# OS PLANOS DE RECUPERAÇÃO CIBERNÉTICA DO SETOR DE SAÚDE NÃO FORAM PROJETADOS PARA ESTE MOMENTO

*O mundo mudou. Os planos de recuperação não.*

Uma pesquisa com 400 tomadores de decisão de operações de TI e segurança de organizações de saúde revela o que acontece quando planos construídos com base em premissas de longa data colidem com ambientes cada vez mais complexos e com a crescente influência da IA.

## ONDE OS PLANOS DE RECUPERAÇÃO FALHAM

A maioria dos planos de recuperação presume que a recuperação ocorrerá de forma previsível. As organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses frequentemente constataram o contrário.

**64%** viram o escopo dos sistemas afetados **se expandir além da avaliação inicial**

**65%** em média, **identificaram lacunas moderadas ou significativas** na forma como os planos consideravam as dependências

**62%** **sofreram atrasos** porque os sistemas ou dados restaurados **não estavam limpos ou seguros para uso**

**83%** disseram que as **diferenças entre as equipes de operações de TI e de segurança** podem atrasar as decisões de recuperação

**85%** concordaram que os planos de recuperação **provavelmente exigirão soluções paliativas ou improvisação**

**85%** excederam os objetivos de tempo de recuperação (RTO), **com a recuperação levando quase 2 vezes mais tempo do que o planejado**

## O QUE A MAIORIA DOS PLANOS DE RECUPERAÇÃO PRIORIZA

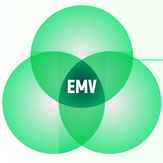
As organizações de saúde frequentemente precisam equilibrar velocidade de recuperação, restauração de sistemas e continuidade da assistência.

**71%** **priorizam a velocidade de recuperação,** mesmo em detrimento da certeza de que os sistemas restaurados estão limpos e seguros

**78%** **dizem que seus planos de recuperação se concentram mais na restauração de sistemas de TI** do que na manutenção de operações críticas e no atendimento a pacientes e clientes

## POUCOS DEFINEM O QUE MAIS IMPORTA ANTES DE UM ATAQUE

Uma Entidade Mínima Viável (EMV) ajuda as organizações de saúde a priorizar e reduzir o escopo da recuperação para minimizar a interrupção da assistência aos pacientes e das operações.

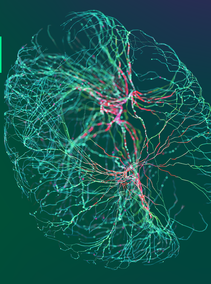



**APENAS 16%**
têm uma EMV formalmente documentada e testada

**61%**
dessas organizações dizem que sua EMV determinou diretamente o que foi restaurado primeiro durante um ciberataque relevante

## A IA ESTÁ SE TORNANDO OPERACIONAL ANTES DE SE TORNAR RECUPERÁVEL

À medida que a adoção de IA se acelera, o planejamento de recuperação tem dificuldade para acompanhar o ritmo.



**99%** **usam sistemas,** aplicações e fluxos de trabalho de IA ou modelos de machine learning

**37%** dizem que seus planos de recuperação **consideram de forma abrangente os ataques direcionados à infraestrutura de IA**

**58%** **não estão bem preparados** para detectar, conter e se recuperar de ações não intencionais ou incorretas realizadas por agentes de IA, copilotos ou fluxos de trabalho de IA

**61%** **não estão muito confiantes** em sua capacidade de verificar a integridade dos modelos de IA e dos dados associados após um ataque

## OS PLANOS ATUAIS NÃO FORAM FEITOS PARA O QUE ESTÁ POR VIR

As organizações de saúde esperam que a IA de fronteira exerça ainda mais pressão sobre as premissas de recuperação atuais.

**85%** **85% acreditam que seus planos de recuperação atuais exigiriam mudanças moderadas a significativas** se a IA de fronteira ampliasse capacidades como descoberta de vulnerabilidades, desenvolvimento de exploits e intrusões em várias etapas

**2%** **Apenas 2% consideram seus planos de recuperação atuais preparados** para essas condições

*Prepare-se para este momento. Planeje o próximo.*

Descubra mais insights do Relatório Global de Resiliência Cibernética da Cohesity de 2026 para o Setor de Saúde

Agende um workshop de resiliência contra ransomware para o setor de saúde

Identifique possíveis lacunas em seu plano de resiliência

### METODOLOGIA

A Cohesity contratou a Vanson Bourne para entrevistar 3.200 tomadores de decisão de TI e segurança em 12 países em julho de 2026. A amostra incluiu 400 participantes do setor de saúde, de organizações com 1.000 ou mais funcionários. Para os fins desta pesquisa, um ciberataque relevante foi definido como aquele com impacto financeiro, reputacional, operacional e/ou de perda de clientes mensurável para a organização.



© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind. 6200079-001-ptBR 10-2026