REQUERIMENTO DE INFORMAÇÃO Nº , DE 2026

(Da Sra. Adriana Ventura)

Requer informações ao Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, Sr. Marcos Antonio Amaro dos Santos, sobre governança cibernética, conformidade normativa, gestão de incidentes e medidas adotadas pelo GSI/PR e pelo CTIR Gov diante de possíveis acessos indevidos a sistemas e informações sensíveis da administração pública federal.

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 Chefe do Gabinete de Segurança Institucional da Presidência da República, Sr. Marcos Antonio Amaro dos Santos, o presente Requerimento de Informação, a fim de que sejam prestados os esclarecimentos e encaminhados os documentos oficiais abaixo especificados acerca da atuação administrativa do Gabinete de Segurança Institucional da Presidência da República, inclusive por sua Secretaria de Segurança da Informação e Cibernética e pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, em relação à governança cibernética, à conformidade normativa, à coordenação interinstitucional, à gestão de incidentes e às medidas adotadas diante de possíveis acessos indevidos a sistemas, bases de dados, documentos e informações sensíveis da administração pública federal,

noticiados publicamente no âmbito da Operação Compliance Zero e do caso Banco Master.

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. Conhecimento institucional e abertura de acompanhamento

Informar se o GSI/PR, a Secretaria de Segurança da Informação e Cibernética, o Departamento de Segurança Cibernética, o CTIR Gov ou qualquer outra unidade vinculada ao Gabinete abriu processo administrativo, registro de acompanhamento, triagem técnica, análise preliminar, monitoramento ou qualquer outra forma de acompanhamento institucional em razão dos fatos noticiados publicamente no âmbito da Operação Compliance Zero e do caso Banco Master.

Em caso positivo, informar:

a) data do primeiro registro;

b) unidade responsável;

c) autoridade que determinou a providência;

d) número do processo SEI;

e) objeto do acompanhamento;

f) providências inicialmente adotadas.

Em caso negativo, informar qual autoridade deliberou pela não abertura de acompanhamento e qual a motivação administrativa correspondente.

2. Ausência de comunicação de incidente e providências adotadas

Considerando que a resposta ao RIC nº 6609/2025 afirmou reiteradamente que não houve comunicação de incidente, informar se o GSI/PR adotou alguma providência para verificar:

a) por que não houve notificação ao CTIR Gov;

b) se o órgão gestor do sistema avaliou formalmente a ocorrência como não notificável;

c) se houve descumprimento de fluxos, orientações ou deveres de comunicação no âmbito da ReGIC;

d) se a ausência de comunicação motivou recomendação corretiva, orientação formal ou apuração administrativa.

Em caso positivo, encaminhar os documentos correspondentes. Em caso negativo, justificar expressamente.

3. Conformidade do MJSP com a estrutura obrigatória de segurança da informação

Informar se, após a publicização do caso, o GSI/PR verificou ou solicitou informações ao MJSP quanto à conformidade com a Instrução Normativa GSI nº 1/2020, especialmente no que se refere a:

a) existência e atualização de Política de Segurança da Informação;

b) designação de Gestor de Segurança da Informação;

c) instituição de Comitê de Segurança da Informação ou estrutura equivalente;

d) existência e funcionamento de ETIR;

e) adoção dos controles gerais de segurança da informação expedidos pelo GSI.

Em caso positivo, encaminhar checklists, relatórios, notas técnicas, ofícios ou despachos correspondentes. Em caso negativo, justificar expressamente.

4. Atuação do CTIR Gov e da ReGIC no caso concreto

Informar se o CTIR Gov recebeu, desde 1º de janeiro de 2024, qualquer notificação, alerta, pedido de apoio ou comunicação correlata proveniente do MJSP, da Polícia Federal ou de outro órgão federal em relação a fatos potencialmente associados aos noticiados no âmbito da Operação Compliance Zero e do caso Banco Master.

Em caso positivo, informar, de forma consolidada:

a) quantidade de notificações;

b) órgãos remetentes;

c) classificação do incidente;

d) providências adotadas;

e) eventual acionamento de ETIRs;

f) eventual articulação no âmbito da ReGIC.

Em caso negativo, informar se houve registro formal dessa ausência e se foram adotadas providências perante os órgãos potencialmente responsáveis pela notificação.

5. Alertas, orientações e recomendações específicas

Informar se, diante dos fatos noticiados publicamente, o GSI/PR ou o CTIR Gov expediu alertas, orientações, recomendações, comunicados técnicos ou pedidos de verificação dirigidos ao MJSP ou a outros órgãos da administração pública federal, inclusive quanto a:

a) revisão de logs;

b) revisão extraordinária de acessos;

c) recadastramento;

d) suspensão preventiva de credenciais;

e) revisão de integrações;

f) verificação de conformidade;

g) reforço de autenticação e segregação de perfis.

Em caso positivo, encaminhar a relação dos documentos expedidos. Em caso negativo, justificar expressamente.

6. Critérios para enquadramento como infraestrutura crítica e alcance do monitoramento

Considerando que a resposta ao RIC nº 6609/2025 informou que o sistema Córtex não integra o rol de infraestruturas críticas monitoradas pelo GSI, informar:

a) quais critérios técnicos, normativos e institucionais são utilizados para esse enquadramento;

b) qual unidade realizou a classificação ou confirmou a não classificação do Córtex;

c) se outros sistemas federais potencialmente sensíveis relacionados aos fatos noticiados são ou não monitorados pelo GSI sob esse regime;

d) se, após a repercussão pública do caso, houve revisão desses critérios ou da classificação atribuída ao Córtex ou a outros sistemas.

7. Coordenação interinstitucional após a repercussão pública

Informar se houve comunicação, reunião, despacho, ofício, troca de informações ou qualquer articulação administrativa entre o GSI/PR e o MJSP, a Polícia Federal, a Controladoria-Geral da União, a Casa Civil, o Tribunal de Contas da União ou outros órgãos federais em razão da repercussão pública do caso, ainda que não tenha havido notificação formal de incidente.

Em caso positivo, informar:

a) data;

b) unidade remetente e destinatária;

c) autoridade subscritora;

d) processo SEI;

e) objeto;

f) documentos encaminhados ou recebidos.

Em caso negativo, indicar expressamente a autoridade que deliberou pela não articulação e a respectiva motivação administrativa.

8. Avaliação interna do GSI/PR sobre sua própria atuação

Informar se o GSI/PR instaurou apuração preliminar, revisão de procedimentos, post-mortem, avaliação formal de risco, tomada de subsídios ou qualquer outro procedimento interno para avaliar a suficiência de seus fluxos de coordenação, de suas rotinas de recebimento de notificação e de sua atuação institucional diante dos fatos noticiados publicamente.

Em caso positivo, encaminhar os atos de instauração, a fase procedimental e, quando possível, extrato consolidado ou versão parcialmente tarjada. Em caso negativo, indicar expressamente a autoridade que deliberou pela não instauração e a motivação correspondente.

9. Medidas estruturantes e aperfeiçoamentos pós-caso

Informar se, após a publicização dos fatos, o GSI/PR adotou, propôs ou estudou medidas estruturantes para fortalecimento da governança cibernética federal, inclusive quanto a:

a) atualização de fluxos de notificação;

b) revisão da atuação da ReGIC;

c) aperfeiçoamento das orientações para comunicação de incidentes ao CTIR Gov;

d) reforço de exigências de conformidade dos órgãos;

e) campanhas, capacitações ou alertas setoriais;

f) revisão de requisitos para sistemas sensíveis ou que tratem informações sigilosas.

Em caso positivo, encaminhar atos, cronogramas, minutas, notas técnicas e planos de ação. Em caso negativo, justificar expressamente.

JUSTIFICAÇÃO

A apresentação do presente Requerimento de Informação decorre da necessidade de apurar, na esfera administrativa do Gabinete de Segurança Institucional da Presidência da República, se houve comunicação formal, coordenação interinstitucional, verificação de conformidade normativa, gestão de incidentes e adoção de providências estruturantes diante de fatos noticiados publicamente acerca de possíveis acessos indevidos a sistemas, documentos e informações sensíveis da administração pública federal. O recorte é compatível com as competências legais e regulamentares do GSI/PR, ao qual cabe planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal. Também se inserem nesse âmbito a atuação do CTIR Gov e a coordenação da Rede Federal de Gestão de Incidentes Cibernéticos – ReGIC.

A resposta encaminhada pelo GSI/PR ao RIC nº 6609/2025 reconheceu expressamente sua competência normativa e coordenadora, mas afirmou que:

- a execução das medidas de segurança, a gestão de riscos e a implementação dos controles cabem ao órgão gestor do sistema;
- o Córtex não integra o rol de infraestruturas críticas monitoradas pelo GSI;

- não houve comunicação de incidente;
- não houve auditorias, pentests ou avaliações de conformidade em sistemas do MJSP realizados diretamente ou sob sua supervisão; e
- não houve coordenação interinstitucional, revisão de protocolos, comunicação institucional específica ou previsão de relatório público sobre o caso, justamente em razão da ausência de notificação.

Além disso, o próprio GSI informou que não existe instrumento de avaliação de riscos cibernéticos do Governo Federal como um todo e que a gestão de vulnerabilidades e inventário de ativos é processo interno do órgão responsável pelo ativo. Ao mesmo tempo, o marco normativo expedido pelo próprio GSI determina aos órgãos e entidades federais a designação de gestor de segurança da informação, a instituição de comitê ou estrutura equivalente, a implementação de ETIR e a observância obrigatória dos controles gerais de segurança da informação. A resposta anterior, contudo, não esclareceu se o GSI verificou a conformidade do MJSP com essas exigências nem se apurou a razão da ausência de notificação ao CTIR Gov.

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. 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

[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
[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

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.

Diante desse contexto, cumpre verificar se o GSI/PR, mesmo diante da ausência de notificação formal, adotou alguma providência para aferir conformidade normativa, apurar a razão da não comunicação, orientar os órgãos potencialmente afetados, fortalecer os fluxos de coordenação e avaliar a suficiência da estrutura federal de gestão de incidentes cibernéticos. O objetivo do presente requerimento é, portanto, obter informações objetivas e documentais sobre a atuação administrativa do GSI/PR, sem avançar sobre conteúdo protegido por sigilo investigativo ou sobre matérias estranhas à competência do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

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)