

## AO MINISTÉRIO PÚBLICO JUNTO AO TRIBUNAL DE CONTAS DA UNIÃO

**ERIKA HILTON**, brasileira, ativista de direitos humanos, vereadora no Município de São Paulo, [REDACTED]

[REDACTED] vêm, respeitosamente, com fundamento no art. 62, do Regimento Interno do Tribunal de Contas da União, comunicar **RELATO DE IRREGULARIDADE** referente à notícia do apagão dos computadores instalados no Palácio do Planalto.

01. Na data de hoje (11.11.2022), por meio de matéria exclusiva da Coluna de Rodrigo Rangel, da rede jornalística Metrôpoles, foi divulgada a notícia de que os computadores instalados no Palácio do Planalto, sede do Poder Executivo Federal brasileiro, tiveram seu conteúdo inteiramente deletado. Segundo a matéria, os funcionários da área de informática do Planalto dizem que o sistema antivírus da rede da Presidência da República “detectou uma ameaça” e que essa foi a motivação para promover o apagamento dos dados constantes nas máquinas.

02. Importante lembrar que esta ação surge na esteira de outros acontecimentos de escala nacional que mostram o interesse da atual gestão da Presidência da República em esconder dados relevantes sobre o governo e sobre potenciais irregularidades praticadas nos últimos quatro anos. Cita-se como exemplo o Decreto Federal nº 9.690/2019 que, logo no início da gestão presidencial, ampliou o número de autoridades que podem definir informações como sigilosas<sup>1</sup>; o sigilo imposto pelo Presidente da República nas reuniões feitas com pastores investigados pelo repasse ilegal de recursos do Ministério da Educação, o que gerou até mesmo um posicionamento do Supremo Tribunal Federal<sup>2</sup>; e o sigilo imposto pelo Ministério da Saúde aos contratos referentes à aquisição da vacina Covaxin, derrubado pela justiça em agosto de 2021<sup>3</sup>.

03. Estes comportamentos absolutamente suspeitos adotados pelo alto escalão da Presidência da República, vale lembrar, têm sido repreendidos pela Controladoria-Geral da União, que reage negativamente à imposição de sigilo nas situações apresentadas,

<sup>1</sup> Para mais, ver: Diário Oficial da União, de 24 de janeiro de 2019.

<sup>2</sup> Para mais, ver: STF, ADPF 961/DF, rel. Ministro André Mendonça, j. 01 de junho de 2022.

<sup>3</sup> Para mais, ver: Justiça Federal, Seção Judiciária do Distrito Federal, 2ª Vara Federal Cível da SJDF, Processo nº 1057367-47.2021.4.01.3400, Mandado de segurança cível, rel. Anderson Santos da Silva, j. 26 de agosto de 2021.

como consta nos Pareceres nº 395/2021/CGRAI/OGU/CGU<sup>4</sup> e 241/2021/CGRAI/OGU/CGU<sup>5</sup>.

04. Para a situação atual do apagamento dos computadores, não se tem notícia da existência de algum *framework* que oriente o apagamento integral dos dados virtuais, em caso de detectada alguma ameaça externa no sistema operacional de um órgão público. Em sentido oposto, a Norma Técnica ABNT NBR ISO/IEC 27002:2005 e o próprio Tribunal de Contas da União, por meio de uma série de acórdãos, recomendam a criação de cópias de segurança de documentos oficiais que estejam sob ameaça de qualquer natureza.

05. Até o momento, não houve nenhum posicionamento oficial advindo do Palácio do Planalto a respeito da denúncia.

06. Em 2012, o Tribunal de Contas da União, por meio de sua Secretaria de Fiscalização de Tecnologia da Informação, produziu o relatório "*Boas práticas em segurança da informação*", onde consta uma série de orientações a respeito dos aspectos da segurança da informação nas instituições governamentais. A partir de julgados da Corte de Contas, o referido material fornece diretrizes para gerenciamento dos dados da própria Presidência da República, com orientações relacionadas à proteção contra códigos maliciosos e móveis, cópias de segurança, gerenciamento da segurança em redes e monitoramento. Eis alguns dos julgados referenciados no relatório de boas práticas em segurança da informação e que tratam do tema em comento nesta petição:

**(I)**

1.4.2.8. defina e formalize uma política de cópias de segurança (backups) que inclua o código-fonte e a base de dados do [Sistema] com base nas necessidades de negócio do [Programa de Governo], incluindo procedimentos regulares de recuperação e observando as recomendações contidas no item 10.5.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

1.4.2.9. considerando a necessidade de proteger o sigilo das informações (...), avalie a conveniência de criptografar os dados gravados nas mídias das cópias de segurança do [Sistema], conforme recomenda a diretriz para implementação “h” do item 10.5.1 da Norma Técnica ABNT NBR ISO/ IEC 27002:2005;

(Acórdão 1.137/2012, 2ª Câmara do TCU)

**(II)**

---

<sup>4</sup> Para mais, ver: CGU, Processo nº 00137.003633/2021-67, rel. Waldir Gomes Dias. Disponível em: <<https://static.poder360.com.br/2022/04/parecer-CGU.pdf>>. Acesso em 11 de novembro de 2022.

<sup>5</sup> Para mais, ver: CGU, Processo nº00137.022808/2020-54, rel. Fabiana Nepomuceno da Cunha. Disponível em: <<https://static.poder360.com.br/2022/04/parecer-CGU-2.pdf>>. Acesso em 11 de novembro de 2022.

9.2. (...) elabore e implante uma Política de Cópias de Segurança na Coordenação-Geral de Modernização e Informática em conformidade com as necessidades do negócio e com o Plano de Continuidade de Negócio a ser elaborado pelo órgão, em consonância com as orientações contidas na NBR ISO/IEC 17799:2005, item 10.5.1 - Cópia de segurança das informações e no Cobit 4.1, item DS11.5 - Backup e restauração;  
(Acórdão 1.382/2009, Plenário do TCU)

### (III)

9.4.7. elabore e implante uma Política de Cópias de Segurança, no âmbito da Coordenação-Geral de Informática e Telecomunicações (...), em conformidade com as necessidades do negócio, com o Plano de Continuidade de Negócio a ser elaborado pelo órgão e com as orientações contidas no item 10.5.1 da NBR ISO/IEC 17799:2005 e no item DS11.5 do Cobit 4.1 (Backup e restauração);  
(Acórdão 669/2008, Plenário do TCU)

### (IV)

9.2.15. formalize política de geração de cópias de segurança para o [Sistema], de acordo com o previsto no item 10.5.1 da NBR ISO/IEC 17799:2005; 9.2.16. armazene as mídias contendo cópias de segurança do [Sistema] em local diverso da operação do sistema, de acordo com a diretriz “d” do item 10.5.1 da NBR ISO/IEC 17799:2005;  
(Acórdão 71/2007, Plenário do TCU)

07. Em outra oportunidade, **o Tribunal também já havia repassado recomendações ao próprio Gabinete de Segurança Institucional da Presidência da República**, no sentido de criar um sistema de segurança da informação eficiente, conforme:

“9.6.1. crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa (...)”.  
(TCU, Acórdão 2471/2008 - Plenário, Ata 46, TC 019.230/2007-2, Relator Ministro Benjamin Zymler, Sessão 05/11/2008, DOU 07/11/2008).

08. Como se vê, a Presidência da República está, há pelo menos uma década, recebendo orientações bastante precisas da Corte de Contas quanto à necessidade de manter uma política de segurança da informação na gestão do Estado brasileiro. Entre as orientações recebidas, muitas delas se relacionam com a importância de criar cópias de segurança (*backup*), como modo de prevenção a eventuais ataques externos e ameaças virtuais.

09. Mesmo diante dessas orientações, a atual gestão da Presidência da República parece abandonar deliberadamente seus compromissos institucionais, colocando interesses pessoais à frente do interesse público e do princípio constitucional à publicidade da atividade governamental.

10. Diante do exposto, é a presente para requerer a abertura de inquérito no Ministério Público de Contas do Tribunal de Contas da União, com a finalidade de:

- a) Intimar a Secretaria-Geral da Presidência e os departamentos de tecnologia a ela vinculados, para que prestem esclarecimentos a respeito do tema, apresentando sua Política de Segurança da Informação;
- b) Investigar as alegações referentes ao apagão dos computadores instalados no Palácio do Planalto, bem como a autenticidade do argumento apresentado pelos técnicos do Poder Executivo, que alegaram, como motivação para a conduta, a existência de ameaças virtuais;
- c) Investigar a autoria da ordem operacional para eliminação dos dados nos computadores do Palácio do Planalto;
- d) Apurar o cumprimento das regras e orientações relativas à segurança da informação, por parte dos servidores públicos envolvidos na situação narrada neste documento, notadamente quanto aquelas constantes no relatório "*Boas práticas em segurança da informação*", elaborado pela Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União, em 2012;
- e) Avaliar a responsabilidade administrativa dos gestores públicos envolvidos na irregularidade narrada neste documento, com a apresentação de recomendações aos órgãos do Poder Executivo Federal; e
- f) Enviar às autoridades competentes, sobretudo o Ministério Público Federal, as provas e informações eventualmente obtidas pelo MP-TCU sobre a denúncia apresentada neste documento, para apuração da responsabilidade civil e penal dos gestores públicos envolvidos.

De São Paulo para Brasília, 11 de novembro de 2022.

**ERIKA HILTON**