SOPHOS

O ESTADO DO RANSOMWARE NO BRASIL 2026

Resultados de uma pesquisa independente e imparcial com 71 organizações no Brasil que foram atingidas por ransomware no último ano.

DOCUMENTO TÉCNICO SOPHOS – JULHO DE 2026

Sobre o relatório

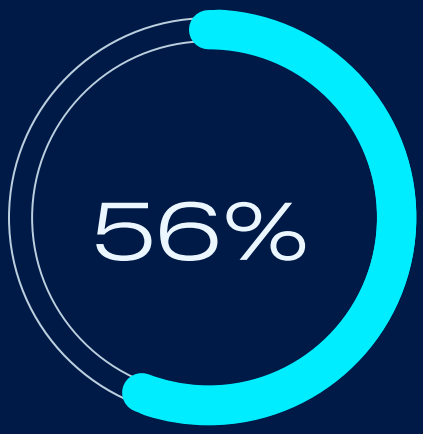
Em sua sétima edição, o relatório O Estado do Ransomware baseia-se nas conclusões de um levantamento independente e totalmente desvinculado de fornecedores encomendado pela Sophos. O relatório global deste ano fundamenta-se nas experiências de 2.158 líderes de TI e segurança cibernética atuando em organizações atingidas por ransomware no último ano, incluindo 71 do Brasil.

A pesquisa foi realizada entre janeiro e março de 2026. Todos os entrevistados trabalham em organizações com entre 100 e 5.000 funcionários e foram solicitados a responder com base na experiência que tiveram nos 12 meses anteriores. Todos os dados financeiros são expressos em dólares americanos. Valores de resgate atípicos, iguais ou superiores a 40 milhões de dólares, foram removidos desses dados.

Pesquisa com

71

líderes de TI e segurança cibernética no Brasil atuando em organizações atingidas por ransomware no último ano.



Porcentagem de ataques que resultaram na criptografia de dados.

Mediana do pedido de resgate no Brasil.

Custo médio para recuperar-se de um ataque de ransomware.

Por que as organizações brasileiras são vítimas de ransomware?

- **E-mails maliciosos foram a causa técnica primária mais comum, utilizados em 37% dos ataques. Essa foi a causa primária com maior porcentagem de e-mails maliciosos entre todos os países analisados no estudo.** Em seguida, vieram as vulnerabilidades exploradas (24%) e o phishing (18%). As vulnerabilidades exploradas caíram dos 44% no relatório de 2025 para 24%.
- **Uma lacuna de segurança desconhecida (42%) foi a causa operacional primária mais comum,** seguida por uma lacuna de segurança conhecida (39%) e pela falta de pessoas/capacidade (37%).
- **(NOVO) 74% confirmaram que o incidente de ransomware do ano passado foi o mesmo evento que o ataque de identidade mais significativo que sofreram.** Embora nem todos os ataques tenham resultado em criptografia de dados, essa descoberta estabelece o comprometimento de identidade como um mecanismo predominante de distribuição de ransomware.

O que acontece aos dados

- **56% dos ataques resultaram em dados criptografados.** Esse valor está alinhado com a média global de 56% e representa um aumento em relação aos 54% relatados pelos entrevistados brasileiros no relatório de 2025.
- **Em 38% dos ataques em que os dados foram criptografados, também houve roubo de dados,** um aumento em relação aos 22% em 2025.
- **98% das organizações brasileiras que tiveram seus dados criptografados conseguiram reavê-los,** acompanhando a média global.
- **45% das organizações brasileiras pagaram o resgate e conseguiram reaver os dados,** uma queda significativa em relação aos 66% do relatório do ano passado.
- **85% das organizações brasileiras usaram backups para recuperar os dados criptografados,** um aumento considerável em relação aos 73% relatados no relatório de 2025.

Pedidos de resgate

- **O valor mediano exigido dos resgates no Brasil foi de US$ 640.000,** um salto de 63% em relação aos US$ 392.500 informados no relatório de 2025.
- **35% dos pedidos de resgate foram de US$ 1 milhão ou mais,** uma queda em relação aos 41% citados no relatório de 2025.

Mediana do pedido de resgate no Brasil.

Impacto comercial do ransomware

- Excluindo quaisquer pagamentos de resgate, **o custo médio de recuperação para as organizações brasileiras após ataques de ransomware foi de US$ 1,05 milhão,** uma ligeira queda em relação à média de US$ 1,19 milhão registrada no relatório de 2025. Isso inclui custo do período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.
- **58% das organizações brasileiras se recuperaram de um ataque de ransomware em até uma semana,** um ligeiro aumento em relação aos 55% relatados no relatório de 2025. 18% levaram entre um e seis meses para se recuperar, uma pequena queda em relação aos 20% no relatório de 2025.

Impacto humano do ransomware nas equipes de TI e segurança cibernética em organizações onde os dados foram criptografados

48% relatam aumento em ansiedade e estresse sobre ataques futuros. Subiu de 31% em 2025

43% relatam aumento do reconhecimento pelos líderes seniores. Também subiu de 31% em 2025

43% vivenciaram mudanças na estrutura organizacional/da equipe.

43% relatam uma mudança de prioridades/foco da equipe.

28% relatam que a liderança da equipe foi substituída.

Recomendações

Reforce a segurança da identidade como uma defesa contra ransomware. Três quartos das vítimas brasileiras de ransomware confirmaram que o incidente de ransomware sofrido foi o mesmo evento que o ataque de identidade mais significativo que sofreram. As organizações devem priorizar a detecção e resposta a ameaças de identidade (ITDR), impor a autenticação multifator em todos os pontos de acesso e auditar regularmente as credenciais de identidade, tanto humanas quanto não humanas.

Reforce a proteção de endpoints para modelos de IA fronteiriça. A IA fronteiriça está acelerando a descoberta e a exploração de vulnerabilidades. Ter defesas robustas nos endpoints que bloqueiem automaticamente ataques baseados em exploits é essencial.

Priorize a segurança de e-mail. Considerando que phishing e e-mails maliciosos representam mais da metade das causas primárias de ransomware no Brasil, as organizações deveriam implantar filtragem de e-mail avançada, implementar os protocolos DMARC/DKIM/SPF e investir em treinamento regular de conscientização sobre phishing.

Invista em infraestrutura de backup e recuperação. Organizações que mantiveram sistemas de backup robustos recuperaram dados criptografados em taxas quase recordes no último ano. Os backups devem ser testados regularmente, armazenados offline ou em formatos imutáveis e integrados a um plano de resposta a incidentes documentado que possa ser executado sob pressão.

Para explorar as formas como a Sophos pode ajudar você a otimizar suas defesas contra ransomware, fale com um consultor ou acesse **sophos.com/ransomware2026**

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2026-07-24 BR-WP (TA) CRE-6010