfeiçoar a articulação, nas páginas 16 e 17, entre a cumulatividade dos três requisitos do acesso provável e o princípio do melhor interesse, preservando a aferição autônoma do requisito de risco, a proporcionalidade do ônus e a natureza relativa das presunções, conforme o Bloco B.

Quanto à Questão “ii” (deveres de prevenção, proteção, informação e segurança), recomenda-se reconhecer a continuidade normativa do dever de prevenção em relação à LGPD, ao CDC e ao ECA, aproveitar as obrigações já consolidadas no art. 14 da LGPD e modular o esforço de adequação conforme o risco e a maturidade do agente, conforme o Bloco C; e estabelecer parâmetros de auditoria para o

perfilamento e a publicidade direcionada a crianças e adolescentes, conforme o Bloco D.

Em síntese, os ajustes propostos não alteram a lógica central do Guia. Buscam aprimorar a sua clareza, proporcionalidade e aplicabilidade prática, fortalecer a atuação fiscalizatória e, sobretudo, atender ao melhor interesse, à proteção integral, à acessibilidade e ao desenvolvimento saudável de crianças e adolescentes no ambiente digital.

Martha Leal - Presidente

Atílio Augusto Segantin Braga – Vice-Presidente

Daiane Dantas – Secretária Geral

Giovanna Sesti Lahude - Associada

Adriana Ruggeri Quinelo – Associada

Instituto Nacional de Proteção de Dados, INPD

www.inpd.com.br

Classificação: INTERNA ( ) CONFIDENCIAL ( ) RESTRITO ( ) PÚBLICO (X)