

Ataque cibernético expôs dados sensíveis de pacientes de unidades geridas pelo Instituto Saúde e Cidadania (Isac), que atua na gestão de unidades de saúde em vários estados brasileiros

-

A Agência Nacional de Proteção de Dados (ANPD) instaurou processo de sanção contra o [Instituto Saúde e Cidadania \(Isac\)](#), organização social com sede administrativa em Brasília, que atua na gestão de unidades públicas de saúde em vários estados brasileiros, como Goiás, Rio Grande do Sul, Bahia, Alagoas, Piauí e Tocantins. O Isac é investigado por falhas na proteção de dados pessoais sensíveis de 500 mil pacientes - falhas na comunicação às vítimas e na adoção de medidas de segurança. A ação decorre de um [incidente de segurança](#) ocorrido em 2025 e comunicado pelo Isac à Agência, o que gerou um processo de apuração dos fatos.

O caso envolveu um ataque cibernético de ransomware, em que os dados são sequestrados e tornados inacessíveis. A instituição informou que o incidente teria afetado cerca de 500 mil registros, dos quais aproximadamente 78.772 seriam de crianças e adolescentes e 47.921 de idosos. Os registros continham dados pessoais de identificação (como nome e data de nascimento) e dados pessoais sensíveis de saúde (histórico de exames, prontuários, prescrições, atendimentos ambulatoriais, internações, diagnósticos e procedimentos realizados).

A ANPD investiga se, em razão desse incidente de segurança, foram cometidas infrações à Lei Geral de Proteção de Dados Pessoais ([LGPD](#)) relacionadas à não adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais; à não comunicação, de maneira adequada, às pessoas afetadas pelo incidente; à não disponibilização de informações relativas ao encarregado pelo tratamento de dados pessoais e ao descumprimento aos princípios da prevenção e da responsabilização e prestação de contas.

Ao ser questionado sobre o real impacto do incidente, o Isac alegou que não haveria risco ou dano relevante aos titulares, argumentando que os invasores teriam acessado apenas informações administrativas e bancos de dados referentes a contratos já encerrados. No entanto, a entidade não apresentou comprovação para essa afirmação. A Agência apurou também que o Isac não comunicou individualmente os titulares afetados, como seria esperado de acordo com a LGPD em circunstâncias semelhantes, tendo se limitado a publicar um aviso em seu site institucional.

Para a ANPD, essa comunicação foi insuficiente, pois não informava a data do incidente, a natureza dos dados e das pessoas afetadas, nem as medidas adotadas antes e depois do ataque — itens exigidos pela LGPD e pela regulamentação específica da Agência sobre Comunicação de Incidentes de Segurança (CIS).

Segundo o auto de infração, o Isac não apresentou evidências técnicas que comprovassem suas alegações mesmo após reiterados questionamentos da ANPD, o que comprometeu a verificação da efetiva adoção de medidas corretivas. A Agência identificou ainda que o Isac não disponibiliza, em seu portal, informações sobre o encarregado pelo tratamento de dados pessoais, conforme exige a LGPD.

O Processo Administrativo Sancionador (PAS) instaurado pela ANPD prevê prazo de dez dias úteis, a contar da intimação, para apresentação da defesa. Se condenado, além da sanção, o Isac será orientado sobre o que precisa fazer para regularizar a situação. As sanções previstas no artigo 52 da LGPD vão desde advertência a multa de até 2% do faturamento e suspensão ou proibição do exercício de atividades de tratamento de dados pessoais. A sanção a ser eventualmente aplicada será definida ao final da análise do processo, conforme o [Regulamento de Dosimetria e Aplicação de Sanções Administrativas da ANPD](#).

» Saiba mais sobre os [Comunicados de Incidentes de segurança](#)

» O Processo número 00261.003381/2026-55 está disponível para pesquisa publica no Sistema

Eletrônico de Informações ([SEI](#))

Fonte: [ANPD](#), em 08.07.2026.