CÂMARA DOS DEPUTADOS
Gabinete do Deputado Jadyel Alencar – Republicanos/PI

COMISSÃO DE DESENVOLVIMENTO ECONÔMICO

REQUERIMENTO Nº , DE 2026
(Do Sr. Jadyel Alencar)

Requer realização de Audiência Pública para debater os impactos econômicos da nova geração de modelos de Inteligência Artificial de fronteira sobre a competitividade da economia brasileira, a estabilidade do setor financeiro, a segurança digital do setor produtivo e a proteção das infraestruturas críticas nacionais, bem como sua relação com o marco regulatório brasileiro de IA.

Senhor Presidente,

nos termos do art. 117, inciso II, combinado com o art. 255 do Regimento Interno da Câmara dos Deputados, a realização de Audiência Pública, no âmbito desta Comissão de Desenvolvimento Econômico, para debater o tema:

“Inteligência Artificial de fronteira, competitividade econômica, estabilidade financeira e proteção das infraestruturas críticas nacionais.”

Sugiro o convite dos seguintes representantes e especialistas:

a) representante do Banco Central do Brasil;
b) representante do Ministério da Fazenda;
c) representante da Federação Brasileira de Bancos — FEBRABAN;
d) representante da Confederação Nacional da Indústria — CNI;
e) representante de time de segurança de empresa desenvolvedora de modelos de Inteligência Artificial de fronteira, preferencialmente com experiência em avaliação de capacidades cibernéticas, acesso controlado ou programas de uso defensivo;
f) especialista nacional ou internacional em avaliação técnica, governança e impactos econômicos de modelos de Inteligência Artificial de fronteira, preferencialmente vinculado ao UK AI Security Institute — AISI, à Model Evaluation and Threat Research — METR, ao ExploitBench, ou a instituição equivalente.

JUSTIFICAÇÃO

A economia brasileira realiza, há mais de uma década, rápida transição para infraestrutura digital crítica. Pix, Open Finance, Sistema de Pagamentos Brasileiro, sistemas de tributação digital, plataformas de crédito, telecomunicações, redes elétricas inteligentes, cadeias logísticas baseadas em software e comércio eletrônico passaram a sustentar o funcionamento cotidiano da atividade produtiva nacional. Esses ganhos de eficiência, inclusão e produtividade são diferenciais competitivos do Brasil, mas também criam dependência sistêmica de software e, portanto, da segurança desse software.

A nova geração de modelos de Inteligência Artificial de fronteira lançada desde abril de 2026, entre eles o Claude Mythos Preview, da Anthropic, e o GPT-5.5, da OpenAI, altera materialmente a economia da segurança cibernética. O problema central, do ponto de vista econômico, não é apenas o aumento de capacidade técnica desses modelos. É que eles podem reduzir drasticamente o custo de produzir ataques cibernéticos funcionais, ao mesmo tempo em que aumentam o custo de defesa para organizações que não dispõem de capacidade técnica equivalente. Falhas em sistemas digitais que antes exigiam equipes especializadas e longos períodos de análise podem ser encontradas, testadas e priorizadas em frações desse tempo. Essa reorganização da relação entre custo de ataque e custo de defesa tem efeitos diretos sobre custo de capital, seguros cibernéticos, adaptação tecnológica, continuidade operacional e confiança no ambiente de negócios brasileiro.

As evidências dessa transformação se acumularam rapidamente. A Model Evaluation and Threat Research — METR, organização independente de avaliação de modelos de IA, documentou em estudo publicado em março de 2025 e atualizado em janeiro de 2026 que a duração das tarefas técnicas que modelos de fronteira conseguem completar autonomamente vem dobrando em escala de poucos meses, não de anos. Em sua atualização de 8 de maio de 2026, a METR incluiu o Claude Mythos Preview em suas medições de task-completion time horizons e passou a advertir que medições acima de 16 horas já não são confiáveis com sua suíte atual de tarefas. Essa métrica não mede o tempo durante o qual o modelo atua autonomamente, mas a duração de tarefas técnicas, estimada pelo tempo que especialistas humanos levariam para completá-las, que agentes de IA conseguem concluir com determinada probabilidade de sucesso. Em paralelo, o UK AI Security Institute — AISI relatou que versões recentes do mesmo modelo foram capazes de completar cenários complexos de ataque em ambientes controlados, inclusive testes que nenhum modelo havia concluído anteriormente, embora o próprio instituto ressalte que tais avaliações cobrem apenas parte das capacidades relevantes para ataques contra sistemas em produção.

Resultados convergentes vieram de empresas que operam infraestrutura digital ou atuam em cibersegurança. A Cloudflare publicou, em maio de 2026, avaliação na qual testou o Claude Mythos Preview contra mais de cinquenta repositórios próprios, destacando a capacidade do modelo de encadear vulnerabilidades menores em cadeias de exploração mais graves e gerar autonomamente código de prova de conceito. A XBOW, empresa especializada em segurança ofensiva, relatou avanço expressivo na identificação e validação de vulnerabilidades, especialmente quando o modelo dispõe de acesso ao código-fonte. Benchmarks especializados publicados em maio de 2026, como o ExploitBench, também indicam que modelos de fronteira já conseguem percorrer

múltiplos estágios do processo de exploração de vulnerabilidades em ambientes controlados. Segundo cobertura jornalística, a empresa de pesquisa em segurança Calif relatou ter desenvolvido, com auxílio do Claude Mythos Preview, código de exploração funcional para vulnerabilidade de escalonamento de privilégios no macOS, ilustrando a capacidade desses modelos de acelerar a reprodução e adaptação de técnicas já conhecidas.

Essas evidências não significam que tais modelos possam, por si só, comprometer na atualidade sistemas financeiros ou infraestruturas críticas reais. Sistemas em produção são complexos, contam com múltiplas camadas de defesa e envolvem fatores técnicos, humanos e institucionais. Os resultados recentes indicam, contudo, uma mudança relevante no cenário de risco econômico: a janela entre a divulgação de uma falha, a produção de um exploit funcional e a necessidade de correção tende a se tornar substancialmente menor, com implicações diretas para o setor financeiro, o setor produtivo digitalmente intensivo e as infraestruturas críticas que sustentam a atividade econômica.

O mesmo conjunto de capacidades também pode operar do lado defensivo, com implicações econômicas positivas. A Mozilla relatou que o Firefox 150 incluiu correções para 271 vulnerabilidades identificadas em um único ciclo de avaliação com o Claude Mythos Preview, ilustrando o potencial dessas capacidades quando aplicadas pelos próprios desenvolvedores de software. A questão econômica relevante para o Brasil, portanto, não é se o uso de tais capacidades deve ser obstado, mas se o ecossistema produtivo brasileiro (empresas, instituições financeiras, operadores de infraestrutura crítica e órgãos públicos) disporá de acesso, coordenação e capacidade técnica suficientes para reduzir a assimetria entre ataque e defesa.

A agenda econômica internacional já tratou do tema. Em 7 de maio de 2026, o Fundo Monetário Internacional publicou análise alertando que modelos de IA avançados podem reduzir drasticamente o tempo e o custo necessários para identificar e explorar vulnerabilidades em infraestrutura digital compartilhada, como software, serviços de nuvem e redes de pagamento, e que perdas decorrentes de incidentes cibernéticos extremos poderiam desencadear tensões de funding, preocupações de solvência e perturbações de mercado mais amplas, afetando diretamente custo de capital, fluxos de investimento e continuidade da atividade econômica real. Em 15 de maio de 2026, o Bank of England, a Financial Conduct Authority e o HM Treasury publicaram declaração conjunta sobre modelos de IA de fronteira e resiliência cibernética, caracterizando-os como uma mudança qualitativa de capacidade (step-change in capability) e reconhecendo que tais capacidades já excedem o que um profissional especializado pode alcançar, em velocidade significativamente maior, escala maior e custo menor. O National Cyber Security Centre do Reino Unido publicou, em paralelo, orientação específica sobre preparação para uma possível “onda de patches” decorrente da aceleração de descoberta e exploração de vulnerabilidades por modelos de IA. O Financial Stability Board, órgão central da governança financeira internacional, também passou a tratar o tema como risco emergente para a estabilidade global, em diálogo direto com a Anthropic.

Neste contexto, o Brasil ocupa hoje, em razão do êxito de sua agenda de inclusão financeira e modernização do sistema de pagamentos, posição de exposição relevante

ao tipo de risco econômico que essas capacidades introduzem. Pix, Open Finance, Sistema de Pagamentos Brasileiro, serviços em nuvem, redes de telecomunicações, provedores comuns de tecnologia e bases de dados compartilhadas constituem parte essencial da infraestrutura digital da economia brasileira. Esse desenho traz ganhos importantes de eficiência, inclusão e competitividade, mas também aumenta a relevância de riscos cibernéticos sistêmicos, em particular o risco de falhas correlacionadas que afetem simultaneamente múltiplas instituições e comprometam pagamentos, liquidez, confiança e continuidade de serviços essenciais para o setor produtivo.

Risco sistêmico, na definição consolidada pelo Bank for International Settlements, pelo Financial Stability Board e pelo Fundo Monetário Internacional em relatório conjunto ao G20, corresponde ao risco de disrupção dos serviços financeiros causada pelo comprometimento de todo ou de parte do sistema financeiro, com potencial de gerar consequências negativas relevantes para a economia real. A literatura especializada, desde os trabalhos de Acharya, Pedersen, Philippon e Richardson sobre mensuração de risco sistêmico, de Brunnermeier, Crockett, Goodhart, Persaud e Shin sobre os fundamentos da regulação financeira, e de Bandt e Hartmann no Banco Central Europeu, associa esse risco a três vetores principais: (i) interconexões e exposições comuns entre instituições; (ii) sincronização de comportamentos sob estresse; e (iii) dependência de infraestruturas, dados e provedores tecnológicos compartilhados.

O próprio Banco Central do Brasil reconheceu, ao editar a Resolução BCB nº 538, de 18 de dezembro de 2025, e a Resolução CMN nº 5.274, de 18 de dezembro de 2025, que o risco cibernético deixou de ser tratado como mero risco operacional contido em cada instituição e passou a ser endereçado como vetor de risco para a estabilidade do Sistema Financeiro Nacional, dada a centralidade do Pix, do Sistema de Pagamentos Brasileiro e da Rede do Sistema Financeiro Nacional. Na mesma direção, o Relatório de Estabilidade Financeira do Banco Central de novembro de 2025 dedicou seções específicas tanto à pesquisa sobre uso de inteligência artificial no Sistema Financeiro Nacional quanto à análise dos incidentes cibernéticos como fatores de risco e suas implicações para a estabilidade financeira, sinalizando que ambos os temas integram, hoje, a agenda macroprudencial brasileira.

Atualmente, o Brasil ainda não dispõe da arquitetura institucional construída ou em desenvolvimento em jurisdições comparáveis para lidar com os riscos econômicos que podem vir a ser originados pela Inteligência Artificial de fronteira, especificamente:

i) instituto técnico de avaliação independente de modelos de IA, análogo aos AI Safety Institutes já existentes ou em desenvolvimento em outras jurisdições;

ii) mecanismo formal de consulta e compartilhamento de informações com laboratórios de IA antes do lançamento de modelos de alta capacidade;

iii) arcabouço federal para avaliação independente de modelos de IA de propósito geral e de fronteira;

iv) regime obrigatório de reporte de incidentes graves envolvendo sistemas de IA;

v) representação consolidada nas redes internacionais de coordenação técnica que vêm se formando em torno desses temas.

As implicações econômicas dessa lacuna institucional são diretas. A ausência dessa arquitetura pode elevar custos para empresas brasileiras, aumentar a dependência de provedores estrangeiros de segurança e auditoria, reduzir a capacidade

de resposta do setor produtivo e dificultar a atração de investimento, talento técnico e empresas do ecossistema de IA e cibersegurança. A construção tempestiva dessa arquitetura é, portanto, fator de competitividade econômica.

Nesse contexto, a urgência do calendário legislativo é ampliada pela velocidade técnica do campo. Capacidades que modelos de fronteira não apresentavam há doze meses são hoje documentadas em avaliações independentes; capacidades hoje no limite da medição podem estar amplamente disponíveis em poucos meses. Caso a matéria não avance em 2026, é provável que a discussão seja postergada para 2027, em novo contexto político e institucional, com perda da janela para construção tempestiva de capacidade pública de avaliação, supervisão e resposta; janela que se traduz, em termos econômicos, em diferencial de competitividade a ser construído ou perdido.

A presente Audiência Pública tem quatro objetivos principais:

i) compreender as implicações econômicas dos riscos que modelos de IA de fronteira podem representar para o setor financeiro brasileiro, para o setor produtivo digitalmente intensivo e para as infraestruturas críticas que sustentam a atividade econômica;

ii) avaliar como a atual arquitetura institucional brasileira afeta a competitividade do país no cenário internacional de IA e cibersegurança, identificando custos suportados pelo setor privado em razão de lacunas regulatórias;

iii) identificar lacunas regulatórias e operacionais nos projetos de lei em tramitação que tenham impacto direto sobre o ambiente de negócios, o custo de capital, a continuidade operacional e a confiança do investidor;

iv) subsidiar esta Comissão no debate sobre competitividade econômica, estabilidade financeira, segurança digital e confiança no ambiente de negócios brasileiro.

A Comissão de Desenvolvimento Econômico tem papel direto nesse debate. A competitividade da economia brasileira, a estabilidade do sistema financeiro, a continuidade de serviços digitais, a confiança de investidores, a proteção de infraestruturas críticas e a capacidade do Brasil de participar de forma segura e competitiva da economia da Inteligência Artificial são temas centrais para o desenvolvimento nacional e para o ambiente de negócios brasileiro.

Pelas razões expostas, conto com o apoio dos nobres pares para a aprovação do presente Requerimento.

Sala das Comissões, 21 de maio de 2026.

Deputado JADYEL ALENCAR
Republicanos/PI

Câmara dos Deputados – Anexo IV – Gabinete 519 – Cep: 70160-900 – Brasília/DF
Telefone: (61) 3215 5519 – E-mail: dep.jadyelalencar@camara.leg.br