

SEGURANÇA

Saúde no Brasil enfrenta crescente ameaça cibernética e expõe desafios

25 de julho de 2025 Por Redação

0 0 0 0 Share



O setor de saúde se tornou o principal alvo de ataques cibernéticos no mundo, ultrapassando empresas do setor financeiro e de consumo, segundo a pesquisa Digital Trust Insights 2025, da PwC. O estudo, que ouviu mais de 4 mil executivos de negócios e tecnologia em 77 países, incluindo o Brasil, revela que hospitais, clínicas e operadoras de planos de saúde estão no centro da mira dos criminosos digitais devido ao vasto volume de dados sensíveis que armazenam.

CONTEÚDO RELACIONADO – [Setor de Saúde lidera uso de GenAI, mas políticas de segurança não suportam adoção](#)

No Brasil, o cenário é ainda mais crítico. O país está entre os mais vulneráveis a ataques cibernéticos na área da saúde, com 12% dos incidentes globais registrados no setor apenas no primeiro semestre de 2023, de acordo com dados globais. Paralelamente, o segmento representa cerca de 10% do PIB brasileiro e deve movimentar R\$ 980,3 bilhões até o final de 2024, conforme o relatório Panorama e Perspectivas da Cadeia de Saúde do Brasil 2024.

Esse crescimento exponencial é impulsionado por investimentos globais no setor de cibersegurança, que movimentaram US\$ 12,2 bilhões em 2023, com expectativa de atingir US\$ 34,7 bilhões até 2029, segundo a National Library of Medicine. No Brasil, essa transformação é facilmente identificada pelo aumento da oferta de serviços online aos pacientes: entre 2022 e 2023, o agendamento de consultas pela internet subiu de 13% para 34%, e a visualização de prontuários eletrônicos dobrou no mesmo período, conforme levantamento do Comitê Gestor da Internet no Brasil (CGI.br). Além disso, a telemedicina se consolidou como uma ferramenta essencial para ampliar o acesso à saúde, com um salto de 172% nas consultas remotas entre 2020 e 2023, atingindo a marca de 30 milhões de atendimentos virtuais, segundo a Fenasaúde.

Para Eduardo Lopes, CEO da Redbelt Security, consultoria especializada em cibersegurança, essa revolução digital na saúde traz um paradoxo preocupante: ao mesmo tempo em que melhora a eficiência dos serviços médicos, amplia a superfície de ataque para cibercriminosos. "Nunca antes tivemos tantos dados sensíveis circulando de forma digital. Informações médicas não são apenas confidenciais: elas podem ser usadas para extorsão, fraudes e até manipulação de diagnósticos. Um vazamento dessa magnitude não afeta apenas a reputação de uma instituição, mas coloca em risco a vida de pacientes", alerta Lopes.

Além dos ataques, as fragilidades internas do setor agravam o problema. Lopes explica que muitas instituições ainda enfrentam desafios estruturais, como a falta de profissionais especializados em cibersegurança, dificuldades para acompanhar a evolução das ameaças e o alto custo das soluções de proteção digital. "Muitas vezes, a cibersegurança é tratada como um problema secundário, quando, na verdade, deveria estar no centro das decisões estratégicas. A falta de investimento e de cultura em segurança abre brechas que tornam os sistemas vulneráveis", afirma.

O executivo destaca que o impacto dos ataques vai além da privacidade dos dados. A interrupção de sistemas pode significar cancelamento de cirurgias, perda de acesso a históricos médicos e falhas críticas no atendimento. "O que estamos discutindo aqui não é apenas um problema de compliance com a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes para a segurança de informações pessoais no Brasil, mas uma questão de infraestrutura essencial para a sociedade. Se um hospital tem seu sistema paralisado por um ataque, por exemplo, isso pode comprometer o atendimento a centenas de pessoas em questão de minutos e por tempo indeterminado", reforça.

Diante dessa realidade, ele alerta que a segurança cibernética precisa ser encarada como prioridade estratégica na área de saúde. "A tecnologia avança, mas a segurança não pode ficar para trás. Sem um planejamento robusto e investimentos contínuos em proteção digital, o setor de saúde pode se tornar um dos mais impactados por ataques cibernéticos nos próximos anos", conclui Lopes.

Participe das comunidades IPNews no [Instagram](#), [Facebook](#), [LinkedIn](#) e [X](#).

CIBERSEGURANÇA DIGITALIZAÇÃO FRAGILIDADE SAÚDE SEGURANÇA DIGITAL

← Artigo Anterior



25 de julho de 2025
Ciberataques expõem falhas críticas na arquitetura de rede, aponta relatório

Próximo Artigo →

28 de julho de 2025
As mais lidas da semana



NEWSLETTER

Inscriva-se para receber nossa newsletter semanal com as principais notícias em primeira mão.

Nome

Email

Ao continuar, você aceita a política de privacidade

SE INSCREVER

Deixe um comentário

O seu endereço de e-mail não será publicado. Campos obrigatórios são marcados com *

Name*

Email*

Website

POST COMMENT



Você não pode perder:

ARTIGOS

Por que uma visão completa de riscos é essencial? Projetos de TI complexos impulsionam o negócio, mas exigem atenção aos riscos

28 de julho de 2025

WIRELESS

Nuvem e expansão de ambientes híbridos elevam mercado de Wi-Fi como Serviço a mais de US\$ 21,9 Bi até 2030

28 de julho de 2025

Em Alta

INTERNACIONAL

4 de julho de 2016

Polícia de Londres usará drones para perseguir ladrões

Por Jackeline Carvalho

Menu

Anuncie

Contato

Quem Somos

Desenvolvido por Agência Hype

Inscriva-se no canal Radar IPNews

