

Segurança e autenticidade no sistema público de alerta

Autor(a): Vitor Soliano

Publicado em: 06 de setembro de 2026

Publicação: conjur_import

Link JurisTube:

<https://juristube.com.br/colunistas/vitor-soliano/seguranca-e-autenticidade-no-sistema-publico-de-alerta>

Fonte original: <https://conjur.com.br/2026-set-06/seguranca-e-autenticidade-nos-sistemas-publicos-de-alerta>

Identificador citável:

juristube.com.br/colunistas/vitor-soliano/seguranca-e-autenticidade-no-sistema-publico-de-alerta#ep-6905ff92

Resumo

No alerta de emergência, a presunção de legitimidade e veracidade opera como condição de funcionamento do sistema

Texto integral

Na noite de 19 para a madrugada de 20 de junho, celulares em diferentes regiões do país emitiram o som reservado ao nível máximo do sistema Defesa Civil Alerta. Em vez de uma orientação sobre enchente, deslizamento ou outro perigo, os destinatários receberam uma mensagem com uma única palavra: “misanthropia”. Em coletiva de imprensa, o secretário nacional de Proteção e Defesa Civil informou dez disparos indevidos, nove por Cell Broadcast e um por SMS, após os quais a plataforma foi retirada temporariamente do ar e o Ministério da Integração e do Desenvolvimento Regional acionou a Polícia Federal e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo [1] . Estimativas preliminares apontam que dezenas de milhões de aparelhos teriam sido atingidos em oito estados e no Distrito Federal. O número exato ainda precisa ser confirmado, assim como a forma de acesso ao sistema e as salvaguardas que não conseguiram impedir os disparos. Esses elementos serão importantes para a atribuição de responsabilidades, embora o problema institucional revelado pelo episódio já possa ser examinado. O Defesa Civil Alerta foi concebido para produzir reação imediata em situações de emergência. Diante de uma inundação ou de um deslizamento iminente, não se pode exigir que o destinatário investigue previamente se a mensagem foi realmente emitida pela autoridade competente. Por essa razão, o aviso se sobrepõe ao uso ordinário do telefone, dispensa cadastro prévio e, quando classificado como extremo, emite sinal sonoro mesmo nos aparelhos configurados no modo silencioso. Nos alertas de emergência, a presunção de legitimidade e veracidade que ordinariamente acompanha a atuação administrativa deixa de ser apenas um efeito jurídico e passa a operar como condição de funcionamento do sistema [2] . O serviço somente protege a população porque o destinatário presume, no momento em que recebe a mensagem, que ela foi emitida por uma autoridade competente. A preservação dessa autenticidade integra, portanto, a própria prestação do serviço e não pode ser tratada como questão restrita à área de tecnologia da informação. O episódio difere, nesse aspecto, de uma notícia falsa difundida em rede social. Nesta espécie de desinformação [3] , um conteúdo fabricado procura adquirir aparência de verdade, enquanto no Defesa Civil Alerta a mensagem falsa foi transmitida por uma infraestrutura efetivamente estatal. A irregularidade

alcançou, assim, o procedimento institucional que atribuía autoria pública à comunicação. Nas estruturas administrativas tradicionais, a aparência de autoridade era produzida pela repartição, pela identificação funcional, pelo documento oficial ou pela publicação em veículo próprio. Nos serviços digitais, ela depende de credenciais, perfis de acesso, níveis de autorização, regras de autenticação e limites incorporados ao sistema. A possibilidade concreta de agir em nome do Estado passa, desse modo, a ser mediada por uma arquitetura técnica. ... Essa arquitetura não é juridicamente neutra, pois traduz, ou deveria traduzir, regras de competência administrativa. O artigo 11 da Lei nº 9.784/1999 determina que a competência é irrenunciável e deve ser exercida pelos órgãos aos quais foi atribuída, ressalvadas as hipóteses legais de delegação e avocação. A Lei nº 12.608/2012, por sua vez, distribui entre União, estados e municípios as atribuições do Sistema Nacional de Proteção e Defesa Civil. No plano operacional, essa distribuição deve ser convertida em credenciais, limitações territoriais, níveis de severidade e mecanismos de validação. Esses elementos não constituem simples escolhas de conveniência tecnológica, porque são os meios pelos quais as competências jurídicas se tornam efetivas dentro da plataforma. Quando essa correspondência falha, o sistema pode permitir, na prática, aquilo que o Direito não autorizou. Nos serviços públicos digitalizados, as normas de competência não se cumprem apenas com a indicação abstrata do órgão responsável. Elas também precisam ser incorporadas à arquitetura de identidades, perfis e permissões, de modo a restringir a atuação de cada usuário aos limites juridicamente estabelecidos. O desenho dos controles de acesso integra, por isso, a organização jurídica da administração e deve ser submetido a formalização, governança e controle. As informações divulgadas até o momento tornam esse problema especialmente relevante. O secretário nacional informou que os credenciamentos para disparo são realizados pelos estados e que uma mesma credencial, em princípio, não deveria permitir o envio de alertas para diferentes unidades federativas. Reportagens posteriores indicaram que teriam sido utilizadas credenciais vinculadas ao Pará, embora o estado não estivesse entre os locais atingidos [4] . Se essa informação for confirmada, será necessário apurar se (1) houve comprometimento das credenciais ou (2) insuficiência dos mecanismos de autenticação ou falha na própria arquitetura de controle de acesso. A primeira hipótese indicaria que controles adequados existiam, mas foram contornados por falhas na custódia ou na utilização das credenciais. A segunda revelaria uma deficiência anterior ao ataque, relacionada à forma como o sistema incorporou as competências, os limites territoriais e os níveis de autorização. A identificação do autor e sua eventual responsabilização penal são relevantes, mas não substituem essa apuração administrativa. Mesmo que a invasão tenha sido praticada por terceiro, permanece necessário compreender por que os controles existentes não impediram ou não contiveram os disparos. A resposta pública ao episódio não pode se limitar ao inquérito criminal, caso haja elementos capazes de revelar uma falha organizacional ou de arquitetura. Precedente, dever de aprender e base normativa O precedente mais útil ocorreu no Havaí, em janeiro de 2018, quando a população recebeu um alerta informando que um míssil balístico se aproximava e que não se tratava de um exercício. A mensagem corretiva enviada pelo próprio sistema demorou 38 minutos, período em que os destinatários permaneceram sem uma confirmação oficial de que o aviso era falso. A Federal Communications Commission não restringiu sua investigação à conduta do operador e examinou também a arquitetura do sistema, os mecanismos de supervisão, a separação entre teste e produção e a ausência de um procedimento previamente estruturado para o cancelamento de alertas indevidos. Em um primeiro comunicado, a FCC já havia constatado que o governo do Havaí não possuía salvaguardas razoáveis ou controles adequados para prevenir a transmissão de um falso alerta [5] . As alterações adotadas posteriormente incluíram dupla verificação, maior diferenciação

entre os ambientes, supervisão dos exercícios e protocolos específicos de correção. O interesse do precedente para o Brasil não decorre de uma suposta identidade entre os sistemas, mas do método utilizado para investigar a falha. Em vez de procurar apenas quem errou, a apuração examinou as condições institucionais que permitiram que uma decisão equivocada produzisse consequências de grande escala. Incidentes dessa natureza devem levar à revisão verificável dos controles, dos procedimentos e das responsabilidades organizacionais. O dever de aprender adquire conteúdo jurídico quando a experiência produz alterações institucionais que possam ser identificadas, avaliadas e auditadas. Não se exige que o sistema se torne infalível, mas que ele não retorne ao funcionamento sem que as causas e as condições do incidente tenham sido examinadas. A Política Nacional de Segurança da Informação, instituída pelo Decreto nº 12.572/2025, fornece base normativa para essa exigência. O decreto prevê estruturas de governança, revisão periódica das políticas internas, avaliação de conformidade e auditoria das ações de segurança da informação pelo Sistema de Controle Interno. A revisão dos controles após um incidente relevante integra, assim, a governança da segurança da informação e não depende apenas da conveniência do gestor. O padrão jurídico exigível deve ser proporcional aos riscos criados pelo sistema. Isso pressupõe controles capazes de prevenir, limitar, detectar e corrigir eventos indevidos, além de procedimentos que permitam uma resposta rápida quando essas barreiras se mostrarem insuficientes. A impossibilidade de eliminar todas as falhas não afasta o dever de reduzir sua probabilidade e de limitar suas consequências. Não parece necessário, para esse fim, aprovar uma nova lei. O ordenamento já contém normas sobre defesa civil, segurança da informação, cibersegurança e proteção de infraestruturas críticas e de dados pessoais, que fornecem fundamento suficiente para tratar o Defesa Civil Alerta como um sistema digital crítico da administração pública. O problema está em saber se essas normas foram efetivamente convertidas em requisitos técnicos, procedimentos operacionais e mecanismos de auditoria compatíveis com a relevância do serviço. Entre os controles esperados estão a autenticação reforçada, a separação entre quem elabora e quem autoriza a mensagem, a limitação territorial das credenciais, a diferenciação dos níveis de severidade, a manutenção de registros auditáveis e a existência de um mecanismo rápido de cancelamento. A apuração deverá indicar quais dessas salvaguardas estavam presentes e como funcionaram durante o incidente. Caberá ao Estado informar os riscos e os controles do sistema, bem como as alterações realizadas depois dos disparos. Episódio ajuda a delimitar o alcance da LGPD O Cell Broadcast difunde mensagens aos aparelhos localizados em determinada área e, em sua arquitetura básica, não depende de uma lista nominal de destinatários. De todo modo, é dever da Administração Pública apurar se o acesso ao sistema pode ter representado exposição de dados pessoais, e, portanto, de alguma forma de incidente de segurança nos termos da Resolução CD/ANPD nº 15, de 2024 [6] . A eventual exposição de credenciais ou de dados associados a agentes públicos ainda deverá ser investigada, mas o objeto diretamente comprometido foi a autenticidade da comunicação estatal. A proteção de dados permanece relevante como parte de uma disciplina mais ampla de governança da informação pública. A LGPD consolidou deveres de prevenção, segurança e responsabilização que podem contribuir para a avaliação do incidente. Embora aplicável ao vazamento de dados pessoais, o Superior Tribunal de Justiça já se manifestou sobre o fato de um ataque hacker não configurar responsabilidade exclusiva de terceiro quando houver obrigação legal de tomar medidas de segurança proporcionais [7] . A resposta administrativa também deve incluir um grau adequado de transparência. Não é necessário, nem recomendável, divulgar informações técnicas que possam facilitar novos ataques, mas a sociedade deve conhecer a extensão geral do evento, a natureza da vulnerabilidade, os controles existentes, as razões de sua insuficiência e as medidas adotadas para

reduzir o risco de recorrência. Essa prestação de contas pode ser realizada independentemente da conclusão do inquérito criminal. A transparência possui, nesse caso, uma função adicional, porque a utilidade do sistema depende da confiança de seus destinatários. Mesmo que permaneça tecnicamente disponível, o Defesa Civil Alerta perderá parte de sua eficácia se a população passar a duvidar das mensagens ou a procurar confirmação em outras fontes antes de agir. O principal dano de um falso alerta pode se manifestar, portanto, na demora da reação diante de um aviso futuro e verdadeiro. A digitalização do Estado costuma ser avaliada pela rapidez dos serviços, pela redução de custos e pela comodidade oferecida aos usuários. Esses critérios são importantes, mas não contemplam o poder institucional concentrado em sistemas capazes de alcançar milhões de pessoas, interromper sua atenção e comunicar uma situação de emergência. A ampliação dessa capacidade deve ser acompanhada por controles compatíveis com seus efeitos. A proteção de dados ensinou a administração a perguntar quem pode acessar as informações que o Estado conserva, para quais finalidades e sob quais garantias. O episódio de junho acrescenta uma questão semelhante sobre a comunicação pública: quem pode emitir mensagens em nome do Estado, para qual território, com que grau de urgência e mediante quais controles. A resposta dependerá de verificar se as competências previstas no ordenamento foram corretamente incorporadas às permissões, aos limites operacionais e aos mecanismos de autenticação do sistema. [1] QUEIROZ, Vitória. Governo identificou 10 alertas falsos em sistema da Defesa Civil. CNN Brasil, Brasília, 20 jun. 2026. Disponível aqui . [2] BRASIL. Ministério da Integração e do Desenvolvimento Regional. Defesa Civil Alerta. Brasília, [2026]. Disponível aqui . [3] WARDLE, Claire; DERA KHSHAN, Hossein. Desordem informacional: para um quadro interdisciplinar de investigação e elaboração de políticas públicas. Estrasburgo: Éditions du Conseil de l'Europe, 2023. 125 p. Disponível aqui . [4] PODER360. Credenciais do Pará foram usadas em alertas da Defesa Civil, diz jornal. Poder360, Brasília, 21 jun. 2026. Disponível aqui . [5] ESTADOS UNIDOS. Federal Communications Commission. Statement of FCC Chairman Pai on false emergency alert in Hawaii. Washington, 14 jan. 2018. Disponível aqui . [6] BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Conselho Diretor. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União: seção 1, Brasília, DF, n. 81, p. 114, 26 abr. 2024 [7] BRASIL. Superior Tribunal de Justiça. REsp n. 2.147.374/SP, relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 3/12/2024, DJEN de 6/12/2024.

Como citar este documento

As citações abaixo seguem os padrões ABNT NBR 6023:2018, APA 7ª edição, Chicago Author-Date (17ª ed.) e BibTeX (LaTeX). Copie o formato exigido pelo periódico ou gerenciador bibliográfico (Zotero, Mendeley, EndNote).

ABNT (NBR 6023:2018)

SOLIANO, Vitor. Segurança e autenticidade no sistema público de alerta. *conjur_import*, 6 set. 2026. Disponível em: <https://conjur.com.br/2026-set-06/seguranca-e-autenticidade-nos-sistemas-publicos-de-alerta>. Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: <https://juristube.com.br/colunistas/vitor-soliano/seguranca-e-autenticidade-no-sistema-publico-de-alerta>. Acesso em: 30 set. 2026.

APA 7ª edição

Soliano, V. (2026, September 6). Segurança e autenticidade no sistema público de alerta. **conjur_import**. <https://conjur.com.br/2026-set-06/seguranca-e-autenticidade-nos-sistemas-publicos-de-alerta>

Chicago Author-Date (17ª ed.)

SOLIANO, Vitor. 2026. “Segurança e autenticidade no sistema público de alerta.” **conjur_import**, September 06. <https://conjur.com.br/2026-set-06/seguranca-e-autenticidade-nos-sistemas-publicos-de-alerta>

BibTeX

```
@article{vitor-soliano-seguran-a-e-autenticidade-no-sistema-p-b-2026,  
author = {Soliano, Vitor},  
title = {Segurança e autenticidade no sistema público de alerta},  
journal = {conjur_import},  
year = {2026},  
url = {https://conjur.com.br/2026-set-06/seguranca-e-autenticidade-nos-sistemas-publicos-de-alerta},  
urldate = {2026-09-06}  
}
```



Licença de Uso — CC BY-NC-SA 4.0

Este conteúdo está licenciado sob a licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0). O uso para fins acadêmicos e educacionais é permitido, desde que citada a fonte original (JurisTube) conforme as normas técnicas indicadas neste documento.

Termos completos:

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt-br>

JurisTube — Acervo Digital de Direito

<https://juristube.com.br/colunistas/vitor-soliano/seguranca-e-autenticidade-no-sistema-publico-de-alerta>

PDF gerado em 2026-09-30 19:22 UTC