33635074 08027.001535/2025-78

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Assuntos Legislativos
Gabinete da Secretaria Nacional de Assuntos Legislativos
Área de Assessoria da Secretaria Nacional de Assuntos Legislativos

OFÍCIO Nº 862/2025/Assessoria-SAL/GAB-SAL/SAL/MJ

Brasília, na data da assinatura.

A Sua Excelência o Senhor
Deputado Federal Carlos Veras
Primeiro-Secretário
Câmara dos Deputados
70160-900 - Brasília - DF

**Assunto:** Requerimento de Informação Parlamentar nº 6610/2025, de autoria da Deputada Adriana Ventura (NOVO/SP) e do Deputado Luiz Lima (NOVO/RJ)

**Referência:** Ofício 1ªSec/RI/E/nº 394

Senhor Primeiro-Secretário,

Reporto-me ao Requerimento de Informação Parlamentar nº 6610/2025, de autoria da Deputada Federal Adriana Ventura (NOVO/SP) e do Deputado Federal Luiz Lima (NOVO/RJ), para encaminhar o OFÍCIO Nº 11394/2025/GAB-SENASP/SENASP/MJ e anexos, elaborados pela Secretaria Nacional de Segurança Pública (SENASP), área técnica deste Ministério da Justiça e Segurança Pública, a fim de subsidiar resposta aos i. parlamentares.

Na oportunidade, renovo protestos de estima e consideração.

Atenciosamente,

**RICARDO LEWANDOWSKI**
Ministro de Estado da Justiça e Segurança Pública

Documento assinado eletronicamente por **Ricardo Lewandowski**, **Ministro de Estado da Justiça e Segurança Pública**, em 08/12/2025, às 19:57, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **33635074** e o código CRC **D17D0692**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Anexos:**

a) OFÍCIO Nº 11394/2025/GAB-SENASP/SENASP/MJ (33619419);
b) INFORMAÇÃO Nº 36/2025/DIOPI/SENASP (33616801), e
c) Anexo QTD ÓRGÃOS POR ESFERAS (33601911).



Esplanada dos Ministérios, Bloco T, Ed. Sede, 4º Andar, Sala 436, - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-3223 - www.gov.br/mj/pt-br

33616801 08027.001535/2025-78

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Diretoria de Operações Integradas e de Inteligência

INFORMAÇÃO Nº 36/2025/DIOPI/SENASP

Processo: **08027.001535/2025-78**

Assunto: **Requerimento de Informação Parlamentar - RIC n.º 6610/2025, de autoria da Deputada Federal Adriana Ventura e outros.**

1. Trata-se do Requerimento de Informação n.º 6610/2025 (33460318), por meio do qual a Deputada Federal Adriana Ventura e outros, requer informações ao Ministério da Justiça e Segurança Pública sobre a governança, os controles de integridade, a segurança cibernética e as medidas corretivas adotadas no âmbito do sistema Córtex, em decorrência de sua utilização indevida por terceiros, inclusive por integrantes de organizações criminosas, conforme reportagens e investigações da Polícia Federal, conforme detalhado abaixo:

> 1) Estrutura e Governança do Sistema
>
> a. Encaminhar organograma atualizado das unidades responsáveis pela gestão, operação e auditoria do sistema Córtex, indicando competências, chefias e vínculos hierárquicos.
>
> b. Descrever a arquitetura de governança aplicada ao Córtex (normas internas, fluxos de decisão, instâncias de supervisão e auditoria).
>
> c. Informar a data e conteúdo das últimas revisões de políticas internas de acesso, controle e integridade do sistema.
>
> 2) Controle de Acesso e Rastreabilidade
>
> a. Descrever os mecanismos de autenticação, logs e trilhas de auditoria implementados, incluindo retenção, revisão e cruzamento de registros de acesso.
>
> b. Informar o número total de perfis de acesso ativos entre 01/01/2024 e 30/09/2025, discriminando por tipo de órgão conveniado (federal, estadual, municipal).
>
> c. Encaminhar relatório (ou amostra representativa) de logs de acesso auditados que tenham identificado consultas atípicas ou indevidas, suprimindo dados pessoais e sigilosos.
>
> d. Informar a frequência e metodologia de auditoria interna de acessos, bem como as instâncias que analisam os resultados e determinam providências.
>
> 3) Incidente de Segurança e Medidas Corretivas
>
> a. Informar a data de detecção da invasão ou uso indevido do Córtex e os principais achados da investigação da Polícia Federal até o momento, limitando-se a informações passíveis de publicidade.
>
> b. Descrever as medidas emergenciais adotadas pelo Ministério para suspender, conter e revisar os acessos indevidos, inclusive bloqueio de credenciais, revisão de perfis e atualização de protocolos.
>
> c. Indicar se foi instaurada sindicância, processo administrativo disciplinar ou outro procedimento interno; encaminhar cópia dos atos de instauração e, se possível, relatórios conclusivos.
>
> d. Especificar eventuais falhas técnicas identificadas e o plano de ação para sua correção, com prazos, responsáveis e metas.
>
> 4) Coordenação Interinstitucional
>
> a. Informar se houve comunicação formal à Controladoria-Geral da União (CGU), ao Gabinete de Segurança Institucional (GSI) e ao Tribunal de Contas da União (TCU) acerca do incidente, anexando ofícios, pareceres e respostas recebidas.
>
> b. Descrever a interação com a Polícia Federal e demais órgãos de segurança para apuração dos fatos, indicando fluxos de cooperação e protocolos de compartilhamento de informações.
>
> c. Apresentar plano de reforço de segurança e governança elaborado em conjunto com CGU e GSI, se existente.
>
> 5) Prevenção, Integridade e Transparência
>
> a. Encaminhar cópia das normas internas, manuais e checklists de integridade e *compliance* digital aplicáveis aos usuários e operadores do Córtex.
>
> b. Informar as ações de capacitação ou sensibilização sobre ética e uso responsável de sistemas de inteligência realizadas em 2024–2025 (quantitativo, público-alvo, conteúdo e periodicidade).
>
> c. Descrever como se dá a publicidade ativa das informações sobre a gestão do Córtex, indicando os relatórios e dados abertos disponíveis (sem conteúdo sensível).
>
> d. Indicar se foi elaborado ou está em elaboração plano de melhoria de governança e segurança cibernética, com cronograma e responsáveis.
>
> 6) Supervisão e Auditoria Externa
>
> a. Informar se o sistema Córtex foi objeto de auditorias pela CGU, TCU ou outros órgãos entre 2023 e 2025; encaminhar cópias dos relatórios, recomendações e planos de ação.
>
> b. Esclarecer quais recomendações foram implementadas e quais permanecem pendentes, com justificativas e prazos de cumprimento.

2. Em atenção ao expediente, cumpre observar, preliminarmente, que a Diretoria de Operações Integradas e de Inteligência (DIOPI/SENASP), inserida na estrutura organizacional da Secretaria Nacional de Segurança Pública - SENASP, tem suas competências delineadas no Art. 28 do Decreto nº 11.348, de 2023, nos seguintes termos:

> "Art. 28. À Diretoria de Operações Integradas e de Inteligência compete:
>
> I - assessorar a Secretaria nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública federais, estaduais, municipais e distritais;
>
> II - implementar, manter e modernizar redes de integração e de sistemas nacionais de inteligência de segurança pública, em conformidade com disposto na Lei nº 13.675, de 2018;
>
> III - promover a integração das atividades de inteligência de segurança pública, em consonância com os órgãos de inteligência federais, estaduais, municipais e distritais que compõem o Subsistema de Inteligência de Segurança Pública;

> IV - coordenar o Centro Integrado de Comando e Controle Nacional e promover a integração dos centros integrados de comando e controle regionais;
>
> V - subsidiar o Secretário na definição da política nacional de inteligência de segurança pública quanto à doutrina, à forma de gestão, ao uso dos recursos e às metas de trabalho;
>
> VI - promover, com os órgãos componentes do Sistema Brasileiro de Inteligência, a integração e o compartilhamento de dados e conhecimentos necessários à tomada de decisões administrativas e operacionais por parte da Secretaria; e
>
> VII - propor ações de capacitação relacionadas com a atividade de inteligência de segurança pública, a serem realizadas em parceria com a Diretoria de Ensino e Pesquisa."

3. Conforme se depreende da leitura, **compete à DIOPI/SENASP o exercício de ações de cunho estratégico**, concernentes ao desenvolvimento de programas e projetos com objetivo de integrar órgãos e ações de inteligência, de manter e modernizar sistemas nacionais de segurança pública, proteger fronteiras, biomas, enfrentar o crime organizado, prover os gestores regionais de informações para tomada de decisões em níveis tático e operacional, além de propor a capacitação dos agentes de segurança pública.

4. Cumpre destacar ainda que esta DIOPI/SENASP não desenvolve atividades finalísticas de segurança pública, cuja atribuição pertence aos órgãos policiais estaduais e federais, em atenção à autonomia dos entes federados. Com efeito, a DIOPI/SENASP desempenha o papel de articulador entre as instituições, fomentando e apoiando a realização de operações integradas preventivas e repressivas a infrações penais, para que os órgãos atuem e se auxiliem mutuamente, dentro de suas atribuições legais, e na medida dos recursos materiais e humanos disponíveis, objetivando atender aos ditames da Lei do SUSP (Lei n. 13.675, de 2018).

5. Vale ressaltar que o acesso aos sistemas de inteligência de segurança pública e as informações a ele relacionadas são consideradas de **acesso restrito**, conforme os termos da Portaria nº 880/2019, de 12 de dezembro de 2019, do Ministro da Justiça e Segurança Pública (disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-880-de-12-de-dezembro-de-2019-233556005), a qual regulamenta os procedimentos relativos ao acesso e ao tratamento de informações e documentos no âmbito do Ministério da Justiça e Segurança Pública, destacando-se, em especial, o disposto no Art. 16, Incisos II, IV e V. Tais dispositivos estabelecem que são consideradas de acesso restrito as informações cujo conhecimento por pessoa não autorizada possa representar risco ou causar dano aos interesses da sociedade e do Estado.

6. Entre as informações cujo acesso é restrito incluem-se: Informações que evidenciem a capacidade operacional dos órgãos de segurança pública e penitenciária, tais como equipamentos, máquinas, veículos, armamentos e seus acessórios, softwares, entre outros; dados relativos à arquitetura dos sistemas de tecnologia da informação e de comunicações; e aparelhos, equipamentos, suprimentos e programas relacionados às atividades de inteligência e repressão a delitos, conforme dispositivo a seguir colacionado:

> PORTARIA Nº 880, DE 12 DE DEZEMBRO DE 2019
>
> Art. 16. São de acesso restrito as informações cujo conhecimento por pessoa não autorizada implique risco ou dano aos interesses da sociedade e do Estado, tais como:
>
> I - manuais de instrução que revelem a doutrina de atuação dos órgãos de segurança pública, penitenciária e inteligência financeira;
>
> **II - informações que evidenciem a capacidade operacional dos órgãos de segurança pública e penitenciária, tais como equipamentos, máquinas, veículos, armamentos e seus acessórios, softwares, entre outros;**
>
> III - dados relativos à distribuição e capacitação dos agentes dos órgãos de segurança pública e penitenciária;
>
> **IV - dados relativos à arquitetura dos sistemas de tecnologia da informação e de comunicações;**
>
> **V - aparelhos, equipamentos, suprimentos e programas relacionados às atividades de inteligência e repressão a delitos;**
>
> VI - recursos criptográficos; e
>
> VII - plantas arquitetônicas e os dados da segurança orgânica das instalações físicas.

7. Adicionalmente, o Art. 17, inciso IV, da mesma Portaria, dispõe que estão sujeitos a salvaguardas de acesso os processos e documentos que contenham informações com restrição de acesso. No mesmo sentido, o Art. 26 dispõe que as informações classificadas como de acesso restrito somente poderão ser acessadas por servidores diretamente designados, por unidades cujas competências regimentais guardem relação com o conteúdo da informação, conforme a classificação de nível de acesso prevista em normativo específico, ou por aqueles que comprovadamente demonstrem necessidade de conhecimento.

> PORTARIA Nº 880, DE 12 DE DEZEMBRO DE 2019
>
> **[...]**
>
> Art. 17. Estão sujeitos às salvaguardas de acesso os processos ou documentos que contenham:
>
> I - informações classificadas em grau de sigilo;
>
> II - informações pessoais e pessoais sensíveis;
>
> III - informações sigilosas, nos termos da lei; e
>
> **IV - outras informações com restrição de acesso.**

> PORTARIA Nº 880, DE 12 DE DEZEMBRO DE 2019
>
> **[...]**
>
> **Art. 26. As informações de acesso restrito poderão ser acessadas apenas pelos servidores aos quais são destinados ou por unidades que desempenhem as competências regimentais a eles relacionadas, conforme discriminação de nível de acesso constante em normativo específico, e por aqueles que apresentem necessidade de conhecer.**

8. Insta consignar que o Sistema Córtex **não é ferramenta de inteligência artificial.** O Córtex é um sistema de consulta a bases de dados integradas que abrange informações sobre Veículos, Pessoas, Embarcações, Radares e a função de alertas de passagem em câmeras OCRs (leitora de placas) instaladas em vias públicas, e é amplamente utilizado em muitas cidades, estados e diversas instituições, como órgãos de trânsito, DNIT, PRF e Infoseg.

9. Face aos esclarecimentos supracitados, em atenção ao solicitado no presente RIC, apresento pontualmente as contribuições desta Diretoria, conforme segue:

> **1) Estrutura e Governança do Sistema**
>
> **a) Encaminhar organograma atualizado das unidades responsáveis pela gestão, operação e auditoria do sistema Córtex, indicando competências, chefias e vínculos hierárquicos.**
>
> **R:**
> O Sistema Córtex está instituído pela Portaria MJSP nº 218/2021 (https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021/view), e estruturado sob coordenação da

Diretoria de Operações Integradas e de Inteligência (DIOPI/SENASP), atualmente vinculada à Secretaria Nacional de Segurança Pública (SENASP/MJSP).

A governança do sistema compete ao Comitê de Governança Digital e Segurança da Informação e Comunicação (CGDSIC), vinculado à Subsecretaria de Tecnologia da Informação e Comunicação (STI/SE/MJSP), em parceria com a Diretoria de Operações Integradas e de Inteligência (DIOPI/SENASP) – responsável pela gestão negocial, modernização e acompanhamento das funcionalidades e responsável pela gestão técnica e operacional do front-end, integração da API, segurança de acesso e painéis de monitoramento.

A gestão é descentralizada, executada por meio de Gestores Institucionais, Auditores, Pontos Focais e Responsáveis Técnicos, designados segundo os Acordos de Cooperação Técnica (ACTs) firmados entre a União, os entes federativos e os órgãos convenentes, conforme os arts. 14 a 20 da Portaria MJSP nº 218/2021.


**b) Descrever a arquitetura de governança aplicada ao Córtex (normas internas, fluxos de decisão, instâncias de supervisão e auditoria).**

**R:**
Acordos de Cooperação Técnica (ACTs) firmados entre a União, os entes federativos e os órgãos convenentes, conforme os arts. 14 a 20 da Portaria MJSP nº 218/2021, para cooperação e definição de responsabilidades locais compartilhadas entre os Gestores Institucionais, Auditores, Pontos Focais e Responsáveis Técnicos.

Fluxo hierárquico de perfis (DIOPI→ ponto focal → usuário), garantindo controle e rastreabilidade;

Supervisão técnica e estratégica pela SENASP/MJSP, com auditoria dos acessos via *front-end* e *Business Intelligence (BI)*;

Revisões e decisões submetidas às instâncias diretivas da DIOPI/SENASP, conforme normativos internos e fluxos registrados no MJSP.

**c) Informar a data e conteúdo das últimas revisões de políticas internas de acesso, controle e integridade do sistema**

**R:**
As políticas internas de acesso, controle e integridade do Sistema Córtex são revisadas periodicamente pela DIOPI/SENASP, de forma perene, com atualizações de regras de autenticação, bloqueio automático por inatividade e critérios elencados nas normativas internas.

Essas políticas são avaliadas e atualizadas de forma contínua pela DIOPI/SENASP, em conformidade com boas práticas de segurança da informação, gestão de acessos, auditoria, rastreabilidade, proteção de dados e *compliance* institucional.

Essas revisões incluem, entre outros:

- Regras de autenticação e cadastro
- Critérios de bloqueio preventivo e por inatividade
- Parâmetros de auditoria automatizada
- Políticas de desbloqueio e revalidação de perfis
- Procedimentos de resposta a incidentes e mitigação
- Critérios de integração e desativação de APIs

A seguir, as principais revisões e atualizações implementadas no período recente:

| Datas | Políticas Internas | Descrição |
|---|---|---|
| Junho/2023 | **A administração da Plataforma Córtex foi transferida para a DIOPI/SENASP.** | |
| Dezembro/2023 | Fluxo de Auditoria | Estabelecido o fluxo de auditoria da Plataforma Córtex.<br>Formalização de rotinas e critérios de auditoria |
| Outubro/2024 | Plano de Gerenciamento de Projeto | Substituição integral da Plataforma Córtex por um novo Sistema. |

| Datas | Políticas Internas | Descrição |
|---|---|---|
| Novembro/2024 | Plano de Ação Emergencial | Plano para o desenvolvimento de três novos sistemas especializados e segregados para substituição emergencial do Córtex. |
| Fevereiro/2025 | Política de *whitelist* | Controle interno para tratar dos limites de acessos preestabelecidos |
| Fevereiro/2025 | Política de desbloqueio de usuários na Plataforma Córtex | Política para tratamento de solicitação e realização de desbloqueio de usuários na Plataforma Córtex. |
| Março/2025 | Auditoria em todas as funcionalidades | Força-tarefa criado para conduzir uma auditoria emergencial e urgente em todas as funcionalidades do Sistema Córtex. |
| Março/2025 | Atualização do Fluxo de Auditoria | Atualização do fluxo de auditoria da Plataforma Córtex. |
| Março/2025 | Inativação gradual da Plataforma Córtex | Nos processos de ciclo de vida de software, segundo a ABNT, a "descontinuação" é o cancelamento do suporte ativo pela organização de operação e manutenção, substituição total ou parcial por um novo sistema, ou instalação de um sistema atualizado. |
| Março/2025 | Descontinuação da Plataforma Córtex | Processo de descontinuação da Plataforma Córtex |
| Março/2025 | Atualização do Fluxo de Auditoria | Atualização do fluxo de auditoria da Plataforma Córtex. |
| Abril/2025 | Novo Fluxo de Auditoria | Desenvolvimento de um novo processo de auditoria para ser utilizado em conjunto com os fluxos já existentes. |
| Maio/2025 | Novas Auditorias nas APIs | Realização de auditoria abrangente em todas as Integrações e órgãos convenentes. |
| Maio/2025 | Consenso técnico para suspensão das APIs | Descontinuação gradual da atual Plataforma Córtex. |
| Maio/2025 | Nova Auditoria para identificação de uso atípico | Auditoria para identificação de padrões anômalos. |
| Maio/2025 | Plano de suspensão temporária do Córtex | Suspensão temporária da Plataforma Córtex por razões técnicas e operacionais. |
| Junho/2025 | Atuação para identificação de riscos | Identificação e avaliação de riscos operacionais ou sistêmicos. |
| Junho/2025 | Atualização do Plano de Ação Emergencial | Plano de Ação Emergencial para Reestruturação e Substituição da Plataforma Córtex atualizado e novo cronograma. |
| Junho/2025 | Solicitação para levantamento das bases de dados integradas | Determinação para documentar de forma clara e formal a arquitetura da versão atual e futura da plataforma, especialmente sob os aspectos de governança, *compliance*, segurança e rastreabilidade. |
| Agosto/2025 | Uso de software para auditoria | Software destinado a auditar o Córtex de modo agnóstico, independente, permanente, contínuo, técnico e imparcial as operações da plataforma. |
| Novembro/2025 | Descontinuação da Plataforma Córtex | Suspensão temporária da Plataforma Córtex por razões técnicas e operacionais. |

**2) Controle de Acesso e Rastreabilidade**

**a) Descrever os mecanismos de autenticação, logs e trilhas de auditoria implementados, incluindo retenção, revisão e cruzamento de registros de acesso.**

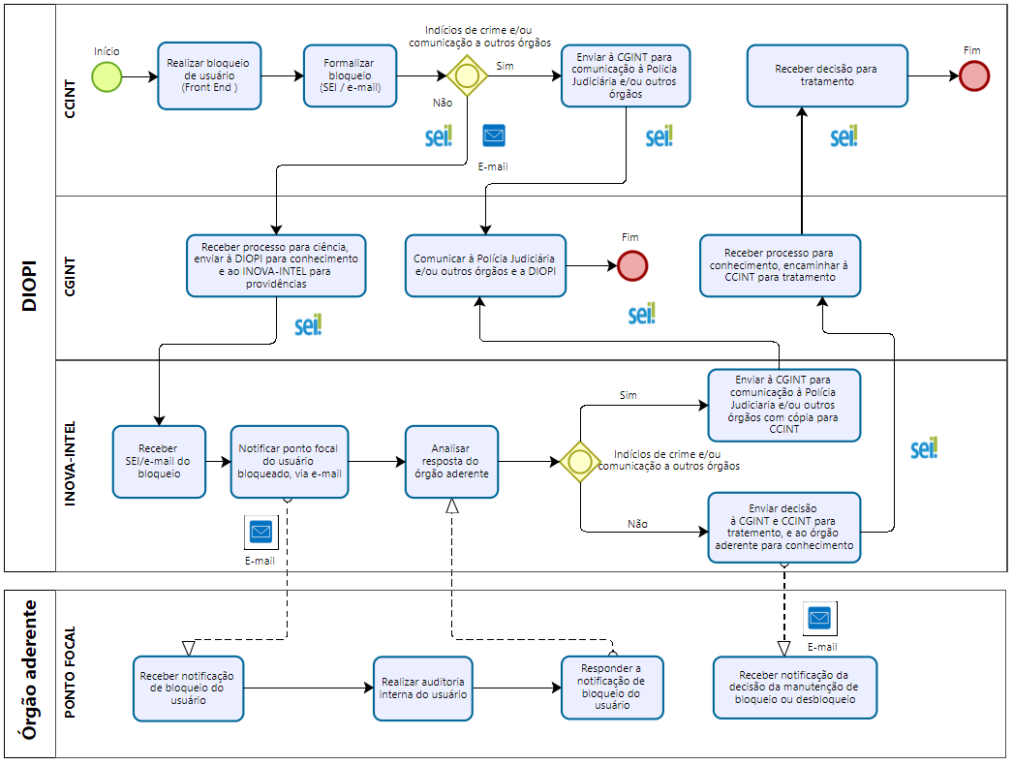
**R:**

O acesso ao Córtex front-end (www.cortex.mj.gov.br) é realizado via GOV.BR, com exigência de nível de segurança "Ouro", dupla autenticação (2FA) e validação de IP para o ambiente de cercamento eletrônico.

Todos os acessos e consultas são registrados em logs estruturados, auditáveis e retidos conforme os prazos legais, sendo acompanhados em painel de *Business Inteligence* desenvolvido pela DIOPI/SENASP, que permite identificar padrões de uso e incongruências.

O acesso ao Córtex via API é realizada utilizando uma arquitetura para fornecer dados a órgãos parceiros e usuários finais. Quando um órgão convenia, recebe uma chave de API única para acessar os dados do Córtex de forma segura e integrada.

Em atenção às duas formas de acesso supracitadas foi criado, **em dezembro de 2023**, um grupo de trabalho composto por servidores da Coordenação-Geral de Inteligência (CGINT/DIOPI/SENASP), que apresentou uma proposta e, que atualmente é utilizada, para o fluxo de auditoria e gestão de usuários bloqueados do módulo cercamento eletrônico do Córtex, conforme imagem abaixo:




**b) Informar o número total de perfis de acesso ativos entre 01/01/2024 e 30/09/2025, discriminando por tipo de órgão conveniado (federal, estadual, municipal).**

**R:**

Considerando perfis de acesso ativos como sendo usuários cadastrados diretamente na interface *web* do sistema por meio dos pontos focais dos órgãos convenentes, o Sistema Córtex contabilizou no período solicitado 39.261 (trinta e nove mil, duzentos e sessenta e um) usuários.

Já a discriminação por tipo de órgão conveniado pode ser verificada na Tabela QTD DE ÓRGÃOS POR ESFERAS (33601911).

**c) Encaminhar relatório (ou amostra representativa) de logs de acesso auditados que tenham identificado consultas atípicas ou indevidas, suprimindo dados pessoais e sigilosos.**

**R:**

O Córtex Front-End possui um módulo específico de Auditoria, destinado ao uso exclusivo dos administradores gerais e auditores designados pelos pontos focais dos órgãos convenentes e pela DIOPI/SENASP.

Esse módulo permite a realização de auditorias direcionadas a partir de parâmetros como CPF do pesquisador, tipo de consulta, objeto pesquisado e período de acesso.

Além disso, há a possibilidade de realizar auditorias a consultas realizadas por meio das APIs integradas (como o BNMP e outros webservices do MJSP), permitindo que sejam identificadas e analisadas eventuais incongruências de uso sem exposição de dados pessoais sensíveis.

De acordo com o art. 29 da Portaria nº 218/2021, os relatórios de auditoria devem abranger três escopos principais:

I – Gestão de usuários, incluindo cadastros, bloqueios e mudanças de perfil;

II – Operações planejadas e coordenadas, para aferição estatística e aprimoramento da plataforma;

III – Comportamento de usuários, com quantificação de atividades, autenticações e padrões de uso.

Cabe destacar que, em observância ao art. 6º, §3º da Lei nº 12.527/2011 (Lei de Acesso à Informação) e ao art. 31 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), os logs brutos e os dados de auditoria individualizada possuem caráter sigiloso, por envolverem informações relacionadas à atividade de segurança pública e consultas de natureza sensível.

Assim, os dados não são compartilhados externamente, mas analisados internamente por meio de painéis *Business Intelligence* que consolidam os indicadores de uso, frequência, bloqueio e anomalias de acesso, permitindo auditoria contínua e responsiva, tanto no nível estratégico (SENASP) quanto operacional (pontos focais).

**d) Informar a frequência e metodologia de auditoria interna de acessos, bem como as instâncias que analisam os resultados e determinam providências.**

**R:**

***Frequência:***

A auditoria interna é realizada de forma contínua e permanente, em tempo real via Sistemas de *Auditoria e Business Intelligence.*

***Metodologia:***

a) Coleta e trilhas de auditoria: captura de eventos de autenticação e uso (timestamp, usuário/perfil, órgão, IP/sessão, endpoint/"tipo de pesquisa", objeto consultado, status), aderente aos escopos de gestão de usuários, operações e comportamento de uso definidos no art. 29 da Portaria nº 218/2021.

b) Detecção de anomalias: regras no front-end/BI para:

- consultas atípicas por volume/horário/origem (ex.: alteração de IP no cercamento durante a sessão);

- uso divergente do perfil/atividade finalística;

- inatividade > 90 dias (bloqueio automático já implementado).

c) Amostragem e 100% dirigido por risco.

d) Rastreabilidade e reprodução: reexecução de trilhas por chave (usuário/período/objeto/pesquisa), com extração controlada para instrução interna — sem exposição externa de logs brutos (LAI/LGPD).

e) Painel gerencial: consolidação em Power BI para séries históricas, rankings por órgão/esfera e indicadores (logins, bloqueios, falhas, tentativas inválidas).

f) Instancias que analisam resultados e determinam providências:

- Nível Operacional (descentralizado): Pontos Focais e Corregedores dos órgãos aderentes analisam o uso local e executam ações imediatas (regularização cadastral, ajuste de perfil, bloqueio/desbloqueio motivado), conforme a lógica hierárquica de perfis prevista na Portaria (ponto focal, gestor regional, usuário).

- Nível Estratégico (federal): DIOPI/SENASP realiza a correlação transversal (multi-órgão), homologa achados e propõe medidas corretivas e de melhoria. Quando necessário, encaminha relatórios/informações às instâncias diretivas da SENASP para deliberação, e envio aos estados alinhados com a portaria Córtex e ACTs.

***Fluxo de providências (resumo):***

1) Detecção (regra/alerta) → 2) Análise (ponto focal/auditor e/ou DIOPI) → 3) Ação imediata (ajuste de perfil/bloqueio motivado) → 4) Registro SEI → 5) Deliberação SENASP para medidas administrativas, técnicas ou normativas.

**3) Incidente de Segurança e Medidas Corretivas**

**a) Informar a data de detecção da invasão ou uso indevido do Córtex e os principais achados da investigação da Polícia Federal até o momento, limitando-se a informações passíveis de publicidade.**

**R:**
A respeito da primeira parte do questionamento, informa-se que as auditorias no âmbito da DIOPI/SENASP, diante da identificação de acessos indevidos à plataforma, todos os registros e evidências relacionados foram encaminhados à Polícia Federal (PF), a quem compete a condução das investigações para apuração dos fatos e responsabilização dos envolvidos.

Informa-se ainda que esta Diretoria não tem acesso a Inquéritos Policiais instaurados pela Polícia Federal, tampouco recebe relatório ou comunicação oficial que informe detalhes da investigação, tais como a data de eventual invasão.

**b) Descrever as medidas emergenciais adotadas pelo Ministério para suspender, conter e revisar os acessos indevidos, inclusive bloqueio de credenciais, revisão de perfis e atualização de protocolo**s

**R:**
De forma imediata e abrangente, o Ministério implementou diversas medidas emergenciais para fortalecer a segurança e conter potenciais acessos indevidos, incluindo:

I - Autenticação gov.br nível ouro: Adoção obrigatória do login via gov.br nível ouro, que exige biometria ou certificado digital, garantindo a validação da identidade do usuário e impedindo cadastros falsos;

II - Duplo fator de autenticação (2FA): Exigência de um fator adicional de segurança, via token ou aplicativo autenticador, dificultando o uso de credenciais furtadas em tentativas de invasão;

III - Restrição de sessão e cookies: Foi reduzido o tempo de expiração das sessões, mitigando o sequestro de cookies e impedindo que um mesmo token fosse utilizado por diferentes IPs para acesso automatizado;

IV - Bloqueio de IPs não autorizados: Implementado bloqueio de requisições provenientes de IPs externos ao país e de IPs diferentes daqueles usados na autenticação inicial, mitigando ataques de origem estrangeira e conexões suspeitas;

V - Controle por lista de IPs autorizados (IP Whitelisting): Cadastro prévio dos IPs institucionais dos órgãos conveniados, permitindo apenas conexões vindas desses endereços. Essa medida reforça a segurança perimetral, limitando o acesso às redes oficiais;

VI - Recadastramento geral de usuários: Todos os usuários foram recadastrados, com inativação de perfis antigos e limitação de "usuários cadastradores", indicados oficialmente por dirigentes dos órgãos convenentes;

VII - Acompanhamento automatizado de volumetria: Implantado bloqueio automático para usuários que realizassem determinado número de consultas por hora ou acessos contínuos 24h/dia, eliminando padrões de uso automatizado e acessos robotizados;

VIII - Auditoria contínua: Equipe de compliance e auditoria com atuação contínua para detecção de incidentes de segurança e/ou vazamento de dados.

**c) Indicar se foi instaurada sindicância, processo administrativo disciplinar ou outro procedimento interno; encaminhar cópia dos atos de instauração e, se possível, relatórios conclusivos.**

**R:**
Esclarece-se que esta Diretoria não teve acesso a Inquérito Policial ou a eventuais ações judiciais relacionadas a incidentes de segurança de dados.

No que tange a instauração de sindicância, processo administrativo disciplinar ou outros procedimentos internos relacionados diretamente à incidentes de segurança de dados, caso recebida indicação de eventual envolvimento de servidores, o Ministério da Justiça e Segurança Pública adotará as providências necessárias para apuração.

**d) Especificar eventuais falhas técnicas identificadas e o plano de ação para sua correção, com prazos, responsáveis e metas.**

**R:**
De forma proativa e preventiva, e com base em uma avaliação contínua de risco e nas melhores práticas de segurança da informação, foram adotadas diversas providências que configuram um robusto plano de ação para aprimorar a resiliência dos sistemas. As medidas detalhadas no item "3.b" acima, como a autenticação Gov.br nível ouro, o duplo fator de autenticação, e os controles de acesso por IP, já fazem parte de um plano estratégico contínuo para fortalecer a segurança do Córtex.

Adicionalmente, e em uma iniciativa de **aprimoramento contínuo e acompanhamento dos avanços tecnológicos**, está em andamento um projeto de reestruturação completa da plataforma. Este novo sistema está sendo totalmente remodelado, incorporando uma nova geração de melhores práticas de segurança da informação, *compliance* e governança desde a sua concepção. A nova plataforma

representa um significativo salto qualitativo, adicionando camadas de proteção e otimização **às já existentes**, explorando as mais recentes tecnologias para oferecer um ambiente ainda mais seguro e eficiente. Este projeto reforça o compromisso do Ministério em prover um ambiente digital de ponta, sempre buscando a excelência em segurança e usabilidade.

**4) Coordenação Interinstitucional**

**a) Informar se houve comunicação formal à Controladoria-Geral da União (CGU), ao Gabinete de Segurança Institucional (GSI) e ao Tribunal de Contas da União (TCU) acerca do incidente, anexando ofícios, pareceres e respostas recebidas.**

**R:**
Os acesso suspeitos foram identificados pela auditoria da DIOPI/SENASP e encaminhados à Polícia Federal, órgão competente para averiguação de possíveis indícios de crimes. Essas análises tramitaram no âmbito de inquérito policial, de natureza sigilosa, por esse motivo, nenhum desdobramento das investigações foram acessados ou comunicados à integrantes da Senasp.

Não houve comunicação à CGU, TCU ou GSI, tendo em vista que a obrigatoriedade está na submissão ao controle e na prestação de contas, não na ação de "solicitar" a auditoria. As entidades sob a jurisdição do TCU e CGU têm o dever legal de manter a conformidade e a transparência de suas contas, que serão auditadas conforme os planos de ação e a legislação vigente, como a Lei nº 10.180/2001 (https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10180.htm) e as Normas de Auditoria do TCU (NAT) - link: https://pesquisa.apps.tcu.gov.br/documento/norma/*/KEY%253ANORMA-21550/score%2520desc/0.

**b) Descrever a interação com a Polícia Federal e demais órgãos de segurança para apuração dos fatos, indicando fluxos de cooperação e protocolos de compartilhamento de informações.**

**R:**
A DIOPI gerencia a Plataforma Córtex, tanto a parte de governança de dados e usuários, quanto as formalizações de acordos de cooperação técnica. Entre as suas funções de governança está a auditoria do uso da ferramenta, ou seja, as regras de uso e de negócios configuradas pelos técnicos nos códigos da Plataforma, assim que são violados ocorre a emissão de alertas automatizados aos auditores e o bloqueio do usuário ou da API responsável pelo possível uso irregular.
De posse dessas informações, os auditores fazem uma análise e questionamentos aos envolvidos para esclarecimentos. Caso as respostas não sejam satisfatórias, todo o procedimento é comunicado à Polícia Federal.

**c) Apresentar plano de reforço de segurança e governança elaborado em conjunto com CGU e GSI, se existente.**

**R:**
Não existe referido plano.

**5) Prevenção, Integridade e Transparência**

**a) Encaminhar cópia das normas internas, manuais e checklists de integridade e compliance digital aplicáveis aos usuários e operadores do Córtex.**

**R:**
A Plataforma Córtex foi instituída pela **Portaria nº 218, de 29 de setembro de 2021**, e atualmente passa por um processo de descontinuação, em virtude do desenvolvimento de uma nova ferramenta que será implementada em substituição.

Essa nova solução tecnológica busca assegurar maior segurança da informação, melhor rastreabilidade das ações dos usuários e ampliação dos mecanismos de controle e governança sobre o uso dos dados.

Deste modo, as normas internas, manuais e checklists de integridade e compliance digital da nova ferramenta estão em fase de elaboração.

**b) Informar as ações de capacitação ou sensibilização sobre ética e uso responsável de sistemas de inteligência realizadas em 2024–2025 (quantitativo, público-alvo, conteúdo e periodicidade).**

**R:**
Após a publicação do Acordo de Cooperação Técnica (ACT) com os respectivos órgãos convenentes, mediante a solicitação destes, são realizados treinamentos virtuais por meio da Plataforma Microsoft Teams, voltados aos pontos focais das instituições convenentes. Essas capacitações abrangem temas como:

a) Uso ético e responsável da Plataforma Córtex;

b) Níveis de acesso e procedimentos de auditoria.

| ***Quantidade*** | |
|---|---|
| ***Capacitações Solicitadas*** | ***Capacitações Realizadas*** |
| *58* | *58* |

**c) Descrever como se dá a publicidade ativa das informações sobre a gestão do Córtex, indicando os relatórios e dados abertos disponíveis (sem conteúdo sensível).**

**R:**
O Ministério da Justiça e Segurança Pública realiza a publicação dos Acordos de Cooperação Técnica – ACT no Diário Oficial e o acompanhamento pode ser feito por meio do link: https://www.gov.br/mj/pt-br/acesso-a-informacao/acts.
No cenário atual de reestruturação da Plataforma Córtex há a previsão de um sítio eletrônico com painéis BI, notícias e relatórios que acompanharão o dia a dia do uso e alcance da Plataforma.
Nesse estágio seus documentos são de acesso restrito, pois são documentos preparatórios que subsidiarão a decisão do Secretário Nacional de Segurança Pública – Senasp e do Ministro.

**d) Indicar se foi elaborado ou está em elaboração plano de melhoria de governança e segurança cibernética, com cronograma e responsáveis.**

**R:**
Assim como informado no quesito anterior, a Plataforma Córtex está em processo de descontinuação para dar lugar a nova Plataforma

Integrada. A Senasp, por meio da Diretoria de Operações Integradas e de Inteligência – DIOPI está em estágio avançado dessa evolução que trará as melhores tecnologias e práticas de governança e segurança cibernética. Devido ao caráter restrito dessas informações e detalhes, eles não podem ser descriminados, sem trazer prejuízos para a segurança do sistema, antes mesmo dele ser ativado.

**6) Supervisão e Auditoria Externa**

**a) Informar se o sistema Córtex foi objeto de auditorias pela CGU, TCU ou outros órgãos entre 2023 e 2025; encaminhar cópias dos relatórios, recomendações e planos de ação.**

**R:**
A Plataforma Córtex não foi objeto de auditorias pela CGU, TCU ou outros órgãos entre 2023 e 2025, pois em período algum houve a provocação ou interesse dessas instituições em realizar auditorias no sistema.

**b) Esclarecer quais recomendações foram implementadas e quais permanecem pendentes, com justificativas e prazos de cumprimento.**

**R:**
Tendo em vista que a Plataforma Córtex não foi submetida a auditorias pela CGU ou pelo TCU, não foi produzido nenhum relatório ou recomendação.

10. Na oportunidade, ressalta-se que a elaboração desta Informação tem como base a compilação das manifestações técnicas das subunidades desta Diretoria.

11. À consideração superior,

ANDRÉ LUIZ GOMES GALVÃO
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

SÉRGIO DO NASCIMENTO PEREIRA
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

HEITOR ROMERO BARBOSA LIMA DE OLIVEIRA
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

BRUNO RICARDO NUNES ROCHA
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

RAFAEL MOISES PENSO
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

ENYRA VIVIANI DO NASCIMENTO OLIVEIRA
Servidor Mobilizado
CSIOPI/CGINT/DIOPI/SENASP/MJSP

PAULO HENRIQUE DE ANDRADE PINTO
Servidor Mobilizado DIOP/SENASP

**DESPACHO CGINT**

Encaminhe-se à DIOPI para ciência e providências pertinentes.

ALEXANDRE FERREIRA DA SILVA
Coordenador de Sistemas de Inteligência e Operações Integradas
CSIOPI/CGINT/DIOPI/SENASP/MJSP

MARCUS VINICIUS DA SILVA DANTAS
Coordenador-Geral de Inteligência
CGINT/DIOPI/SENASP/MJSP

**DESPACHO**

Ciente e de acordo. Encaminhe-se ao Gabinete da Senasp para ciência e providências pertinentes.

RODNEY DA SILVA
Diretor de Operações Integradas e de Inteligência

Documento assinado eletronicamente por **Paulo Henrique de Andrade Pinto**, **Servidor(a) Mobilizado(a)**, em 04/11/2025, às 19:49, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RODNEY DA SILVA**, **Diretor(a) de Operações Integradas e de Inteligência**, em 04/11/2025, às 19:55, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Alexandre Ferreira da Silva**, **Coordenador(a) de Sistemas de Inteligência e Operações Integradas**, em 04/11/2025, às 19:57, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Andre Luiz Gomes Galvao**, **Servidor(a) Mobilizado(a)**, em 04/11/2025, às 20:01, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Heitor Romero Barbosa Lima de Oliveira**, **Servidor(a) Mobilizado(a)**, em 04/11/2025, às 20:23, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RAFAEL MOISES PENSO**, **Servidor(a) Mobilizado(a)**, em 04/11/2025, às 20:29, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **SÉRGIO DO NASCIMENTO PEREIRA**, **Servidor(a) Mobilizado(a)**, em 04/11/2025, às 20:48, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcus Vinicius da Silva Dantas**, **Coordenador(a)-Geral de Inteligência**, em 04/11/2025, às 23:50, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Enyra Viviani do Nascimento Oliveira**, **Servidor(a) Mobilizado(a)**, em 05/11/2025, às 08:52, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **BRUNO RICARDO NUNES ROCHA**, **Servidor(a) Mobilizado(a)**, em 05/11/2025, às 16:14, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **33616801** e o código CRC **BD53340C**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Referência:** Processo nº 08027.001535/2025-78 SEI nº 33616801

33619419 08027.001535/2025-78

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública

OFÍCIO Nº 11394/2025/GAB-SENASP/SENASP/MJ

Brasília, na data da assinatura.

Ao Senhor
MARIVALDO DE CASTRO PEREIRA
Secretário Nacional de Assuntos Legislativos
Ministério da Justiça e Segurança Pública
Brasília/DF

**Assunto: Requerimento n.º 6610/2025.**

Senhor Secretário,

Cumprimentando-o cordialmente, refiro-me ao Requerimento n.º 6610/2025 (33460318), datado de 21 de outubro de 2025, por meio do qual a Deputada Federal Adriana Ventura e outros, requer informações ao Ministério da Justiça e Segurança Pública sobre a governança, os controles de integridade, a segurança cibernética e as medidas corretivas adotadas no âmbito do sistema Córtex, em decorrência de sua utilização indevida por terceiros, inclusive por integrantes de organizações criminosas, conforme reportagens e investigações da Polícia Federal.

Nesse sentido, informo que as considerações desta Secretaria Nacional de Segurança Pública acerca do sistema Córtex, seguem colacionadas na Informação n.º 36 (33616801), na qual a área técnica, entre outros aspectos, enfrenta pontualmente aos questionamentos aduzidos pelos parlamentares.

Atenciosamente,

MARIO LUIZ SARRUBBO
Secretário Nacional de Segurança Pública

Documento assinado eletronicamente por **Mario Luiz Sarrubbo**, **Secretário(a) Nacional de Segurança Pública**, em 06/11/2025, às 19:36, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **33619419** e o código CRC **51415086**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Anexos:**
- Requerimento n.º 6610/2025 (33460318);
- Informação n.º 36 (33616801).

**Referência:** Caso responda este Ofício, indicar expressamente o Processo nº 08027.001535/2025-78 SEI nº 33619419

Esplanada dos Ministérios, Bloco T, Edifício Sede, sala 500, Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-9169 - https://www.justica.gov.br
Para responder, acesse http://sei.protocolo.mj.gov.br

33635127 08027.001535/2025-78

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Assuntos Legislativos
Área de Assessoria da Secretaria Nacional de Assuntos Legislativos

DESPACHO Nº 688/2025/ASSESSORIA-SAL/GAB-SAL/SAL

Destino: **Carlos Veras - Primeiro-Secretário da Câmara dos Deputados**
Assunto: **Requerimento de Informação Parlamentar nº 6610/2025**
Interessado**: Deputada Adriana Ventura (NOVO/SP) e Deputado Luiz Lima (NOVO/RJ)**

De ordem, encaminho à DIAPRO, para envio, ao Sr. Carlos Veras, Primeiro Secretário da Câmara dos Deputados, dos documentos abaixo listados, por intermédio do e-mail **ric.primeirasecretaria@camara.leg.br**

a) RIC nº 6610/2025, de autoria da Deputada Adriana Ventura (NOVO/SP) e do Deputado Luiz Lima (NOVO/RJ) (33460318);
b) OFÍCIO Nº 862/2025/Assessoria-SAL/GAB-SAL/SAL/MJ (33635074);
c) OFÍCIO Nº 11394/2025/GAB-SENASP/SENASP/MJ (33619419);
d) INFORMAÇÃO Nº 36/2025/DIOPI/SENASP (33616801), e
e) Anexo QTD ÓRGÃOS POR ESFERAS (33601911).

Atenciosamente,

Documento assinado eletronicamente por **Vivian Rodrigues Camara (PST)**, **Prestador(a) de Serviço - Apoio Administrativo**, em 08/12/2025, às 18:34, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **33635127** e o código CRC **07141882**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Referência:** Processo nº 08027.001535/2025-78 SEI nº 33635127

| Esfera | órgão | Qtd de Usuários Ativos (01/01/2024 a 30/09/2025) |
|---|---|---|
| ESTADUAL | BAVBM | 1 |
| | BOPE | 1 |
| | CABM | 7 |
| | CASA MILITAR | 7 |
| | CBM | 192 |
| | CICC | 5 |
| | CICCE | 7 |
| | Corregedoria Geral | 1 |
| | CPC | 42 |
| | CPCHQ | 12 |
| | CPM | 23 |
| | CRBM | 73 |
| | CRPO AJ | 11 |
| | CRPO CENTRAL | 6 |
| | CRPO CS | 7 |
| | CRPO FNO | 14 |
| | CRPO FO | 38 |
| | CRPO LITORAL | 19 |
| | CRPO MISSÕES | 14 |
| | CRPO PLANALTO | 51 |
| | CRPO SERRA | 73 |
| | CRPO SUL | 19 |
| | CRPO VC | 11 |
| | CRPO VRP | 72 |
| | CRPO VRS | 72 |
| | CRPO VT | 4 |
| | DEFESA CIVIL | 1 |
| | DETRAN | 12 |
| | DI | 1 |
| | DIEP | 10 |
| | IGP | 3 |
| | INTELIGÊNCIA | 1 |
| | MB | 1 |
| | MINISTÉRIO PÚBLICO | 380 |
| | PC | 7312 |
| | PERÍCIA | 7 |
| | PM | 19366 |
| | POL TÉCNICA/CIENTÍFICA | 40 |
| | POLíCIA CIVIL | 10 |
| | POLÍCIA PENAL | 38 |
| | POLÍCIA TÉCNICA | 1 |
| | SDS/PE | 54 |
| | SEAP | 19 |
| | SEC EST SEG PÚBLICA | 20 |
| | SECRETARIA DE SEGURANÇA SJP | 25 |
| | SECRETARIA ESTADUAL DA CASA CIVIL | 21 |
| | SEFAZ | 54 |
| | SEJUSP | 57 |
| | SESDEC | 5 |
| | SESED | 1 |
| | SESP | 7 |
| | SIST PENITENCIÁRIO | 1 |
| | SSP | 2432 |
| | SSPDS | 15 |
| | TRE | 21 |

| | | |
|---|---|---|
| **ESTADUAL Total** | | **30697** |
| FEDERAL | ABIN | 2 |
| | ADMINISTRAÇÃO PÚBLICA | 9 |
| | ANTT | 6 |
| | CIODS | 1 |
| | CIOF | 24 |
| | CNJ | 52 |
| | CORREIOS | 1 |
| | DEPEN | 35 |
| | DINT | 19 |
| | DIOPI/SENASP | 47 |
| | DNIT | 1 |
| | DTIC/MJSP | 5 |
| | EB | 103 |
| | FAB | 6 |
| | FNSP | 1 |
| | FORÇA NACIONAL | 50 |
| | FORÇA NACIONAL PERITO CRIMINAL | 1 |
| | GSI | 3 |
| | IBAMA | 3 |
| | MARINHA DO BRASIL | 24 |
| | MD | 24 |
| | MINISTERIO DA SAUDE | 1 |
| | MINISTÉRIO PÚBLICO DO TRABALHO | 2 |
| | MJSP | 91 |
| | MPE | 327 |
| | MPM | 4 |
| | PETROBRAS | 1 |
| | PF | 2130 |
| | POLÍCIA FEDERAL | 1 |
| | PRF | 1842 |
| | RECEITA FEDERAL | 139 |
| | SENASP | 9 |
| | SENATRAN | 1 |
| | TSE | 8 |
| **FEDERAL Total** | | **4973** |
| MUNICIPAL | GUARDA MUNICIPAL | 2977 |
| | GUARDA PORTUÁRIA | 18 |
| | ORG. MUNICIPAL DE TRÂNSITO | 26 |
| | PREFEITURA MUNICIPAL | 123 |
| | SEC MUN SEG PÚBLICA | 233 |
| | SEC MUN TRÂNSITO | 191 |
| | SECRETARIA MUNICIPAL DE DEFESA SOCIAL | 16 |
| | SECRETARIA MUNICIPAL DE ORDEM PúBLICA | 3 |
| | SMTT | 4 |
| **MUNICIPAL Total** | | **3591** |
| **Total de Usuários Ativos no Período.** | | **39261** |

**REQUERIMENTO DE INFORMAÇÃO Nº , DE 2025**

(Da Sra. Adriana Ventura e outros)

Requer informações ao Ministro de Estado da Justiça e Segurança Pública, Sr. Ricardo Lewandowski, sobre a governança, os controles de integridade, a segurança cibernética e as medidas corretivas adotadas no âmbito do sistema Córtex, em decorrência de sua utilização indevida por terceiros, inclusive por integrantes de organizações criminosas, conforme reportagens e investigações da Polícia Federal.

Senhor Presidente,

Com fundamento no art. 50, §2º, da Constituição Federal, e nos 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. Ricardo Lewandowski, o presente Requerimento de Informação, a fim de que sejam prestados esclarecimentos e fornecida documentação oficial sobre a gestão, integridade e segurança do sistema Córtex, incluindo logs de acesso, fluxos de governança, controles de auditoria e medidas de prevenção a usos indevidos.

Requer-se que as respostas sejam apresentadas item a item, acompanhadas dos documentos comprobatórios em formato pesquisável (OCR), com referência a número de processo/SEI e controle de versão.

**1) Estrutura e Governança do Sistema**

a) Encaminhar organograma atualizado das unidades responsáveis pela gestão, operação e auditoria do sistema Córtex, indicando competências, chefias e vínculos hierárquicos.

b) Descrever a arquitetura de governança aplicada ao Córtex (normas internas, fluxos de decisão, instâncias de supervisão e auditoria).

c) Informar a data e conteúdo das últimas revisões de políticas internas de acesso, controle e integridade do sistema.

**2) Controle de Acesso e Rastreabilidade**

a) Descrever os mecanismos de autenticação, logs e trilhas de auditoria implementados, incluindo retenção, revisão e cruzamento de registros de acesso.

b) Informar o número total de perfis de acesso ativos entre 01/01/2024 e 30/09/2025, discriminando por tipo de órgão conveniado (federal, estadual, municipal).

c) Encaminhar relatório (ou amostra representativa) de logs de acesso auditados que tenham identificado consultas atípicas ou indevidas, suprimindo dados pessoais e sigilosos.

d) Informar a frequência e metodologia de auditoria interna de acessos, bem como as instâncias que analisam os resultados e determinam providências.

**3) Incidente de Segurança e Medidas Corretivas**

a) Informar a data de detecção da invasão ou uso indevido do Córtex e os principais achados da investigação da Polícia Federal até o momento, limitando-se a informações passíveis de publicidade.

b) Descrever as medidas emergenciais adotadas pelo Ministério para suspender, conter e revisar os acessos indevidos, inclusive bloqueio de credenciais, revisão de perfis e atualização de protocolos.

c) Indicar se foi instaurada sindicância, processo administrativo disciplinar ou outro procedimento interno; encaminhar cópia dos atos de instauração e, se possível, relatórios conclusivos.

d) Especificar eventuais falhas técnicas identificadas e o plano de ação para sua correção, com prazos, responsáveis e metas.

**4) Coordenação Interinstitucional**

a) Informar se houve comunicação formal à Controladoria-Geral da União (CGU), ao Gabinete de Segurança Institucional (GSI) e ao Tribunal de Contas da União (TCU) acerca do incidente, anexando ofícios, pareceres e respostas recebidas.

b) Descrever a interação com a Polícia Federal e demais órgãos de segurança para apuração dos fatos, indicando fluxos de cooperação e protocolos de compartilhamento de informações.

c) Apresentar plano de reforço de segurança e governança elaborado em conjunto com CGU e GSI, se existente.

**5) Prevenção, Integridade e Transparência**

a) Encaminhar cópia das normas internas, manuais e checklists de integridade e compliance digital aplicáveis aos usuários e operadores do Córtex.

b) Informar as ações de capacitação ou sensibilização sobre ética e uso responsável de sistemas de inteligência realizadas em 2024–2025 (quantitativo, público-alvo, conteúdo e periodicidade).

c) Descrever como se dá a publicidade ativa das informações sobre a gestão do Córtex, indicando os relatórios e dados abertos disponíveis (sem conteúdo sensível).

d) Indicar se foi elaborado ou está em elaboração plano de melhoria de governança e segurança cibernética, com cronograma e responsáveis.

**6) Supervisão e Auditoria Externa**

a) Informar se o sistema Córtex foi objeto de auditorias pela CGU, TCU ou outros órgãos entre 2023 e 2025; encaminhar cópias dos relatórios, recomendações e planos de ação.

b) Esclarecer quais recomendações foram implementadas e quais permanecem pendentes, com justificativas e prazos de cumprimento.

**JUSTIFICAÇÃO**

Reportagens[1][2][3] noticiaram que a Polícia Federal identificou uso indevido do sistema Córtex, ferramenta de inteligência artificial sob responsabilidade do Ministério da Justiça e Segurança Pública, inclusive por membros de organizações criminosas, com o propósito de monitorar autoridades públicas, como juízes, promotores e parlamentares.

As matérias indicam falhas de controle de acesso, vulnerabilidades de segurança e insuficiente rastreabilidade de logs, com potencial violação de sigilos e risco à integridade de dados públicos sensíveis.

Considerando o dever de fiscalização do Poder Legislativo e o princípio da transparência na gestão de sistemas estratégicos da administração pública, é imprescindível que esta Casa obtenha informações detalhadas sobre a governança, segurança e integridade do sistema Córtex, bem como sobre as medidas adotadas para corrigir falhas e prevenir novos incidentes.

As informações ora requeridas visam assegurar a responsabilização administrativa, a prevenção de riscos cibernéticos e o fortalecimento da confiança institucional nos sistemas de inteligência do Estado, em estrita observância aos princípios da eficiência, da legalidade e da moralidade administrativa.

Sala das Sessões, em de outubro de 2025.

Deputada **ADRIANA VENTURA**
NOVO - SP

[1] https://www.gazetadopovo.com.br/brasil/pf-expoe-nova-invasao-cortex-ia-espia-do-governo-federal-e-uso-pelo-pcc-para-monitorar-moro-promotor-stf/
[2] https://www.gazetadopovo.com.br/brasil/repercussao-reportagem-gazeta-do-povo-kataguiri-convocacao-lewandowski-vazamento-ia-espia/
[3] https://www.band.com.br/noticias/jornal-da-band/ultimas/pf-investiga-uso-de-sistema-do-ministerio-da-justica-por-membros-do-pcc-202509202001

# Requerimento de Informação

## Deputado(s)

1 Dep. Adriana Ventura (NOVO/SP)
2 Dep. Luiz Lima (NOVO/RJ)