SENADO FEDERAL

REQUERIMENTO Nº DE

Requer que sejam prestadas, pelo Senhor Ministro de Estado da Integração e do Desenvolvimento Regional, Waldez Góes, informações acerca de providências adotadas diante do incidente cibernético ocorrido na madrugada do dia 20 de junho de 2026, com envio indevido de mensagem para milhares de pessoas no País, classificada como "Alerta Extremo" pelo sistema Defesa Civil Alerta, acompanhada do sinal sonoro característico desse nível de emergência e contendo a palavra "misantropi4".

Senhor Presidente,

Requeiro, nos termos do art. 50, § 2º, da Constituição Federal e dos arts. 216 e 217 do Regimento Interno do Senado Federal, que sejam prestadas, pelo Senhor Ministro de Estado da Integração e do Desenvolvimento Regional, Waldez Góes, informações acerca de providências adotadas diante do incidente cibernético ocorrido na madrugada do dia 20 de junho de 2026, com envio indevido de mensagem para milhares de pessoas no País, classificada como "Alerta Extremo" pelo sistema Defesa Civil Alerta, acompanhada do sinal sonoro característico desse nível de emergência e contendo a palavra "misantropi4".

Nesses termos, requisita-se:

I – DO INCIDENTE E DAS PROVIDÊNCIAS INICIAIS

1. Apresente cronologia detalhada do incidente, indicando:

a) a data e o horário em que ocorreu o envio da mensagem indevida;

b) o momento em que a Secretaria Nacional de Proteção e Defesa Civil tomou conhecimento dos fatos;

c) as providências adotadas imediatamente após a identificação do incidente;

d) a data e o horário da suspensão preventiva do sistema Defesa Civil Alerta; e

e) as medidas emergenciais implementadas para contenção do incidente.

2. Informe quais unidades administrativas do Ministério e da Secretaria Nacional de Proteção e Defesa Civil participaram da resposta inicial ao incidente, especificando as respectivas atribuições.

3. Informe quais órgãos e entidades federais passaram a integrar a apuração dos fatos e a resposta governamental ao incidente.

II – DO FUNCIONAMENTO DO SISTEMA DEFESA CIVIL ALERTA

4. Descreva a arquitetura funcional do sistema Defesa Civil Alerta, indicando:

a) sua finalidade institucional;

b) os órgãos autorizados a emitir alertas;

c) os níveis de classificação das mensagens;

d) os fluxos de autorização para emissão de alertas; e

e) os mecanismos de autenticação atualmente utilizados.

5. Informe quais tecnologias são utilizadas para transmissão das mensagens à população, especificando a utilização da tecnologia **Cell Broadcast** e outras eventualmente empregadas.

6. Informe quais mecanismos impedem a emissão não autorizada de mensagens classificadas como **"Alerta Extremo"**, indicando se existe:

a) autenticação multifator;

b) dupla validação operacional;

c) segregação de perfis de acesso;

d) registro obrigatório de auditoria; e

e) outros controles preventivos.

III – DA SEGURANÇA CIBERNÉTICA E DA GOVERNANÇA

7. Informe, em caráter preliminar, quais são as hipóteses técnicas atualmente consideradas para explicar o incidente, indicando se existem indícios de:

a) ataque cibernético externo;

b) exploração de vulnerabilidade tecnológica;

c) comprometimento de credenciais;

d) falha operacional;

e) erro humano; ou

f) outra hipótese em investigação.

8. Informe se foram identificados indícios de comprometimento da infraestrutura tecnológica utilizada pelo sistema ou de quaisquer de seus ambientes computacionais.

9. Informe se o sistema Defesa Civil Alerta integra formalmente o rol de infraestruturas críticas da União ou se possui classificação equivalente em razão de sua relevância para a proteção da população.

10. Informe se, antes do incidente ocorrido em 20 de junho de 2026, esse Ministério, a Secretaria Nacional de Proteção e Defesa Civil ou quaisquer órgãos vinculados receberam comunicações, auditorias, alertas técnicos, relatórios de vulnerabilidade, notificações, recomendações ou quaisquer outras informações relativas a riscos envolvendo o sistema Defesa Civil Alerta ou sua infraestrutura tecnológica.

Em caso positivo, informar:

a) a origem do alerta;

b) a data do recebimento;

c) a classificação do risco apontado;

d) as providências adotadas;

e) eventual comunicação aos demais órgãos competentes; e

f) os motivos pelos quais eventual vulnerabilidade permaneceu existente.

11. Informe se existe Política formal de Segurança da Informação aplicável ao sistema Defesa Civil Alerta, encaminhando cópia dos normativos de caráter ostensivo atualmente vigentes.

12. Informe se existem Plano de Continuidade de Negócios, Plano de Recuperação de Desastres, Plano de Resposta a Incidentes Cibernéticos ou instrumentos equivalentes aplicáveis ao sistema, indicando a data de sua última atualização.

13. Informe quando foram realizados:

a) a última auditoria de segurança da informação;

b) o último teste de intrusão (*penetration test*);

c) a última avaliação independente de vulnerabilidades;

d) a última revisão dos perfis de acesso administrativo; e

e) as principais recomendações formuladas nessas avaliações e o estágio de implementação de cada uma delas.

IV – DAS CONTRATAÇÕES, DESENVOLVIMENTO E MANUTENÇÃO DO SISTEMA

14. Informe quais empresas, consórcios ou entidades participaram do desenvolvimento, implantação, integração, manutenção, suporte técnico, hospedagem, operação ou evolução tecnológica do sistema Defesa Civil Alerta, indicando:

a) o objeto de cada contratação;

b) o período de vigência;

c) os respectivos valores contratados; e

d) a forma de contratação.

15. Informe quais mecanismos de fiscalização contratual, auditoria e controle de desempenho são adotados pelo Ministério para acompanhamento da execução desses contratos.

16. Informe se, após o incidente, foi determinada auditoria extraordinária sobre a plataforma tecnológica, os contratos vigentes ou os fornecedores envolvidos, especificando o escopo da apuração.

V – DOS IMPACTOS DO INCIDENTE

17. Informe a estimativa oficial do número de pessoas potencialmente impactadas pelo envio indevido da mensagem, bem como a correspondente

estimativa do número de aparelhos celulares que receberam o alerta, discriminando a metodologia utilizada para esses cálculos.

18. Informe a abrangência territorial do incidente, discriminando:

a) os Estados atingidos;

b) os Municípios atingidos;

c) as áreas geográficas abrangidas pelo disparo;

d) a quantidade estimada de estações rádio-base (ERBs) envolvidas, caso essa informação esteja disponível.

e) se a área efetivamente alcançada pelo disparo correspondeu à área originalmente prevista pelo sistema ou se houve ampliação indevida da abrangência geográfica da mensagem, esclarecendo, em caso positivo, as causas técnicas já identificadas para essa divergência.

19. Informe se o incidente comprometeu, ainda que temporariamente, a capacidade operacional do sistema Defesa Civil Alerta para emissão de alertas reais de emergência durante o período em que permaneceu suspenso, especificando:

a) o período de indisponibilidade operacional;

b) as medidas contingenciais adotadas para garantir a continuidade da emissão de alertas à população;

c) se houve ocorrência de eventos reais que demandariam utilização do sistema durante esse período; e

d) quais protocolos alternativos permaneceram disponíveis para comunicação de situações de risco.

VI – DA GESTÃO DE RISCOS E DO APERFEIÇOAMENTO DO SISTEMA

20. Informe quais medidas corretivas foram adotadas imediatamente após o incidente para impedir nova emissão indevida de alertas.

21. Informe quais vulnerabilidades técnicas ou operacionais já foram identificadas até o presente momento e quais medidas corretivas já foram implementadas.

22. Informe se o episódio motivará revisão:

a) da arquitetura tecnológica do sistema;

b) dos protocolos de autenticação;

c) dos fluxos de autorização para emissão de alertas;

d) da política de gestão de acessos;

e) da política de segurança da informação; e

f) dos protocolos nacionais de proteção e defesa civil relacionados ao sistema Defesa Civil Alerta.

23. Informe se existem estudos para implementação de mecanismos adicionais de segurança, tais como autenticação reforçada, dupla validação obrigatória, monitoramento contínuo, inteligência artificial para detecção de comportamentos anômalos ou outras soluções tecnológicas.

VII – DA ARTICULAÇÃO INSTITUCIONAL

24. Informe quais órgãos federais participaram da resposta ao incidente, especificando as competências exercidas por cada um.

25. Informe se o Ministério comunicou formalmente o incidente à Polícia Federal, ao Ministério da Justiça e Segurança Pública, ao Ministério das Comunicações, à Agência Nacional de Telecomunicações – Anatel, à Autoridade Nacional de Proteção de Dados – ANPD, ao Centro Integrado de Segurança Cibernética do Governo Federal, ao Centro de Prevenção, Tratamento e Resposta

a Incidentes Cibernéticos de Governo – CTIR Gov ou a quaisquer outros órgãos competentes, indicando:

a) a data das comunicações;

b) o objeto de cada comunicação; e

c) as providências decorrentes dessas articulações.

VIII – DA TRANSPARÊNCIA E DA PRESTAÇÃO DE CONTAS

26. Informe se será elaborado Relatório Técnico Final acerca do incidente, indicando:

a) o órgão responsável por sua elaboração;

b) o prazo estimado para conclusão;

c) se o documento será disponibilizado ao Congresso Nacional; e

d) se haverá divulgação pública das conclusões, ressalvadas as informações protegidas por sigilo legal.

27. Informe se será elaborado Plano de Ação destinado ao fortalecimento da segurança cibernética, da governança tecnológica e da gestão de riscos do sistema Defesa Civil Alerta, encaminhando cópia do documento quando concluído.

28. Encaminhe cópia dos atos administrativos públicos relacionados ao incidente, das notas técnicas, pareceres, recomendações, comunicações oficiais, determinações administrativas e demais documentos públicos produzidos em decorrência dos fatos, ressalvadas apenas as informações protegidas por sigilo legal.

29. Encaminhe cópia dos relatórios técnicos, auditorias, avaliações independentes de segurança, pareceres especializados, planos de ação, planos de resposta, recomendações técnicas e demais documentos públicos produzidos em decorrência do incidente, indicando expressamente, quando houver restrição de

acesso a qualquer documento solicitado, o respectivo fundamento jurídico da negativa, com especificação da norma legal aplicável.

30. Informe se esse Ministério pretende encaminhar ao Congresso Nacional relatório circunstanciado contendo as conclusões da investigação administrativa, as medidas corretivas implementadas, as recomendações formuladas e o cronograma de aperfeiçoamento da segurança do sistema Defesa Civil Alerta, de forma a assegurar transparência, prestação de contas e fortalecimento da confiança da sociedade nos sistemas oficiais de comunicação de emergências.

JUSTIFICAÇÃO

Conforme amplamente noticiado e relatado por inúmeras pessoas em suas redes sociais, na madrugada do dia 20 de junho de 2026, milhões de brasileiros foram surpreendidos pelo recebimento, em seus aparelhos celulares, de mensagem classificada como "Alerta Extremo", acompanhada do sinal sonoro característico reservado às comunicações de risco iminente à vida, emitida por meio do sistema Defesa Civil Alerta. A mensagem, entretanto, não correspondia a qualquer desastre natural, emergência ou situação concreta que justificasse o acionamento da ferramenta, limitando-se à divulgação da palavra "misantropi4", fato que provocou insegurança na população e ampla repercussão nacional.

Em razão da gravidade do ocorrido, o Governo Federal informou a suspensão preventiva da plataforma, comunicou a adoção de medidas emergenciais para contenção do incidente e anunciou a instauração de procedimentos destinados à apuração de possível ataque cibernético, bem como a atuação coordenada dos órgãos competentes para investigação dos fatos e restabelecimento da segurança do sistema.

Os fatos possuem elevada relevância institucional por envolverem uma das principais ferramentas de comunicação de emergência da Administração Pública Federal, concebida para alertar a população sobre situações de risco iminente, tais como enchentes, deslizamentos, rompimentos de barragens, incêndios florestais, tempestades severas e outros eventos extremos capazes de colocar em risco a vida, a integridade física e o patrimônio de milhares de brasileiros.

O Defesa Civil Alerta constitui importante instrumento da Política Nacional de Proteção e Defesa Civil, permitindo a rápida disseminação de informações oficiais diretamente aos aparelhos celulares localizados em áreas potencialmente afetadas por desastres. A efetividade dessa política pública depende, em grande medida, da confiança da população na autenticidade, tempestividade e confiabilidade das mensagens emitidas pelo sistema.

Quando um alerta extremo é recebido, espera-se que os cidadãos adotem imediatamente medidas de autoproteção, muitas vezes em questão de minutos. Por essa razão, qualquer comprometimento da credibilidade do sistema possui potencial para reduzir a confiança da sociedade justamente quando o mecanismo vier a ser utilizado em situações reais de emergência, circunstância que pode comprometer a efetividade das ações de proteção e defesa civil e, em última análise, colocar vidas em risco.

Sob outro aspecto, o episódio suscita legítima preocupação quanto à governança das infraestruturas tecnológicas estratégicas do Estado brasileiro. Ainda que as investigações estejam em curso, mostra-se imprescindível compreender se o incidente decorreu de ataque cibernético, exploração de vulnerabilidade tecnológica, comprometimento de credenciais, falha operacional, deficiência de controles internos, inadequação da arquitetura tecnológica ou qualquer outra hipótese capaz de revelar fragilidades na gestão da segurança da informação aplicada a sistemas críticos da Administração Pública.

No âmbito de suas atribuições institucionais, compete ao Ministério da Integração e do Desenvolvimento Regional, por intermédio da Secretaria Nacional de Proteção e Defesa Civil, coordenar a implementação e o funcionamento do sistema Defesa Civil Alerta, assegurando sua disponibilidade, confiabilidade, integridade e capacidade operacional para atendimento das finalidades previstas na Política Nacional de Proteção e Defesa Civil.

Nesse contexto, revela-se indispensável que o Congresso Nacional conheça não apenas as circunstâncias do incidente, mas também os mecanismos de governança adotados para proteção do sistema, os protocolos de autenticação utilizados para emissão dos alertas, as políticas de gestão de riscos, os procedimentos de segurança cibernética implementados, as auditorias realizadas, os testes de vulnerabilidade executados e as medidas corretivas já adotadas para impedir a repetição de fatos semelhantes.

Também merece especial atenção a necessidade de esclarecer se, anteriormente ao incidente, esse Ministério ou a Secretaria Nacional de Proteção e Defesa Civil receberam comunicações, relatórios técnicos, auditorias, notificações, recomendações ou alertas acerca de vulnerabilidades relacionadas ao sistema Defesa Civil Alerta ou às tecnologias empregadas em sua operação. A identificação de eventuais alertas prévios, bem como das providências adotadas em resposta a essas comunicações, constitui elemento indispensável para aferição da efetividade da gestão de riscos, da governança tecnológica e dos mecanismos preventivos existentes.

Da mesma forma, mostra-se relevante conhecer a estrutura contratual responsável pelo desenvolvimento, manutenção e evolução tecnológica da plataforma, bem como os mecanismos de fiscalização contratual empregados pela Administração Pública, permitindo avaliar se a arquitetura atualmente utilizada atende aos padrões compatíveis com a criticidade do serviço prestado.

Outro aspecto que justifica a presente iniciativa refere-se à necessidade de conferir plena transparência às providências administrativas

adotadas após o incidente. A elaboração de relatórios técnicos, planos de ação, auditorias independentes e avaliações de segurança representa importante instrumento de prestação de contas à sociedade e de fortalecimento da confiança nas instituições públicas.

Cumpre destacar que a segurança cibernética das infraestruturas críticas nacionais constitui tema de crescente relevância para a proteção da soberania, da continuidade dos serviços públicos essenciais e da segurança da população. Incidentes dessa natureza exigem não apenas adequada responsabilização dos eventuais autores, mas também permanente aperfeiçoamento das políticas públicas de governança digital, gestão de riscos, segurança da informação e continuidade dos serviços públicos estratégicos.

Nos termos do art. 49, inciso X, da Constituição Federal, compete ao Congresso Nacional exercer a fiscalização e o controle dos atos do Poder Executivo. De igual modo, o art. 50, § 2º, da Constituição assegura às Casas do Congresso Nacional a prerrogativa de requisitar informações aos Ministros de Estado acerca de assuntos inerentes às respectivas atribuições, permitindo ao Parlamento acompanhar a implementação das políticas públicas e avaliar a eficiência da atuação administrativa.

As informações ora solicitadas permitirão ao Senado Federal exercer adequadamente sua função constitucional de controle externo, contribuindo para o aperfeiçoamento da Política Nacional de Proteção e Defesa Civil, para o fortalecimento da governança do sistema Defesa Civil Alerta, para a evolução dos mecanismos de segurança cibernética aplicáveis às infraestruturas tecnológicas estratégicas da Administração Pública Federal e para a preservação da confiança da população nos sistemas oficiais destinados à proteção da vida.

Mais do que apurar as circunstâncias de um episódio específico, a presente iniciativa busca contribuir para que sistemas essenciais à proteção da sociedade brasileira sejam continuamente aperfeiçoados, tornando-se cada vez

mais resilientes, seguros e confiáveis diante das crescentes ameaças cibernéticas que desafiam as administrações públicas em todo o mundo.

Diante da elevada relevância institucional dos fatos e do inequívoco interesse público envolvido, impõe-se o encaminhamento do presente Requerimento de Informações.

Sala das Sessões, 22 de junho de 2026.

Senadora Damares Alves