À SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA DO PARANÁ
Comissão do Sandbox Regulatório SESP/PR
Endereço eletrônico: sandbox@sesp.pr.gov.br

CONTRIBUIÇÃO TÉCNICA À AUDIÊNCIA PÚBLICA DO EDITAL Nº 001/2026/SESP

Sandbox Regulatório para Tecnologias Aplicadas à Segurança Pública na Faixa de Fronteira do Paraná

Documento apresentado nos termos dos itens 6 e 7 do Regulamento da Audiência Pública.

IDENTIFICAÇÃO DO(A) INTERESSADO(A)			
Interessada	Fabiana Cebrian	**Contato**	[redacted]
Qualificação	Pesquisadora em direito digital, proteção de dados pessoais e governança de IA. Doutoranda.	**Manifestação**	Acadêmica e pessoal

A presente contribuição é apresentada em caráter pessoal e acadêmico e não representa posição institucional de organizações às quais a interessada esteja vinculada.

Para fins desta contribuição, as remissões a artigos sem indicação de diploma referem-se ao Edital nº 001/2026/SESP. As referências ao Decreto Estadual nº 13.728/2026, à Lei nº 13.709/2018 e aos demais diplomas são identificadas expressamente. A presente contribuição é apresentada por escrito, e a interessada requer sua inscrição para manifestação verbal na sessão da Audiência Pública de 28 de julho de 2026, nos termos do item 6.2 do Regulamento da Audiência Pública.

APRESENTAÇÃO E PREMISSAS

A instituição de ambiente regulatório experimental para tecnologias aplicadas à segurança pública na fronteira é iniciativa relevante para testar soluções em condições controladas, produzir evidências e aperfeiçoar a regulação antes de eventual adoção em escala. A Lei Estadual nº 20.744/2021 e o Decreto Estadual nº 13.728/2026 oferecem base jurídica ao vincularem a autorização temporária a condições, limites, salvaguardas, indicadores, monitoramento e descontinuidade. A minuta avança ao priorizar aplicabilidade resolutiva, mitigação de riscos, soberania tecnológica, residência de dados, transparência algorítmica e supervisão humana. Também merece reconhecimento a vedação do art. 11, inciso II, do Decreto Estadual nº 13.728/2026 à substituição do juízo humano por decisões automatizadas em atividades típicas de segurança pública.

Embora formalmente instituído como ambiente regulatório experimental pela Lei Estadual nº 20.744/2021 e pelo Decreto Estadual nº 13.728/2026, o Sandbox SESP/PR apresenta, segundo a tipologia da Datasphere Initiative, natureza funcional híbrida. Seu desenho combina aprendizagem regulatória, flexibilização temporária, supervisão pública e produção de recomendações normativas com experimentação técnica em ambientes controlados e reais, acesso a dados e infraestruturas públicas, integração de sistemas e validação operacional de tecnologias. Trata-se, portanto, de sandbox híbrido, com predominância regulatória em sua estrutura institucional e componente operacional relevante na fase de execução. Essa qualificação não altera a denominação jurídica do programa, mas evidencia que seu planejamento, monitoramento e avaliação devem contemplar, de forma articulada, tanto o aprendizado regulatório quanto o desempenho e os impactos da experimentação técnica (Datasphere Initiative, 2026, p. 17-18).

Essa natureza híbrida exige que o sandbox não seja avaliado apenas pelo número de soluções selecionadas ou pelo desempenho técnico do piloto. Seus resultados devem compreender tanto conhecimento regulatório confiável, reutilizável e publicamente justificável quanto evidências operacionais sobre eficácia, segurança, interoperabilidade, supervisão humana, integração aos fluxos institucionais e capacidade de descontinuidade das soluções. O Guia Referencial da Advocacia-Geral da União trata o instrumento como metodologia de colaboração e aprendizagem e recomenda transparência e participação ao longo da implementação (AGU, 2024, p. 15 e 24-29). Guio Español e Koenig destacam aprendizagem institucional, redução de assimetrias informacionais e reporte sistemático como critérios de êxito (Guio Español e Koenig, 2025, p. 11-14). A Datasphere Initiative organiza a implementação em iniciação, planejamento, execução, comunicação e engajamento, encerramento e avaliação, com ênfase em transparência, confiança e inclusão (Datasphere Initiative, 2025, p. 6-7). O IFOW, por sua vez, concebe o sandbox como infraestrutura sociotécnica de pesquisa regulatória orientada por independência, análise integral da cadeia tecnológica, interdisciplinaridade, prestação de contas, transparência e participação (Gilbert, Marriott e Leslie, 2026, p. 6-12).

DELIMITAÇÃO DO OBJETO E COERÊNCIA NORMATIVA

O art. 1º, § 1º, deve ser ajustado porque afirma que as condições diferenciadas permitirão desenvolver, testar e aperfeiçoar uma “solução de inteligência artificial”, embora o edital alcance tecnologias aplicadas à segurança pública e o art. 20 inclua sensores, plataformas de comunicação, sensoriamento remoto, sistemas anti-drone e gravimetria. A definição de IA do art. 2º, inciso II, também pode excluir sistemas híbridos ou incluir técnicas que não constituem IA. Sugere-se substituir a referência exclusiva por “solução tecnológica” e adotar definição funcional de sistema de IA apenas quando necessária, preservando o alcance sobre tecnologias não algorítmicas.

Há inconsistências materiais a corrigir. O art. 21 menciona “validação pedagógica”, o art. 32 refere-se a “direitos educacionais” e o art. 35 inclui “adequação pedagógica”, expressões estranhas à segurança pública e aparentemente oriundas de outro modelo normativo. A sequência salta do art. 28 para o art. 30. Além disso, o art. 12, inciso IV, admite “simulação conceitual”, enquanto o art. 6º, inciso IV, veda propostas meramente conceituais. Recomenda-se esclarecer que a apresentação técnica (*pitch*) pode empregar simulação para demonstrar solução já validada por prova de conceito ou protótipo, sem reduzir a maturidade mínima exigida pela Lei Estadual nº 20.744/2021 e pelo Decreto Estadual nº 13.728/2026.

O edital deve explicitar quais normas ou procedimentos poderão ser flexibilizados e quais permanecerão inderrogáveis. O art. 1º, §§ 1º a 4º, trata amplamente de modulações, mas não exige nexo preciso entre flexibilização, experimento, prazo e controles compensatórios. Recomenda-se complementar o art. 6º, inciso VII, e o art. 17 para que o Termo Específico de Admissão (TEA), definido no art. 2º, inciso V, do Decreto Estadual nº 13.728/2026, contenha matriz com fundamento de competência, necessidade, prazo, limite geográfico, volume máximo de dados ou operações, salvaguardas, responsáveis e condição de reversão. A medida concretiza o art. 12 do Decreto, evita dispensa genérica de conformidade e corresponde ao protocolo experimental recomendado pela AGU (AGU, 2024, p. 49-51).

O relatório do IFOW oferece critério metodológico útil ao sustentar que o sandbox deve responder a perguntas regulatórias precisas quando houver incerteza jurídica ou de governança, baixa interoperabilidade ou lacuna que exija evidência empírica. A minuta solicita a indicação das normas cuja flexibilização seria necessária, mas não exige demonstração da adicionalidade regulatória. Recomenda-se complementar o art. 6º e o Anexo IV para exigir a questão sociotécnica, a hipótese de teste, a intervenção normativa ou operacional, as evidências necessárias e a decisão pública que poderá ser informada. A proposta deverá justificar por que a dúvida não pode ser resolvida por prova de conceito, laboratório técnico, contratação experimental ou procedimento administrativo comum, além de mapear os regimes jurídicos e padrões técnicos envolvidos. A Comissão deverá confrontá-la com iniciativas de outros órgãos, evitando duplicação e impedindo que o sandbox funcione apenas como demonstração tecnológica ou via de entrada no mercado (Gilbert, Marriott e Leslie, 2026, p. 6 e 13-16).

SELEÇÃO ORIENTADA A RISCO E RESOLUTIVIDADE OPERACIONAL

A Matriz Avaliativa do Anexo V acerta ao atribuir peso elevado à aplicabilidade resolutiva e à mitigação de riscos éticos e jurídicos. Porém, como não há nota mínima eliminatória, uma proposta pode obter desempenho insuficiente nesses critérios e ainda ser classificada pela soma global. Em segurança pública, solução tecnicamente promissora não deve avançar para testes reais com proteção de dados, segurança cibernética ou supervisão humana inadequadas. Sugere-se nota mínima 3 nos critérios 1, 2 e 3 do Anexo V, relativos à aplicabilidade resolutiva, à mitigação de riscos éticos e jurídicos e ao potencial operacional, além de pontuação global mínima. A nota no critério 2 deverá considerar evidências de conformidade com a LGPD e segurança da informação, enquanto o critério 3 deverá abranger supervisão humana e integração aos fluxos decisórios. Observe-se, ainda, que o Anexo V posiciona a conformidade básica com a LGPD como descritor da Nota 3 do critério 2, tratando como atributo graduável aquilo que constitui pressuposto de legalidade, pois a conformidade não deveria pontuar, mas condicionar a habilitação. Para tecnologias de alto impacto, RIPD inadequado, arquitetura de segurança não verificável ou ausência de mecanismo de interrupção imediata devem impedir a fase de campo.

O critério de inovação tecnológica, capaz de alcançar nota máxima por “inovação disruptiva”, pode privilegiar novidade em detrimento de confiabilidade, interoperabilidade e adequação. Em segurança pública, a superioridade deve ser comprovada. Recomenda-se que a nota máxima exija comparação com a linha de base, maturidade compatível, desempenho reproduzível, robustez e benefício público mensurável. Inovação incremental que reduza falsos positivos, tempo de resposta, custo de integração ou exposição de agentes pode ser mais valiosa do que tecnologia imatura e deve receber tratamento equivalente quando apresentar melhor relação entre benefício e risco.

Os indicadores do Anexo IV e do art. 21 devem ser vinculados a hipóteses de teste. A avaliação deverá abranger precisão, taxas de falso positivo e negativo, disponibilidade, resiliência, recuperação, intervenção humana, revisão de recomendações, carga de trabalho, cadeia de custódia, incidentes, reclamações, custo total e integração. Quando houver risco de tratamento desigual, deverá examinar desempenho por contexto e grupos pertinentes, sem criar bases sensíveis desnecessárias. A comparação deverá utilizar linha de base, modo sombra, simulação ou desenho quase experimental compatível com a atividade policial, evitando submeter a população a testes sem benefício justificável.

PROTEÇÃO DE DADOS PESSOAIS E GOVERNANÇA DE DADOS

A exigência de RIPD preliminar pelo art. 11 do Edital e de RIPD prévio para tecnologias de alto impacto pelo art. 11, inciso III, do Decreto Estadual nº 13.728/2026 constitui salvaguarda essencial. Recomenda-se sua complementação e aprovação antes de qualquer tratamento de dados pessoais em ambiente real, com atualização após mudança relevante de finalidade, dados, modelo, fornecedor, integração, escala ou local. O RIPD deverá indicar finalidade, necessidade, proporcionalidade e a hipótese legal de cada fluxo, na forma do parágrafo seguinte, e abranger titulares, dados, compartilhamentos, retenção, descarte, riscos a direitos fundamentais, medidas de segurança, supervisão humana e riscos residuais, com versão pública resumida (ANPD, 2023).

O Edital pressupõe a aplicação da Lei nº 13.709/2018 em quatro dispositivos: o art. 3º, que a elege entre os princípios de condução do Sandbox; o art. 6º, inciso XI, que exige profissional responsável pela governança e

proteção de dados; o art. 11, que impõe o RIPD; e a Cláusula Quarta do Anexo X, que obriga a participante à observância integral da lei. Em nenhum momento, porém, exige que se declare a hipótese legal de cada tratamento. A omissão é relevante porque a experimentação em ambiente real envolverá imagens, dados biométricos e geolocalização de pessoas que não participam do experimento e não têm como dele se afastar. Recomenda-se que os arts. 11 e 17 e o TEA exijam matriz por fluxo de tratamento, com indicação de finalidade, dados, agentes, ambiente, possibilidade de reutilização e da hipótese legal invocada entre as dos arts. 7º e 11 da LGPD, observadas as orientações da ANPD sobre tratamento de dados pessoais pelo Poder Público (ANPD, 2022b, p. 7-21). Tratando-se de dados biométricos, qualificados como sensíveis, a matriz deverá apontar especificamente a hipótese do art. 11. A matriz deverá ser aprovada pela Comissão antes do primeiro uso de dados pessoais reais e revista a cada alteração de finalidade, dados, modelo, fornecedor, integração, escala ou local, vedada a ampliação de finalidade sem nova aprovação. O acesso da participante a bases da SESP configura transferência a entidade privada, sujeita às restrições do art. 26, § 1º, devendo o instrumento ser comunicado à ANPD na forma do art. 26, § 2º, e do art. 27.

O edital e o TEA devem identificar controlador, operador ou controladores conjuntos em cada tratamento. A qualificação depende de quem define finalidade e elementos essenciais, não da simples presença de empresa participante. A SESP poderá ser controladora ao determinar objetivos, dados, integrações e usos, enquanto a participante poderá atuar como operadora ou controladora em operações próprias (ANPD, 2022a, p. 8-12). Quando atuar como operadora, a participante deverá tratar dados pessoais exclusivamente conforme instruções documentadas da SESP, vedado o tratamento autônomo para finalidade própria. Recomenda-se matriz de responsabilidades sobre atendimento a titulares, registros, instruções, suboperadores, auditoria, incidentes, compartilhamento, descarte e cooperação com a ANPD. A definição também é necessária para corrigir as cláusulas genéricas dos arts. 26 e 27.

A vedação do Anexo X ao uso das informações do sandbox para treinamento de modelos de IA é adequada quanto a reutilizações secundárias, melhoria de modelos gerais e desenvolvimento comercial. Porém, ela entra em tensão com o art. 19, § 3º, que pressupõe modelos e pesos treinados para o piloto. Deve-se distinguir avaliação operacional de treinamento destinado ao desenvolvimento da solução. O uso de dados pessoais reais para desenvolver ou aperfeiçoar modelos deve ser excepcional, juridicamente enquadrado e segregado do fluxo operacional, pois, quando beneficia o produto da participante, configura finalidade diversa daquela que autorizou o acesso aos dados. Devem ser priorizados dados sintéticos, efetivamente anonimizados ou legitimamente tratados. Qualquer ajuste autorizado deverá limitar dados, finalidade, ambiente, prazo e equipe, impedir incorporação a modelos de propósito geral, registrar linhagem e versões e determinar eliminação ou devolução ao final. Dados reais somente deverão ser utilizados quando alternativas menos invasivas forem insuficientes, mediante fundamentação no RIPD e decisão da Comissão.

A anonimização não deve ser tratada como solução automática. O item 5 do Anexo III, cuja execução é determinada pelo art. 24, prevê eliminação ou anonimização, mas dados audiovisuais, biométricos e georreferenciados podem manter risco de reidentificação. Recomenda-se testar a eficácia da anonimização, avaliar vinculação, proibir reversão e exigir certificado de eliminação. Devem existir ambientes segregados, criptografia, gestão de chaves, autenticação forte, privilégio mínimo, registros imutáveis, monitoramento de extração, inventário, testes de vulnerabilidade e resposta a incidentes. O TEA deverá definir quem decide contenção, comunicação à ANPD e aos titulares, preservação de evidências e suspensão do teste.

TRANSPARÊNCIA ALGORÍTMICA, SUPERVISÃO HUMANA E TECNOLOGIAS DE ALTO IMPACTO

A transparência algorítmica do art. 3º e do art. 19, § 4º, deve operar em camadas. Ao público devem ser informados finalidade, local e duração do teste, tipos de dados, fornecedor, riscos, critérios de desempenho, supervisão, incidentes relevantes e resultados agregados. À SESP e aos auditores devem ser acessíveis arquitetura, versões, dados de treinamento e validação, métricas, limitações, dependências, parâmetros, logs, testes adversariais e componentes de terceiros. Ao agente deve ser oferecida explicação compreensível sobre origem do resultado, confiança, limites e necessidade de confirmação. Assim se evita tanto opacidade quanto divulgação que comprometa segurança, segredo industrial ou resistência a ataques.

A rastreabilidade do Anexo IV deve abranger identificação e versão do sistema, data e hora, fonte dos dados, transformações, resultado, confiança, alertas de qualidade, operador, decisão humana, justificativa, ação subsequente e alterações. Os registros devem ser protegidos contra adulteração e conservados pelo período necessário à auditoria, cadeia de custódia e exercício de direitos, com minimização. Para visão computacional, biometria ou análise comportamental, devem ser definidos limiares de confiança, condições ambientais e verificação independente antes de medida restritiva de direitos.

A vedação de substituição do juízo humano deve assegurar supervisão significativa, não confirmação formal. O agente precisa de competência, tempo, informação, autoridade e condições para discordar. O Plano Operacional e de Treinamento do art. 6º, inciso VI, deverá abordar viés de automação, verificação, escalonamento, simulações, proficiência e concordância automática. Em abordagem, busca, apreensão, prisão, investigação individualizada, sanção, restrição de liberdade ou uso da força, a saída tecnológica não deve ser fundamento único ou determinante e deverá haver confirmação independente baseada em elementos juridicamente admissíveis.

O art. 20, inciso VI, merece revisão ao admitir plataformas anti-drone com neutralização autônoma. A atuação física pode causar danos irreversíveis, interferir em comunicações, afetar aeronaves legítimas e envolver competência federal. Recomenda-se limitar a prioridade à detecção, identificação e rastreamento, condicionando

neutralização a autorização humana individualizada, protocolo específico, competência legal, coordenação federal e mecanismo seguro de interrupção. A mesma lógica deve alcançar qualquer sistema que atue sobre o ambiente físico. O sandbox pode testar detecção e apoio decisório, mas não flexibilizar normas superiores sobre uso da força, telecomunicações, aviação, processo penal ou direitos fundamentais.

SOBERANIA TECNOLÓGICA, CÓDIGO ABERTO E RESIDÊNCIA DE DADOS

A soberania tecnológica do art. 3º e da Matriz deve significar capacidade estatal de conhecer, governar, auditar, manter, migrar e interromper a solução, não apenas propriedade do código ou localização do servidor. Residência de dados no Brasil é pertinente para bases críticas, mas não elimina dependência de fornecedor. Devem ser avaliados localização de dados e backups, jurisdição, chaves criptográficas, subcontratados, acesso remoto, nuvem, componentes estrangeiros, atualizações, telemetria, continuidade, portabilidade e plano de saída. Para dados críticos ou sensíveis, o edital pode exigir processamento nacional, controle de chaves pela Administração ou entidade autorizada e vedação de transferência internacional não aprovada.

O art. 19 impõe código aberto, enquanto a Matriz o pontua e o art. 14 o utiliza como desempate. Além da incoerência, a publicação obrigatória de código, modelos, pesos e arquiteturas pode afastar soluções maduras, violar direitos preexistentes e ampliar riscos. Recomenda-se regime graduado com padrões abertos, APIs documentadas, interoperabilidade, portabilidade, exportação de dados e registros, inventário de componentes, acesso auditável aos artefatos necessários, direitos de uso e manutenção e depósito de código-fonte em custódia (*escrow*), quando indispensável. Código desenvolvido com recursos públicos específicos poderá receber licença aberta, desde que escopo, segurança, direitos de terceiros e exceções estejam previamente definidos.

A publicação de modelos e pesos do art. 19, § 3º, deve ser substituída por transparência proporcional. Quando não houver risco à segurança, aos dados, às técnicas operacionais ou à propriedade intelectual, a abertura poderá ser estimulada. Nos demais casos, SESP e auditores independentes deverão receber acesso suficiente para reproduzir testes e verificar conformidade sob confidencialidade. Ficha pública deverá indicar finalidade, versão, dados em termos agregados, métricas, limitações, riscos, supervisão e resultados. A solução equilibra acesso a informações críticas e confidencialidade, como recomendam Guio Español e Koenig (2025, p. 16-18), sem reduzir transparência à publicação indiscriminada de artefatos técnicos.

A visão integral da cadeia tecnológica, referida como *full stack* pelo relatório do IFOW, deve complementar a análise de soberania e transparência. A avaliação não pode limitar-se à proponente, pois a solução pode depender de desenvolvedores de modelos, nuvem, sensores, bases de dados, bibliotecas, telemetria, suporte remoto e subcontratados que condicionam desempenho e auditabilidade. Recomenda-se que o art. 17 e o Anexo IV exijam Relatório de Escolhas de Projeto e Mapa da Cadeia de Valor, com atores, componentes, jurisdições, responsabilidades, dependências críticas e alternativas de substituição. A SESP deverá acessar, sob sigilo proporcional, contratos de licenciamento, acordos de compartilhamento de dados, níveis de serviço e informações de auditoria. No contexto fronteiriço, a análise deverá abranger competências federais, cooperação com Paraguai e Argentina, transferências internacionais e acesso remoto estrangeiro, sem presumir que a residência física do dado no Brasil elimine riscos jurisdicionais ou dependências externas (Gilbert, Marriott e Leslie, 2026, p. 8-10 e 17-19).

GOVERNANÇA INSTITUCIONAL E PARTICIPAÇÃO DA SOCIEDADE CIVIL

A composição mínima da Comissão prevista no art. 4º do Decreto Estadual nº 13.728/2026 é predominantemente governamental e o art. 30 da minuta admite, em caráter consultivo, apenas representantes de órgãos de segurança e universidades. Para reduzir assimetrias de informação, prevenir captura regulatória e incorporar impactos sociais, recomenda-se prever instância consultiva plural, com participação periódica de especialistas independentes em proteção de dados, segurança cibernética, direitos humanos, processo penal e avaliação de tecnologias, além de representantes da sociedade civil e de comunidades da região de fronteira. Essa participação pode ocorrer sem acesso a informações operacionais sigilosas, mediante versões públicas dos documentos, sessões reservadas quando necessárias e termos de confidencialidade proporcionais.

A audiência pública prevista no art. 23 é relevante, mas aparece apenas como evento destinado à transparência de resultados parciais. O Guia da AGU recomenda que a participação social atravesse as fases de definição, implementação e avaliação, com prazo compatível, publicação dos documentos necessários e resposta administrativa às contribuições (AGU, 2024, p. 24-29). A Datasphere Initiative também ressalta que a ausência de sociedade civil e academia enfraquece a confiança e o interesse público (Datasphere Initiative, 2025, p. 7 e 29). Sugere-se instituir ao menos uma consulta antes da autorização dos testes de alto impacto, uma prestação de contas intermediária e uma avaliação pública final, resguardados os sigilos legais. O painel previsto no art. 10, § 2º, do Decreto Estadual nº 13.728/2026 deve ser atualizado durante a execução e conter decisões de admissão, fundamentação dos critérios, flexibilizações concedidas, indicadores, mudanças relevantes, incidentes agregados e síntese das providências adotadas.

A participação social pode ser convertida em metodologia operacional de avaliação sem expor informações sensíveis. O IFOW demonstra que pessoas afetadas ou responsáveis pelo uso cotidiano da tecnologia possuem conhecimento contextual indispensável para revelar impactos não antecipados. Recomenda-se integrar ao RIPD um Relatório de Escolhas de Projeto, com problema, alternativas, objetivos, dados, limites e integração institucional; um Relatório de Mapeamento e Engajamento de Partes Afetadas, com justificativa da amostragem e registro das contribuições; uma Avaliação Ex Ante de Riscos e Impactos; e um Plano de Mitigação com riscos

prioritários, responsáveis, recursos e limiares de suspensão. Durante a execução, fórum próprio deverá revisar impactos e eficácia das medidas. Agentes de linha de frente, operadores dos centros de comando, encarregado, Ouvidoria, especialistas independentes e representantes das comunidades locais poderão participar em formatos diferenciados, com anonimização, agregação ou sessões reservadas. A estrutura evita que impactos sejam previstos exclusivamente pela proponente ou pela Comissão (Gilbert, Marriott e Leslie, 2026, p. 12 e 17-20).

A governança deve incluir política de conflitos de interesses mais ampla do que a declaração prevista no art. 28. Recomenda-se publicar composição, currículos institucionais, impedimentos, atas e votos ou fundamentos, preservadas informações sensíveis. Consultores, avaliadores técnicos e entidades de apoio devem declarar vínculos com proponentes e fornecedores. Apoios financeiros, técnicos ou em espécie, bem como assessorias externas relacionadas ao programa, devem ser divulgados em registro público. A Comissão deve dispor de secretaria técnica multidisciplinar, autoridade para suspender testes, canal protegido para relato de falhas e procedimento de revisão independente. A Ouvidoria mencionada no art. 10, § 4º, do Decreto Estadual nº 13.728/2026 deve oferecer canal acessível à população afetada e encaminhar relatórios agregados à Comissão e ao encarregado pelo tratamento de dados.

EXPERIMENTAÇÃO, MONITORAMENTO E APRENDIZADO REGULATÓRIO

A fase de campo prevista no art. 18 deve ser precedida por progressão de risco. Recomenda-se organizar os testes em ambiente isolado com dados sintéticos, validação com dados históricos protegidos, operação em modo sombra, piloto real limitado e eventual ampliação condicionada. Cada transição deve depender de decisão fundamentada da Comissão com base em desempenho, segurança, proteção de dados e supervisão humana. Antes do uso de dados pessoais reais, a decisão deverá registrar a hipótese legal de cada fluxo. O TEA deve definir limites geográficos, temporais, populacionais, funcionais e de volume, além de gatilhos de suspensão, mecanismo de interrupção imediata (*kill switch*), reversão segura (*rollback*), contingência manual e proibição de expansão de finalidade. Alterações relevantes de modelo, dados, fornecedor ou integração devem ser previamente autorizadas.

O monitoramento não deve se limitar a relatórios apresentados pelo participante. A SESP deve manter capacidade própria ou independente de auditoria, acesso a logs, verificação de métricas, inspeção de versões e realização de testes adversariais. O art. 10, caput e § 1º, do Decreto Estadual nº 13.728/2026 e o art. 21 do Edital devem exigir relatórios periódicos padronizados, com incidentes, intervenções humanas, mudanças, desempenho, riscos materializados, reclamações e medidas corretivas. Guio Español e Koenig mostram que mecanismos sistemáticos de reporte são essenciais para transmitir conhecimento para além dos participantes (Guio Español e Koenig, 2025, p. 16-18). Recomenda-se, portanto, que o relatório final do Anexo VII inclua avaliação das flexibilizações testadas, adequação das salvaguardas, limitações metodológicas, riscos residuais, transferibilidade dos resultados e recomendações normativas, e não apenas descrição da solução e dos testes.

Os termos de participação devem estabelecer condições para que a aprendizagem seja efetiva. Recomenda-se exigir dirigente sênior responsável, responsáveis técnicos e jurídicos, estimativa de recursos destinados à governança, acesso da Comissão aos profissionais e documentos necessários e dever permanente de colaboração. A participante deverá comunicar incidentes, anomalias, limitações e mudanças materiais antes de sua implementação. A retenção injustificada de informação, a recusa de acesso a evidências ou a alteração da solução sem ciência da SESP devem constituir hipóteses expressas de suspensão ou encerramento. Essas obrigações de transparência interna podem coexistir com a proteção de segredo comercial, desde que a confidencialidade não impeça fiscalização, auditoria ou responsabilização (Gilbert, Marriott e Leslie, 2026, p. 16).

O aprendizado deve ser convertido em produtos institucionais. O Relatório Consolidado Anual previsto no art. 10, § 3º, do Decreto Estadual nº 13.728/2026 pode formar repositório de evidências com versões públicas e reservadas, metodologia comum, indicadores comparáveis e registro das decisões. O êxito deve ser medido também pela capacidade regulatória criada, pelos protocolos aperfeiçoados, pela redução de incerteza e pelas lições negativas documentadas. A conclusão do sandbox não constitui selo de qualidade, conforme corretamente dispõe o art. 34, mas a SESP deverá informar quais resultados são válidos, em que condições, com quais margens de erro e por quanto tempo. A avaliação deverá registrar anomalias, contradições, resultados negativos e mudanças ao longo do tempo. O relatório final deverá distinguir validade interna, limites de generalização e condições de transferência para outros municípios, forças ou escalas. Assim, casos limitados produzem aprendizagem sem converter um piloto contextual em prova universal de eficácia (Gilbert, Marriott e Leslie, 2026, p. 17).

RESPONSABILIDADE, SEGURANÇA JURÍDICA E ALOCAÇÃO DE RISCOS

Os arts. 26 e 27 devem ser reformulados. A atribuição integral de responsabilidade às entidades participantes e a isenção absoluta da SESP não refletem a diversidade de papéis que podem existir no experimento e não afastam responsabilidades estabelecidas pela Constituição, pela LGPD e por outras leis. A SESP continuará responsável por decisões públicas, supervisão, legalidade dos acessos, definição de finalidades e atuação de seus agentes, enquanto a participante responderá por falhas de sua esfera de controle, descumprimento de instruções, defeitos, segurança e informações inexatas. Recomenda-se substituir as cláusulas gerais por matriz de responsabilidades no TEA, vinculada à causalidade, aos papéis de tratamento, ao dever de diligência e às obrigações específicas de cada parte.

A matriz deve disciplinar danos a terceiros, incidentes de dados, propriedade intelectual, continuidade, cadeia de custódia, subcontratação, atualização de software, segurança de equipamentos, suporte, investigação de falhas e preservação de registros. Quando proporcional ao risco, pode ser exigida comprovação de seguro, garantia técnica ou capacidade financeira, sem transformar o sandbox em barreira intransponível para universidades, ICTs e organizações da sociedade civil admitidas pelo art. 5º. Também se recomenda procedimento claro de reparação e tratamento de reclamações, com preservação do direito de regresso e sem limitar direitos dos afetados. A autorização temporária não pode converter a população em portadora involuntária dos riscos empresariais do experimento.

DESCONTINUIDADE, SUSTENTABILIDADE E ESCALABILIDADE

O Plano de Descontinuidade do Anexo III está bem estruturado, mas precisa abranger a continuidade mínima de serviços essenciais, a reversibilidade de integrações, a portabilidade de dados e configurações, a revogação de credenciais, a remoção de componentes, a verificação de cópias e backups e o suporte pós-encerramento. A AGU recomenda plano para encerramento planejado e emergencial, comunicação antecipada, cumprimento de obrigações e proteção da integridade dos dados (AGU, 2024, p. 55-56). Sugere-se exigir teste do plano antes da operação real e atualização durante o piloto. O cancelamento por falha crítica, previsto no art. 25, deve acionar protocolo com preservação de evidências, contenção, comunicação, retorno ao processo manual e avaliação dos impactos sobre pessoas afetadas.

A sustentabilidade econômico-operacional recebe peso 1 na Matriz, embora a dependência tecnológica seja risco central para a Administração. Recomenda-se elevar seu peso e exigir custo total de propriedade, despesas de infraestrutura, licenças, conectividade, treinamento, manutenção, auditoria, atualização, armazenamento, suporte e desativação. A proposta deve demonstrar quem sustentará a solução após o piloto, quais capacidades serão internalizadas, quais dependências permanecerão e como ocorrerá migração para outro fornecedor. A escalabilidade deve ser avaliada não apenas pela capacidade de ampliar usuários ou território, mas pela manutenção de desempenho, segurança, supervisão e proteção de dados em maior escala.

A passagem do sandbox para eventual contratação deve permanecer separada do processo experimental. O art. 12, inciso VIII, menciona a viabilidade de futura contratação em larga escala, mas a participação não pode conferir preferência, expectativa de contratação ou validação automática, conforme o art. 1º, § 3º, do Decreto Estadual nº 13.728/2026. Recomenda-se que o relatório final declare que eventual aquisição dependerá de planejamento, estudo técnico preliminar, análise de alternativas, estimativa de custos, requisitos de interoperabilidade e segurança e procedimento de contratação aplicável. Os dados e conhecimentos produzidos devem favorecer competição futura e evitar especificações direcionadas e aprisionamento tecnológico.

SÍNTESE CONCLUSIVA

A minuta apresenta base promissora para experimentação responsável em contexto operacional complexo, ao incorporar proteção de dados, supervisão humana, soberania tecnológica, transparência, descontinuidade e monitoramento. Para concretizar esses princípios, recomenda-se corrigir inconsistências de escopo e redação, estabelecer critérios eliminatórios de segurança e direitos, adotar progressão de testes orientada a risco, definir papéis e responsabilidades, distinguir treinamento autorizado de reutilização secundária de dados e substituir a abertura indiscriminada de código e modelos por transparência proporcional e auditabilidade efetiva.

Também se mostra necessário ampliar a participação social contínua, estruturar o aprendizado regulatório, fortalecer sustentabilidade e saída e assegurar que a flexibilização seja individualizada, motivada, temporária, reversível e acompanhada por controles compensatórios. Com esses ajustes, o Sandbox SESP/PR poderá conciliar resolutividade na fronteira com legalidade, proteção de direitos fundamentais, segurança da informação, autonomia tecnológica e confiança pública.

REFERÊNCIAS

ADVOCACIA-GERAL DA UNIÃO; MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS. Guia Referencial de Sandbox Regulatório. Brasília, DF, 2024. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. 2. ed. Brasília, DF, 2022a. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Tratamento de dados pessoais pelo Poder Público. Brasília, DF, 2022b. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Relatório de Impacto à Proteção de Dados Pessoais (RIPD): perguntas e respostas. Brasília, DF, 2023. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

DATASPHERE INITIATIVE. *Sandboxes for DPI: co-creating the blocks of digital trust*. 2026. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

DATASPHERE INITIATIVE. Sandboxes for AI: tools for a new frontier. 2025. Disponível em: acesso eletrônico. Acesso em: 24 jul. 2026.

GILBERT, A.; MARRIOTT, J.; LESLIE, M. IFOW Sandbox: Phase 1 Methodology Report. London: Institute for the Future of Work, 2026. DOI: 10.5281/zenodo.18480973.

GUIO ESPAÑOL, A.; KOENIG, P. D. Regulatory sandboxes for AI in the majority world: a learning-centric approach to legal adaptation. Cambridge Forum on AI: Law and Governance, v. 1, e42, p. 1-20, 2025. DOI: 10.1017/cfl.2025.10015.

PARANÁ. Lei Estadual nº 20.744, de 6 de outubro de 2021. Dispõe sobre as regras para a constituição e normas gerais de funcionamento de ambiente regulatório experimental no Estado do Paraná.

PARANÁ. Decreto Estadual nº 13.728, de 19 de maio de 2026. Regulamenta, no âmbito da Secretaria de Estado da Segurança Pública, o Ambiente Regulatório Experimental da Segurança Pública.

PARANÁ. Secretaria de Estado da Segurança Pública. Minuta do Edital nº 001/2026/SESP e Anexos I a X. Sandbox Regulatório SESP/PR - Fronteira. Curitiba, 2026.

PARANÁ. Secretaria de Estado da Segurança Pública. Regulamento da Audiência Pública do Edital nº 001/2026/SESP. Curitiba, 2026.

PEDIDO

Ante o exposto, requer-se que as observações e propostas desta contribuição sejam recebidas, analisadas e consideradas no aperfeiçoamento da minuta do Edital nº 001/2026/SESP e de seus anexos, com a publicação da resposta administrativa nos termos dos itens 7.7 e 7.8 do Regulamento da Audiência Pública. Requer-se, ainda, a inscrição da interessada para manifestação verbal na sessão de 28 de julho de 2026, nos termos do item 6.2 do referido Regulamento.

Curitiba, 24 de julho de 2026.

Fabiana Cebrian

Pesquisadora em direito digital, proteção de dados pessoais e governança de IA.

Doutoranda em direito - PUCPR

Manifestação pessoal e acadêmica