



SENADO FEDERAL

PROJETO DE LEI Nº 3318, DE 2026

Dispõe sobre requisitos de segurança para o envio de mensagens em sistemas de divulgação de alertas públicos e dá outras providências.

AUTORIA: Senador Jader Barbalho (MDB/PA)



[Página da matéria](#)



PROJETO DE LEI Nº , DE 2026
(Do Sr. Jader Barbalho)

Dispõe sobre requisitos de segurança para o envio de mensagens em sistemas de divulgação de alertas públicos e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei estabelece requisitos mínimos de segurança para a operação de sistemas de divulgação de mensagens de alerta público, com o objetivo de prevenir o envio indevido, não autorizado, fraudulento ou errôneo de comunicações destinadas à população.

Parágrafo único. Consideram-se sistemas de divulgação de mensagens de alerta público, para os fins desta Lei, os mecanismos públicos ou privados destinados à transmissão massiva de mensagens de aviso, emergência, desastre, risco ou utilidade pública, tais como alertas de defesa civil, emergências meteorológicas, evacuação, segurança pública e demais comunicações oficiais dirigidas à população por meio de telefonia móvel, transmissão de rádio e televisão, aplicativos ou outros canais de difusão.

Art. 2º Para os fins desta Lei, considera-se:

I – **autenticação criptográfica:** o processo de verificação da identidade do operador e da integridade da mensagem mediante





uso de certificado digital, chaves criptográficas ou mecanismo equivalente que assegure a origem e a não adulteração do conteúdo;

II – termo de responsabilidade individualizado: documento eletrônico, vinculado a cada mensagem específica, no qual o operador declara a veracidade, a pertinência e a autorização para o envio, assinado digitalmente;

III – dupla supervisão: procedimento que condiciona o envio de cada mensagem à autorização prévia de supervisor distinto do operador que a elaborou.

Art. 3º O envio de mensagens por meio de sistemas de divulgação de alertas públicos observará, cumulativamente, os seguintes requisitos de segurança:

I – autenticação criptográfica do operador e da mensagem, mediante certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil ou tecnologia de segurança equivalente;

II – assinatura de termo de responsabilidade individualizado para cada mensagem a ser enviada, com identificação do operador, data, hora e registro do conteúdo;

III – dupla supervisão, de modo que nenhuma mensagem seja transmitida sem a autorização prévia e expressa de supervisor distinto do operador responsável por sua elaboração.

§ 1º A autorização do supervisor de que trata o inciso III será igualmente registrada com autenticação criptográfica e identificação individualizada.

§ 2º Todos os atos de elaboração, autorização e envio serão objeto de registro eletrônico inalterável, com preservação por prazo mínimo de 5 (cinco) anos, para fins de auditoria e responsabilização.

Art. 4º Em situações de emergência que exijam celeridade incompatível com o cumprimento integral dos requisitos





SENADO FEDERAL

Gabinete do Senador JADER BARBALHO (MDB/PA)

SF/26955.12012-43

do art. 3º, o regulamento poderá estabelecer procedimento simplificado, preservados, no mínimo, a autenticação criptográfica e o registro inalterável do envio, com supervisão posterior obrigatória.

Art. 5º O descumprimento dos requisitos previstos nesta Lei sujeita os responsáveis às sanções administrativas, civis e penais cabíveis, sem prejuízo da responsabilização do órgão ou entidade operadora.

Art. 6º O Poder Executivo regulamentará esta Lei, definindo padrões técnicos e autoridades competentes com acesso de supervisor no sistema.

Art. 7º Os sistemas em operação deverão adequar-se ao disposto nesta Lei no prazo de 1 (um) ano, contado da publicação de sua regulamentação.

Art. 8º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Os sistemas de alerta público constituem instrumento essencial de proteção à vida, sobretudo diante do agravamento dos desastres naturais e das emergências climáticas. Sua eficácia, contudo, depende integralmente da credibilidade e da segurança da infraestrutura que os opera, sob pena de se converterem em vetor de pânico e de desinformação.

O episódio ocorrido entre a noite de 19 de junho e a madrugada de 20 de junho de 2026 evidenciou, de forma grave, a fragilidade dessa infraestrutura no Brasil. O sistema oficial da Defesa Civil foi comprometido por agente externo, e celulares de aproximadamente trinta milhões de pessoas em oito estados (São Paulo, Rio de Janeiro, Minas Gerais, Bahia, Pará, Mato Grosso, Goiás e o Distrito Federal) receberam notificação falsa classificada





SENADO FEDERAL

Gabinete do Senador JADER BARBALHO (MDB/PA)

SF/26955.12012-43

como "Alerta Extremo", categoria mais severa do sistema, normalmente reservada a desastres iminentes. A mensagem continha apenas a palavra "misanthropia", sem qualquer relação com situação real de emergência.

Segundo o Secretário Nacional de Proteção e Defesa Civil, foram emitidos dez alertas indevidos durante a ação criminosa, sendo nove pelo sistema Cell Broadcast e um pelo antigo sistema de SMS. O comando do disparo foi realizado remotamente por usuário externo, sem qualquer ligação com o Sistema Nacional de Proteção e Defesa Civil, o que levou à suspensão preventiva da plataforma e ao acionamento da Polícia Federal para apurar a autoria e a extensão do ataque.

O incidente expôs problema estrutural: o sistema permitiu que um único acesso não autorizado disparasse, sem qualquer barreira de verificação de identidade, sem responsabilização individualizada e sem aprovação humana intermediária, alertas máximos para dezenas de milhões de cidadãos.

Além do alarme social imediato, episódios dessa natureza corroem a confiança da população no sistema, criando risco de que alertas legítimos e vitais sobre enchentes, deslizamentos ou outros desastres reais venham a ser ignorados no futuro.

A presente proposta responde diretamente a essas vulnerabilidades, instituindo três camadas cumulativas de proteção. A autenticação criptográfica impede que comandos partam de origem não verificada ou remota não autorizada, exatamente a falha explorada no ataque de junho de 2026. O termo de responsabilidade individualizado assegura rastreabilidade e responsabilização de cada disparo. E a dupla supervisão elimina a possibilidade de que um único ponto de acesso comprometido, humano ou cibernético, transmita mensagens à população sem validação independente. O





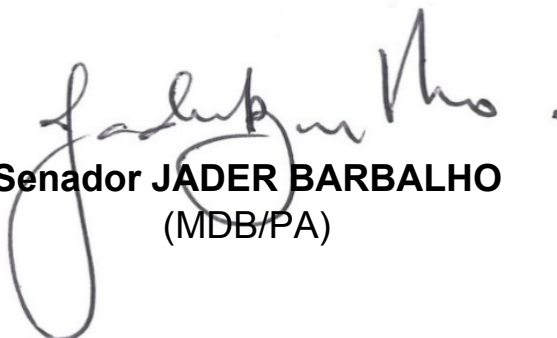
SENADO FEDERAL

Gabinete do Senador JADER BARBALHO (MDB/PA)

texto preserva, ainda, a celeridade indispensável às emergências, mediante procedimento simplificado com supervisão posterior obrigatória.

Tratando-se de matéria que toca diretamente a segurança e a vida da população, e diante da demonstração concreta e recente dos riscos envolvidos, conta-se com o apoio dos nobres Pares para a aprovação deste projeto.

Sala das Sessões, em 25 de junho de 2026.



Senador JADER BARBALHO
(MDB/PA)

