REQUERIMENTO DE INFORMAÇÃO Nº , DE 2026

(Da Sra. Adriana Ventura)

Requer informações ao Ministro de Estado da Justiça e Segurança Pública, Sr. Wellington César Lima e Silva, sobre governança de acessos, auditoria, resposta a incidentes e medidas corretivas relativas à Plataforma Córtex e a outros sistemas sob responsabilidade do MJSP.

Senhor Presidente,

Nos termos do artigo 50, § 2º da Constituição Federal e dos artigos 115, I e 116 do Regimento Interno da Câmara dos Deputados, solicito a Vossa Excelência que seja encaminhado ao Ministro de Estado da Justiça e Segurança Pública, Sr. Wellington César Lima e Silva, o presente Requerimento de Informação, a fim de que sejam prestados os esclarecimentos e encaminhados os documentos oficiais abaixo especificados acerca da cronologia administrativa dos eventos de segurança, da governança de acessos, das trilhas de auditoria, da coordenação interinstitucional, das apurações administrativas e das medidas corretivas relativas à Plataforma Córtex e a outros sistemas, bases de dados, módulos, integrações, APIs, painéis e ferramentas de apoio à atividade de inteligência, investigação criminal, segurança pública e monitoramento operacional sob responsabilidade, gestão, custódia ou supervisão do Ministério da Justiça e Segurança Pública.

Requer-se que as respostas sejam apresentadas item a item, com indicação expressa do respectivo número de processo SEI, da unidade responsável, da

autoridade subscritora, da data de emissão e, quando houver, do controle de versão do documento encaminhado. Na hipótese de sigilo legal, requer-se a indicação expressa do fundamento jurídico da restrição e o envio de versão parcialmente tarjada, extrato consolidado ou síntese técnica não sigilosa, sempre que possível.

1. Delimitação dos sistemas alcançados e cronologia administrativa dos eventos

Informar quais sistemas, bases de dados, módulos, integrações, APIs, painéis e ferramentas de apoio à atividade de inteligência, investigação criminal, segurança pública e monitoramento operacional, sob responsabilidade, gestão, custódia ou supervisão do MJSP, da SENASP e de órgãos a ele subordinados, inclusive a Polícia Federal, registraram, desde 1º de janeiro de 2024, quaisquer dos seguintes eventos:

a) alerta de segurança;

b) acesso suspeito;

c) consulta atípica;

d) uso incompatível com a finalidade funcional;

e) compartilhamento ou uso indevido de credenciais;

f) bloqueio de usuário;

g) bloqueio de API;

h) revisão extraordinária de perfis;

i) suspensão de integração;

j) descontinuação, suspensão parcial ou substituição do sistema.

Para cada sistema ou ferramenta identificado, informar, com data, hora, unidade responsável e processo SEI:

i) a data do primeiro alerta interno;

ii) a data da primeira análise de auditoria;

iii) a data do primeiro bloqueio de usuário ou API;

iv) a data da primeira comunicação interna à chefia;

v) a data da primeira comunicação à Polícia Federal ou a outro órgão competente;

vi) a data de eventual revisão extraordinária de acessos;

vii) a data de eventual suspensão, descontinuação ou substituição.

2. Atos formais de governança, segurança e decisão

Encaminhar cópia, ainda que parcialmente tarjada, dos atos normativos, notas técnicas, pareceres, manuais, fluxos operacionais, matrizes de responsabilidade, procedimentos operacionais padrão, termos de referência, políticas de segurança, registros de versão, despachos e documentos decisórios que disciplinaram, entre 1º de janeiro de 2024 e a data da resposta, a governança, a gestão de usuários, a auditoria, a segurança da informação, a resposta a incidentes e a revisão de acessos da Plataforma Córtex e dos demais sistemas identificados no item 1.

3. Relatórios consolidados de auditoria por sistema

Encaminhar relatórios consolidados e anonimizados, sem logs brutos, relativamente à Plataforma Córtex e aos demais sistemas identificados no item 1, contendo ao menos:

a) quantidade de alertas por mês;

b) quantidade de usuários bloqueados e desbloqueados;

c) quantidade de APIs suspensas;

d) classificação das anomalias identificadas;

e) tempo médio entre alerta e bloqueio;

f) quantidade de casos encaminhados à Polícia Federal ou a outro órgão competente;

g) quantidade de revisões extraordinárias de perfil;

h) indicação de quais sistemas foram submetidos a varredura técnica, revisão de logs ou auditoria extraordinária em razão dos fatos noticiados publicamente no âmbito do caso Banco Master.

4. Quantificação das ocorrências administrativas por sistema

Informar o número total de ocorrências administrativas identificadas entre 1º de janeiro de 2024 e a data da resposta, discriminadas por sistema, módulo ou integração e por tipo de ocorrência, inclusive:

a) consulta atípica;

b) divergência de perfil;

c) alteração suspeita de IP;

d) volumetria anômala;

e) acesso fora do escopo funcional;

f) uso por credencial de terceiro;

g) compartilhamento irregular de credenciais;

h) extração ou tentativa de extração de dados;

i) acesso por integração automatizada em desconformidade com regras de negócio;

j) falha de segregação de perfis ou permissões excessivas.

5. Trilhas de auditoria, retenção e rastreabilidade

Informar, para a Plataforma Córtex e para os demais sistemas identificados no item 1:

a) quais trilhas de auditoria eram ou são mantidas;

b) quais campos mínimos eram capturados nos logs de front-end e APIs;

c) quais os prazos de retenção;

d) qual a base normativa aplicável;

e) qual a unidade custodiante;

f) quais perfis institucionais detinham competência para auditoria, bloqueio preventivo e desbloqueio;

g) se havia mecanismos de correlação de eventos entre módulos e integrações;

h) se os registros eram exportáveis para instrução de procedimentos internos.

6. Medidas emergenciais e efetividade

Para cada medida corretiva ou emergencial eventualmente adotada em relação à Plataforma Córtex e a outros sistemas identificados no item 1, inclusive autenticação reforçada, duplo fator de autenticação, restrição de sessão, bloqueio de IPs, whitelist, recadastramento de usuários, limitação de perfis cadastradores, bloqueio por volumetria, revisão extraordinária de acessos, suspensão de integrações e auditoria contínua, informar:

a) data de implantação;

b) processo SEI;

c) autoridade que aprovou;

d) sistema, módulo ou integração afetado;

e) universo de usuários alcançados;

f) exceções autorizadas;

g) indicador de efetividade adotado;

h) resultado aferido até a data da resposta.

Informar, ainda, se, diante dos fatos noticiados publicamente no âmbito da Operação Compliance Zero e do caso Banco Master, o MJSP determinou varredura técnica, revisão de logs, auditoria extraordinária, recadastramento, suspensão preventiva de perfis ou revisão de integrações em outros sistemas, bases ou ferramentas além da Plataforma Córtex. Em caso positivo, encaminhar a relação dos sistemas alcançados, a data da deliberação, a autoridade responsável e os documentos correspondentes. Em caso negativo, justificar expressamente.

7. Comunicação institucional e coordenação interinstitucional

Informar se houve comunicação formal à Polícia Federal, à Controladoria-Geral da União, ao Gabinete de Segurança Institucional, ao CTIR Gov, ao Tribunal de Contas da União ou a outros órgãos de controle, governança cibernética ou persecução, indicando:

a) data;

b) unidade remetente;

c) autoridade subscritora;

d) processo SEI;

e) fundamento técnico ou jurídico;

f) documentos encaminhados.

Na hipótese de não ter havido comunicação a algum desses órgãos, informar:

i) a unidade que examinou o tema;

ii) a autoridade decisória;

iii) a data da deliberação;

iv) a manifestação técnica ou jurídica que a embasou;

v) as medidas alternativas eventualmente adotadas.

8. Apuração administrativa e responsabilização

Informar se foram instauradas apurações preliminares, sindicâncias, processos administrativos disciplinares, revisões extraordinárias de credenciamento, auditorias especiais, tomadas de subsídios ou quaisquer outros procedimentos administrativos relacionados ao uso indevido da Plataforma Córtex ou de outros sistemas identificados no item 1. Em caso positivo, encaminhar os atos de instauração, a indicação da autoridade competente, a fase processual e, quando possível, extrato consolidado ou versão parcialmente tarjada. Em caso negativo, indicar expressamente a autoridade que deliberou pela não instauração e a respectiva motivação administrativa.

9. Auditoria externa, controle interno e revisão pós-incidente

Informar se a Plataforma Córtex ou quaisquer dos sistemas identificados no item 1 foram objeto de auditorias, avaliações de conformidade, testes de segurança, revisões independentes, pentests, post-mortem ou análises formais de risco por órgãos de controle interno, auditoria interna, corregedoria, CGU, GSI, CTIR Gov, TCU ou terceiros contratados. Em caso positivo, encaminhar os relatórios, recomendações, planos de ação e cronogramas de implementação. Em caso negativo, informar se houve recomendação interna para adoção dessas providências, quem decidiu não adotá-las e com qual motivação.

10. Convenentes, instrumentos jurídicos, integrações e acessos compartilhados

Encaminhar a relação completa dos Acordos de Cooperação Técnica, termos de adesão, instrumentos equivalentes, autorizações de integração e atos de compartilhamento vigentes entre 1º de janeiro de 2024 e a data da resposta, relativos à Plataforma Córtex e a outros sistemas ou ferramentas referidos no item 1, com indicação de:

a) órgão ou entidade convenente;

b) vigência;

c) objeto;

d) perfis autorizados;

e) bases ou módulos acessíveis;

f) existência de acesso via front-end, API, webservice ou mecanismo equivalente;

g) regras de auditoria;

h) hipóteses de suspensão e bloqueio;

i) unidade responsável pela supervisão do convenente ou integração.

JUSTIFICAÇÃO

A gravidade do tema recomenda o aprofundamento da fiscalização parlamentar não apenas sobre a Plataforma Córtex, mas também sobre outros sistemas, bases, módulos, integrações e ferramentas de apoio à atividade de inteligência, investigação criminal, segurança pública e monitoramento operacional sob responsabilidade, gestão, custódia ou supervisão do Ministério da Justiça e Segurança Pública. Em nota oficial divulgada em 4 de março de 2026, a Polícia Federal informou que a 3ª fase da Operação Compliance Zero[1] tem por objeto apurar a possível prática dos crimes de ameaça, corrupção, lavagem de dinheiro e invasão de dispositivos informáticos por organização criminosa, com apoio do Banco Central do Brasil.

[1] https://www.gov.br/pf/pt-br/assuntos/noticias/2026/03/policia-federal-deflagra-3a-fase-da-operacao-compliance-zero?utm_source=chatgpt.com

Além da comunicação oficial, reportagens[2][3][4][5][6] recentemente divulgadas acerca do caso Banco Master trouxeram a público informações sobre possível obtenção indevida de dados e acessos irregulares a sistemas e documentos sensíveis. Segundo o noticiário, elementos colhidos no curso das investigações da Polícia Federal indicariam acesso antecipado a documentos relacionados à apuração em trâmite na Justiça Federal e no Banco Central, inclusive mediante uso indevido de credenciais e monitoramento de autoridades. Também foram divulgadas informações sobre a possível existência de estrutura paralela voltada à vigilância e à intimidação de críticos, com menção à obtenção ilícita de informações sigilosas e a acessos indevidos a bases restritas de órgãos públicos.

Tais elementos recomendam que o presente requerimento não se restrinja à Plataforma Córtex. A função fiscalizatória da Câmara dos Deputados exige verificar, na esfera administrativa do Poder Executivo federal, se houve detecção de acessos suspeitos, revisão extraordinária de perfis, bloqueios, auditorias, comunicação institucional, medidas corretivas e apurações internas em outros sistemas ou integrações sensíveis sob responsabilidade do MJSP. O objetivo do presente requerimento é, portanto, aferir a robustez dos controles de acesso, das trilhas de auditoria, da segregação de perfis, da resposta a incidentes e da governança de dados no âmbito ministerial, sem avançar sobre conteúdo protegido por sigilo investigativo ou sobre sistemas estranhos à competência do Ministro de Estado.

Diante disso, as informações ora requeridas mostram-se necessárias para apurar, de forma objetiva e documental, se o Ministério adotou providências adequadas e tempestivas para identificar eventuais vulnerabilidades, conter riscos, revisar acessos, fortalecer mecanismos de auditoria e aperfeiçoar a governança de sistemas sensíveis, em estrita observância à competência fiscalizatória do Congresso Nacional.

---

[2] https://g1.globo.com/politica/noticia/2026/03/04/grupo-comandado-por-vorcaro-acessou-sistemas-restritos-da-pf-mpf-fbi-e-interpol-aponta-investigacao.ghtml
[3] https://www.gazetadopovo.com.br/republica/sicario-vorcaro-invadiu-sistema-justica-4-meses-banqueiro-preso/
[4] https://www.gazetadopovo.com.br/republica/como-o-grupo-de-daniel-vorcaro-invadiu-sistemas-da-justica-e-do-banco-central/
[5] https://www.estadao.com.br/politica/blog-do-fausto-macedo/equipe-de-vorcaro-usou-tecnica-hacker-para-roubar-senhas-de-funcionarios-do-ministerio-publico/?srsltid=AfmBOor5QsMgYX3sDfCT4xIYmVVRLZBLm_0FXmp7026-dKz9J0jlh0Vt
[6] https://www.migalhas.com.br/quentes/451086/a-turma-vorcaro-tinha-milicia-privada-para-monitorar-criticos-diz-pf

Diante do exposto, conto com o apoio dos nobres Pares para a aprovação deste Requerimento de Informação.

Sala das Sessões, em de de 2026.

Deputada Federal **Adriana Ventura**
NOVO/SP

Requerimento de Informação

Deputado(s)

1 Dep. Adriana Ventura (NOVO/SP)
2 Dep. Luiz Lima (NOVO/RJ)
3 Dep. Gilson Marques (NOVO/SC)
4 Dep. Marcel van Hattem (NOVO/RS)
5 Dep. Diego Garcia (REPUBLIC/PR)