COHESITY

SETEMBRO DE 2026

SAÚDE
RELATÓRIO DE RESILIÊNCIA CIBERNÉTICA

Os planos de recuperação cibernética não foram projetados para este momento

QUANDO A PROTEÇÃO FALHA, O CUIDADO NÃO PODE PARAR

Ataques cibernéticos destrutivos não respeitam o horário de visitas. Eles não se importam se seus prontuários eletrônicos (EHRs), imagens ou dados de pesquisa estão hospedados localmente ou na nuvem. Eles apenas buscam a forma mais rápida de invasão, explorando quaisquer lacunas em sua estratégia de resiliência cibernética. Quando as organizações de saúde descobrem essas lacunas, muitas vezes já é tarde, no meio do ataque. O resultado? Tempo de inatividade. Isso não é apenas um item em um relatório de incidente. **Isso afeta o cuidado clínico de pessoas reais.**

Isso não é hipotético.

Quando invasores entraram na rede do NYC Health + Hospitals em novembro de 2025, passaram onze semanas sem ser detectados, copiando dados pessoais, médicos, financeiros e biométricos, incluindo impressões digitais de pacientes, antes de o sistema de saúde identificá-los em fevereiro de 2026. A violação afetou pelo menos **1,8 milhão de pessoas,** uma das maiores violações de saúde relatadas naquele ano. E a DaVita, uma das maiores fornecedoras de diálise dos Estados Unidos, sentiu na pele o impacto financeiro de um ataque quando seu ataque de ransomware de 2025 expôs os dados de 2,7 milhões de pacientes, custando à empresa US$ 25 milhões em despesas diretas e mais US$ 15 milhões para resolver os processos judiciais subsequentes.

O custo e a exposição de dados são apenas parte do prejuízo. O cuidado ao paciente é outra parte. Líderes de TI e segurança do setor de saúde relatam que ciberataques contribuíram para piores desfechos em pacientes, desde procedimentos adiados até aumento da mortalidade. No Reino Unido, um ataque de ransomware em 2024 à Synnovis cancelou mais de **1.700 cirurgias** e desencadeou uma escassez de sangue em toda a cidade. Quase dois anos depois, incidentes de segurança do paciente relacionados a resultados patológicos incorretos ou atrasados ainda estavam sendo registrados.

Esses não são casos isolados. Eles mostram que os planos de recuperação ainda não estão otimizados para minimizar o tempo de inatividade, pagamentos de resgate ou impactos no cuidado ao paciente. Igualmente preocupante: **poucos planos são ágeis o suficiente para acompanhar a rapidez com que a IA está mudando a própria ameaça.**

Os dados tornam o impacto claro:

78% (ante 66%)

das organizações de saúde sofreram um ciberataque relevante nos últimos 12 meses, ante 66% no ano anterior.

US $ 6,54 milhões

custo médio de uma violação de dados no setor de saúde, o mais alto entre todos os setores pelo 13º ano consecutivo.

(IBM, Relatório Custo de uma Violação de Dados 2026)

85%

das organizações de saúde atingidas por um ciberataque relevante nos últimos 12 meses excederam seu objetivo de tempo de recuperação, com a recuperação levando **quase o dobro** do tempo planejado

38% (ante 49%)

dos líderes de TI e segurança do setor de saúde têm total confiança em sua estratégia de resiliência cibernética, uma queda acentuada em relação ao ano anterior.

VOCÊ PRECISA DE UMA ENTIDADE MÍNIMA VIÁVEL.

Porque restaurar sistemas não é o mesmo que restaurar o cuidado. Uma Entidade Mínima Viável (MVE) é a capacidade de um sistema de saúde de restaurar seus serviços clínicos mais críticos a um estado confiável, mesmo quando sistemas, registros e identidades foram comprometidos. Ela começa pela identidade e se estende às plataformas de prontuário eletrônico (Epic, Oracle Health, MEDITECH), diagnóstico por imagem, laboratórios e outros serviços críticos. É um modelo operacional de recuperação definido e testado antes de uma crise, não durante ela.

Por que este relatório e por que agora.

Os CISOs e CIOs já sabem que o setor de saúde é um alvo, mas saber por que os planos de recuperação falham pode ser um ponto cego. Este relatório mostra como premissas ultrapassadas estão moldando estratégias de resiliência cibernética, criando lacunas nos planos e aumentando a exposição. Sem resolver essas lacunas, e com as ameaças de IA de fronteira se acelerando, as organizações de saúde podem esperar mais pressão sobre os planos de recuperação existentes.

Os sistemas de saúde são construídos em torno da disponibilidade e da continuidade do cuidado. Ataques cada vez mais sofisticados, combinados a planos de recuperação ultrapassados, tornam isso mais do que um problema técnico. **Recuperação atrasada significa cuidado atrasado.**

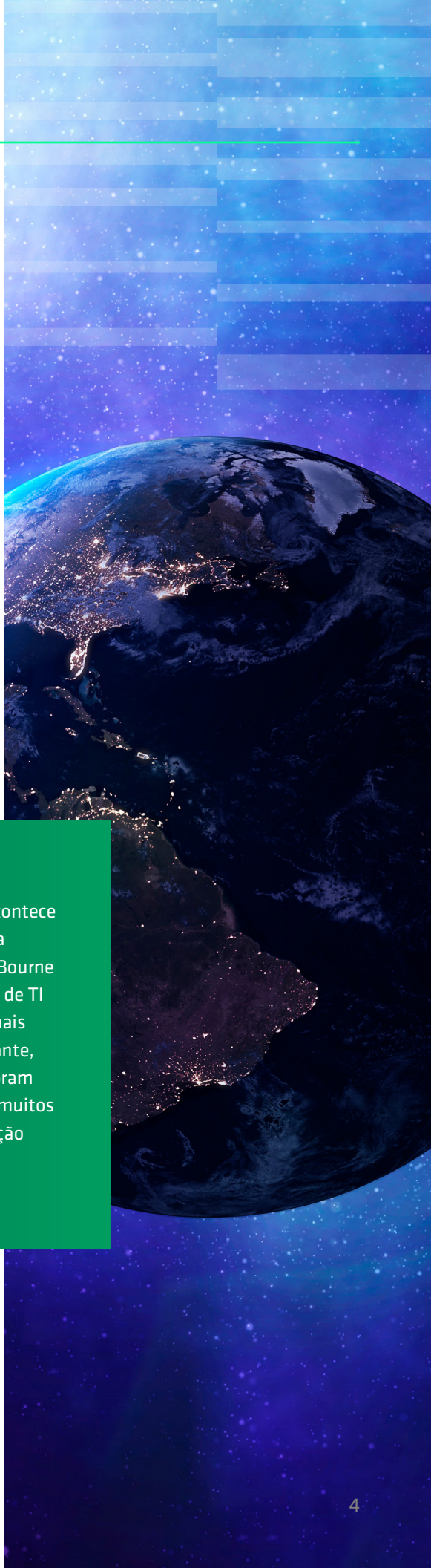
Apenas **16%**

das organizações de saúde têm uma MVE formalmente documentada e testada, e a maioria não validou se ela realmente funcionaria em condições reais.

O problema não é o playbook. É o mundo para o qual ele foi escrito.

A maioria dos playbooks de recuperação cibernética foi criada com base em um conjunto de premissas que faziam sentido na época em que foram escritos. Eles presumiam que o escopo de um incidente seria compreendido, as dependências estariam mapeadas e a recuperação seguiria uma sequência previsível.

O cenário de ameaças atual desafia essas premissas. A IA e os agentes autônomos estão criando novos caminhos de comprometimento e acelerando a rapidez com que vulnerabilidades são descobertas e transformadas em armas. A expansão da nuvem e do SaaS continua aumentando o número de sistemas, serviços e dependências envolvidos na recuperação. À medida que os incidentes avançam, o escopo se amplia, surgem dependências inesperadas e a sequência prevista no plano deixa de corresponder à realidade na prática.



3.200
tomadores de decisão de TI e segurança

1.000+
funcionários por organização

12
países

Para entender melhor como a recuperação acontece nos ambientes atuais, a Cohesity contratou a empresa independente de pesquisa Vanson Bourne para entrevistar 3.200 tomadores de decisão de TI e segurança de organizações com 1.000 ou mais funcionários em 12 países. O relatório resultante, "Os planos de recuperação cibernética não foram projetados para este momento", sugere que muitos ainda dependem de abordagens de recuperação criadas para um mundo que não existe mais.

Este relatório examina as descobertas de 400 respondentes que representam organizações de saúde. Ele revela onde os esforços de recuperação se tornam mais difíceis do que o esperado, como as organizações de saúde estão definindo e testando uma Entidade Mínima Viável (MVE) e como a IA está remodelando tanto as ameaças cibernéticas quanto a resiliência cibernética.

PRINCIPAIS DESCOBERTAS PARA O SETOR DE SAÚDE

A maioria dos planos de recuperação é construída com base em premissas que podem não sobreviver a um ataque real.

Noventa e dois por cento dos respondentes do setor de saúde dizem que seus planos de resposta e recuperação cibernética dependem, em algum grau, de todas as cinco premissas comuns testadas neste estudo. A dependência é maior entre aqueles que expressam total confiança em sua estratégia de resiliência cibernética.

Muitas organizações de saúde concentram seus planos de recuperação na linha de chegada errada.

Mais de três quartos (78%) concordam que seus planos se concentram mais em restaurar sistemas do que em manter operações críticas e atender pacientes durante a recuperação do sistema.

Poucas formalizaram o que precisam para continuar operando durante a recuperação.

Apenas 16% têm uma Entidade Mínima Viável (MVE) formalmente documentada e testada. Desse grupo, 92% dizem que sua MVE informou ou influenciou suas prioridades de recuperação.

A IA está se tornando operacional antes de se tornar recuperável.

Embora 99% dos respondentes usem sistemas de IA, aplicações, fluxos de trabalho ou modelos de aprendizado de máquina, apenas 37% dizem que seus planos de resposta e recuperação cibernética consideram de forma abrangente ataques direcionados a eles.

A IA de fronteira exigirá uma nova geração de planejamento de recuperação cibernética.

Oitenta e cinco por cento dos respondentes do setor de saúde acreditam que seus planos de recuperação atuais exigiriam mudanças moderadas a significativas se a IA de fronteira avançasse capacidades como descoberta de vulnerabilidades, desenvolvimento de exploits e intrusões em múltiplas etapas. Apenas 2% consideram seus planos atuais preparados para essas condições.

5 PREMISSAS QUE SABOTAM A RECUPERAÇÃO CIBERNÉTICA

Todo plano de recuperação é uma aposta. Ele reflete escolhas deliberadas sobre o que as organizações de saúde acreditam que vai acontecer quando um ciberataque ocorrer. O desafio é que o cenário de ameaças atual testa cada vez mais essas crenças. O percentual de tomadores de decisão com total confiança em sua estratégia de resiliência cibernética caiu de 49% em 2025 para 38% em 2026. O percentual dos que relatam que sua estratégia precisa de melhorias subiu de 49% para 61%.

Sua organização tem uma estratégia de resiliência cibernética que você considera adequada para as ameaças e os desafios atuais?

Sim, temos uma estratégia e tenho total confiança nela (ela não precisa de melhoria ou precisa de melhoria mínima)

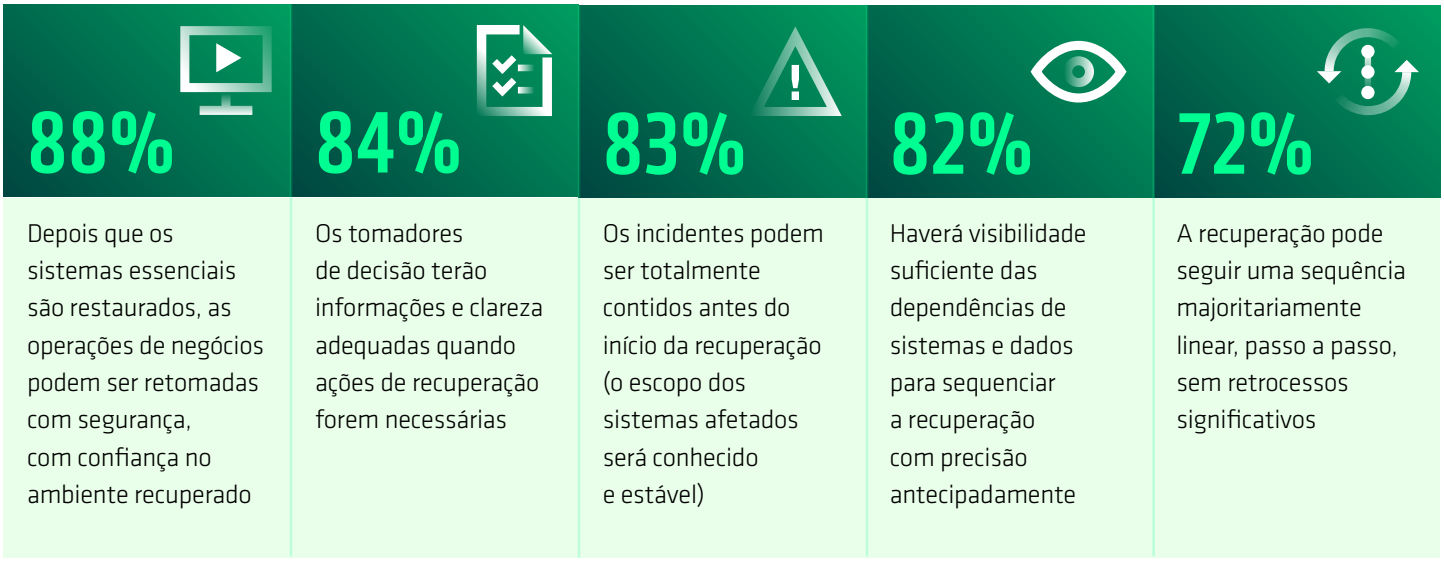
Sim, temos uma estratégia de resiliência cibernética, mas ela requer melhoria

Os números de 2025 são do Relatório Global de Resiliência Cibernética da Cohesity para o Setor de Saúde, publicado em fevereiro de 2026

5 PREMISSAS QUE SABOTAM A RECUPERAÇÃO CIBERNÉTICA

Uma esmagadora maioria dos participantes diz que seus planos de resposta e recuperação dependem de todas as cinco premissas avaliadas neste estudo. A dependência é mais forte entre aqueles que expressam total confiança em sua estratégia de resiliência cibernética e consistentemente menor entre os que acreditam que melhorias significativas são necessárias. Isso sugere que a confiança pode estar mais enraizada em crença do que em testes comprovados nas condições atuais.

Organizações de saúde cujos planos de resposta e recuperação dependem das seguintes premissas em alguma ou grande medida



92%

dos planos de resposta e recuperação cibernética dependem, em algum grau, de todas as cinco premissas comuns

O cenário de ameaças mudou. As prioridades de investimento não.

Se as premissas acima são a aposta, os gastos mostram onde as organizações de saúde estão colocando suas fichas. Perguntamos aos respondentes como o investimento em resiliência cibernética é alocado entre as cinco funções do NIST Cybersecurity Framework: Identificar, Proteger, Detectar, Responder e Recuperar. Em comparação com 2025, os gastos se deslocaram ainda mais para Proteger. Responder e Recuperar continuam recebendo a menor parcela do investimento, representando apenas 33% dos gastos totais em resiliência cibernética. Vale destacar que três quartos (75%) das organizações concordam que seu investimento em resiliência cibernética está excessivamente direcionado à prevenção, em detrimento da resposta e da recuperação.

O PLANEJAMENTO DE RECUPERAÇÃO ENCONTRA A REALIDADE

Nosso estudo faz uma distinção clara entre eventos de segurança do dia a dia e incidentes que interrompem de forma significativa a operação de uma empresa ou organização. Ao longo deste relatório, usamos o termo "ciberataque relevante" para descrever tentativas deliberadas de comprometer, interromper ou obter acesso não autorizado a sistemas, redes ou dados que resultem em impacto financeiro, operacional, reputacional ou ao cliente mensurável. Esses ataques estão se tornando mais frequentes.

O escopo raramente permanece onde começou.

Quase dois terços (64%) das organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses viram o escopo dos sistemas afetados se expandir além da avaliação inicial durante a recuperação. Esses ataques frequentemente se revelam ao longo do tempo. Novos sistemas entram no escopo. Comprometimentos adicionais são descobertos. E as equipes de recuperação se veem respondendo a um incidente maior do que haviam identificado inicialmente.

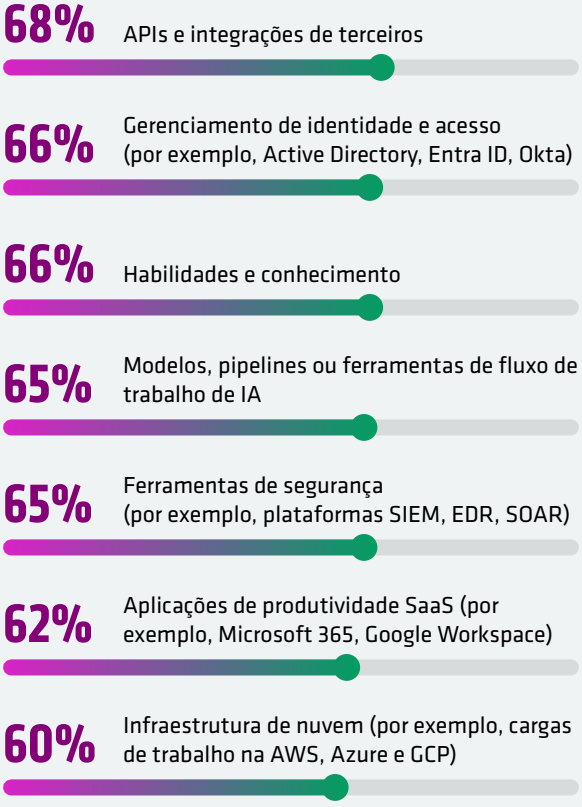
Surgem lacunas de dependência.

Surgiram lacunas em toda a gama de dependências identificadas neste estudo, incluindo modelos e pipelines de IA, integrações de terceiros e gerenciamento de identidade. Entre as organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses, em média 65% encontraram lacunas moderadas a significativas na forma como seus planos de resposta e recuperação consideravam as dependências. As descobertas não apontam para uma única dependência como o principal desafio. Em vez disso, mostram como pode ser difícil prever com antecedência as diversas tecnologias, serviços e pessoas interconectadas das quais a recuperação moderna depende.

- Mais de três quartos (78%) das organizações de saúde afirmam ter sofrido um ciberataque relevante nos últimos 12 meses, ante 66% em 2025.
- Para a grande maioria (85%) dessas organizações, a recuperação real excedeu o objetivo de tempo de recuperação (RTO). Em média, a recuperação levou quase o dobro do tempo do RTO.
- Oitenta e cinco por cento também afirmam que seu plano de recuperação provavelmente exigirá soluções paliativas ou improvisação durante um ataque real.

Durante o ciberataque, em que medida sua organização identificou lacunas na forma como seu plano de resposta e recuperação considerava as seguintes dependências?

Significant or moderate gaps



Exibindo dados das organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses.

O PLANEJAMENTO DE RECUPERAÇÃO ENCONTRA A REALIDADE

Restaurado não significa pronto.

Colocar um sistema de volta online não é o mesmo que confiar nele. Antes de reconectar sistemas ou dados restaurados aos ambientes de produção, os respondentes utilizaram uma série de práticas de validação, incluindo verificações de integridade de dados, varreduras de segurança, validação de dependências e testes isolados. No entanto, nenhum método único foi aplicado de forma consistente, e a revisão forense independente de terceiros foi a prática de verificação menos comum.

Antes de reconectar sistemas ou dados restaurados aos ambientes de produção, que etapas sua organização adotou para verificar se eram seguros para uso?

55%

Validou se as principais dependências estavam funcionando corretamente antes de reconectar

51%

Realizou verificações de integridade de dados antes de reconectar sistemas ou dados restaurados

49%

Verificou pontos de restauração em relação a backups reconhecidamente íntegros ou imutáveis

47%

Executou varreduras de segurança ou de ameaças nos dados ou sistemas restaurados

46%

Testou os sistemas restaurados em um ambiente isolado ou limpo

36%

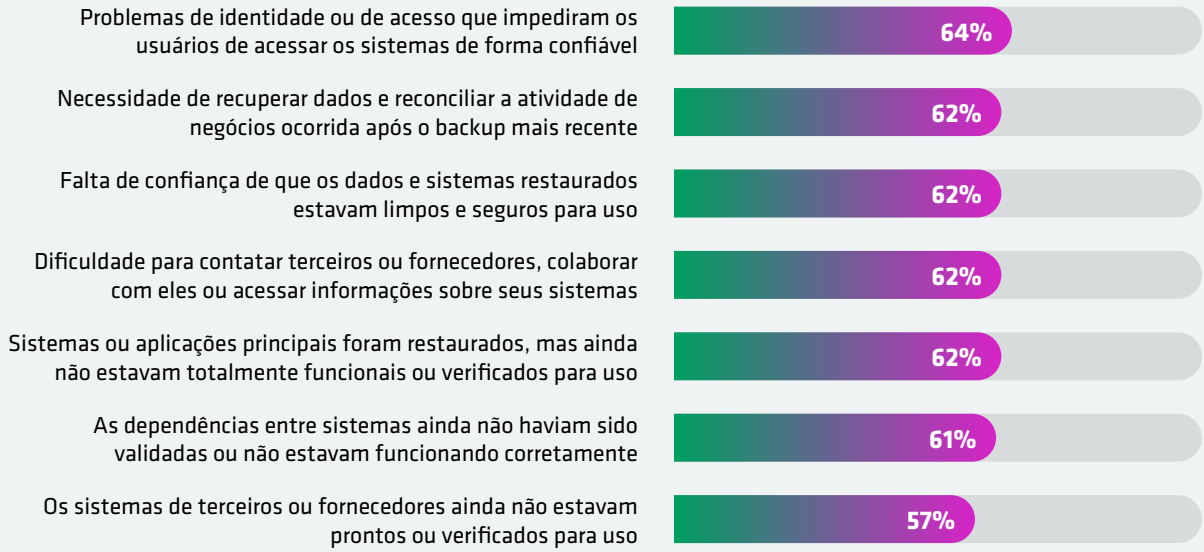
Usou revisão forense de terceiros para validar os sistemas antes de reconectar

Exibindo dados das organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses.

O PLANEJAMENTO DE RECUPERAÇÃO ENCONTRA A REALIDADE

Restaurar sistemas pode ser um marco na recuperação, mas, para muitos, não é o ponto em que as operações normais podem ser retomadas com segurança. Por exemplo, 69% das organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses admitem que nem sempre testam os sistemas de identidade após o ataque para verificar se os mecanismos de persistência e o acesso do invasor foram eliminados. Em muitos casos, os atrasos também continuam muito depois de os sistemas terem sido tecnicamente restaurados. Aproximadamente três em cada cinco participantes que sofreram um ciberataque relevante nos últimos 12 meses também relataram atrasos moderados ou significativos relacionados a todos os fatores medidos neste estudo.

Depois que os sistemas foram restaurados após o ciberataque, em que medida cada um dos itens a seguir atrasou a capacidade de sua organização de retomar as operações normais de negócios?



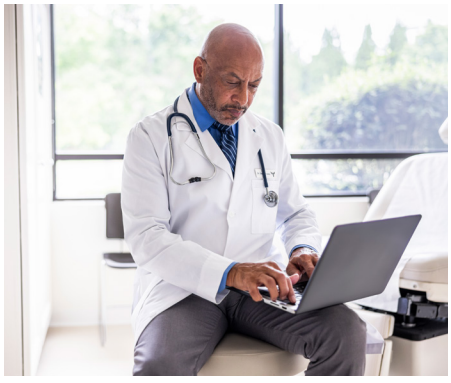
Exibindo dados das organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses.

Organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses

73%
encontraram todos os sete fatores de atraso na recuperação

83%
concordam que diferenças entre as equipes de TI e de segurança podem atrasar as decisões sobre quando é seguro colocar os sistemas de volta online

74%
priorizam a velocidade de recuperação em detrimento da certeza de que os sistemas restaurados estão limpos e seguros



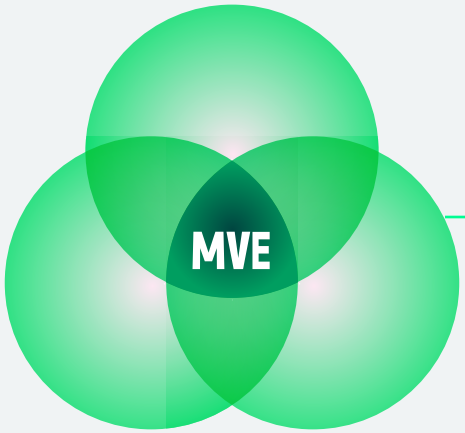
O POTENCIAL DA MVE CONTINUA EM GRANDE PARTE INEXPLORADO

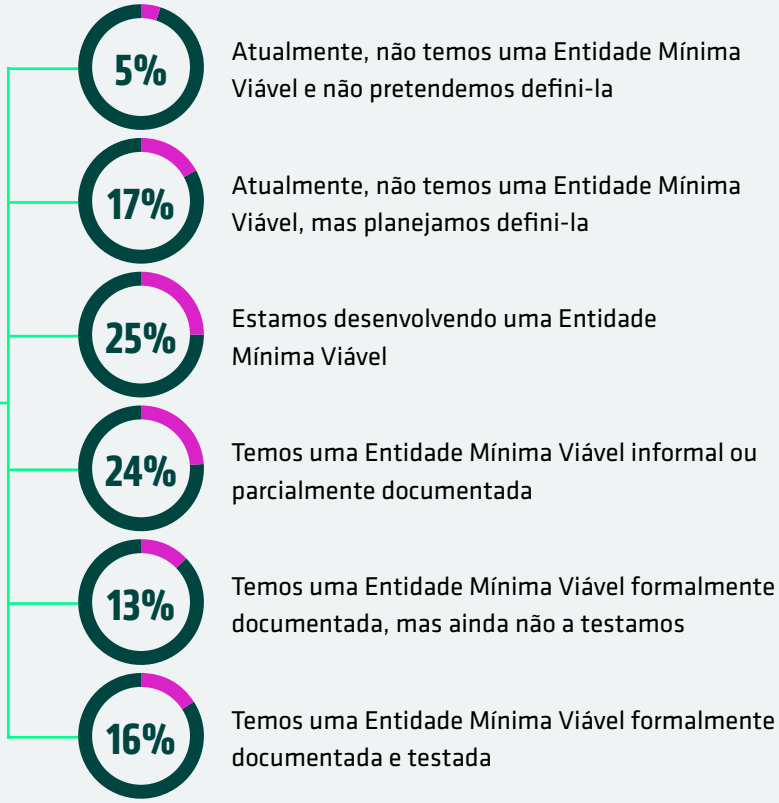
A dependência de premissas questionáveis e de abordagens ultrapassadas de resposta e recuperação ajuda a explicar por que tantos planos permanecem focados na restauração de sistemas. Mais de três quartos (78%) dos tomadores de decisão de TI e segurança do setor de saúde concordam que seu plano de resposta e recuperação cibernética se concentra mais em restaurar sistemas do que em como o sistema de saúde ou organização continuará a atender pacientes e manter operações críticas durante a recuperação.

Uma MVE é o conjunto mínimo de capacidades clínicas e operacionais – atendimento de emergência, administração de medicamentos, acesso a registros de pacientes – que uma organização de saúde deve manter em funcionamento enquanto a recuperação mais ampla continua. É um modelo operacional definido sobre o que mais importa, decidido antes de uma crise ocorrer.

Apesar da atenção crescente ao planejamento da MVE, relativamente poucas organizações de saúde têm uma MVE formalmente documentada e testada. Apenas 16% dos participantes dizem ter feito isso. Entre aqueles com uma MVE formalmente documentada e testada, no entanto, 92% dizem que ela informou ou influenciou suas prioridades de recuperação. Dentro desse grupo, 61% dizem que a MVE determinou diretamente o que foi priorizado e restaurado primeiro durante um ciberataque.

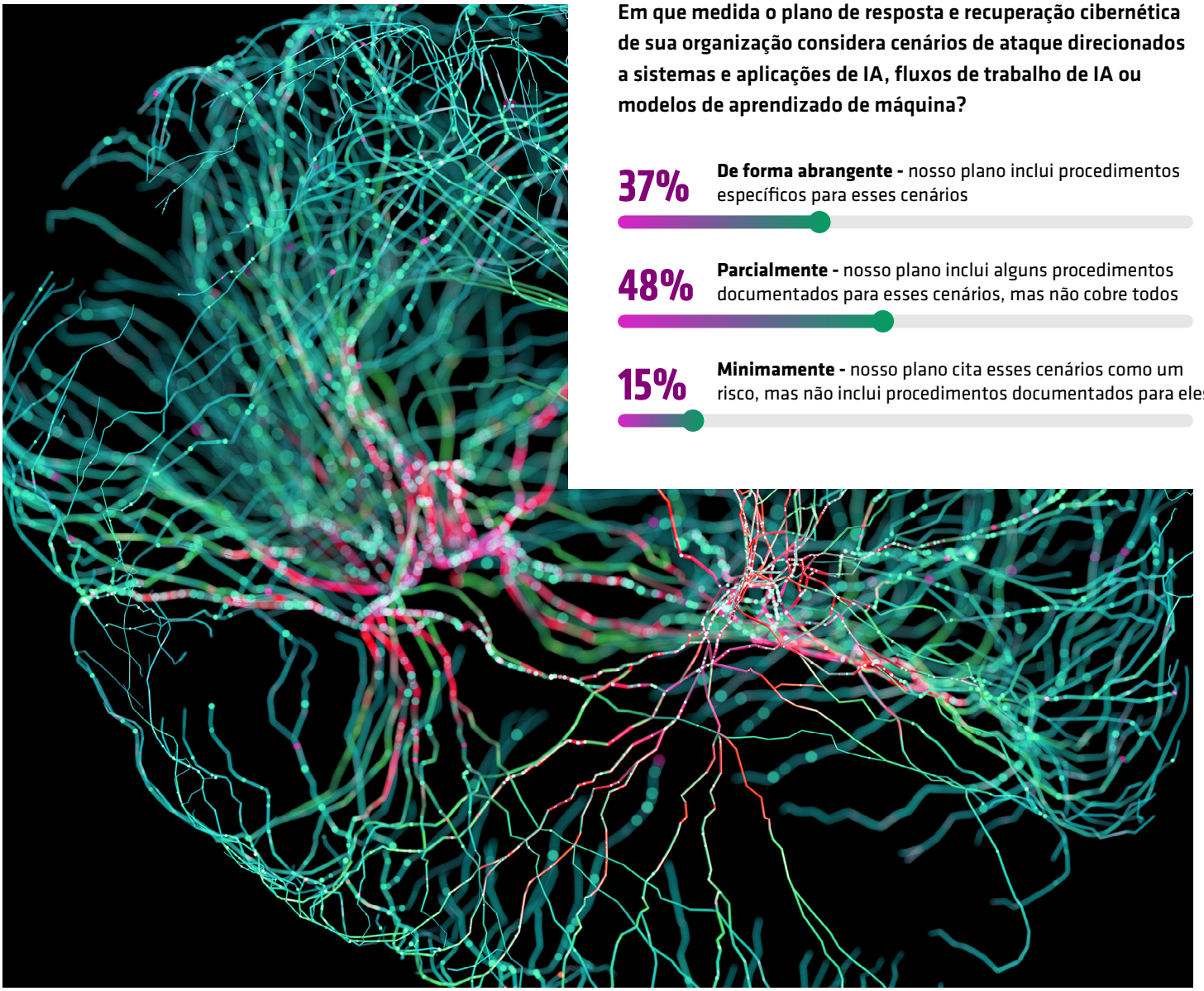
Qual das opções a seguir melhor descreve a abordagem atual de sua organização para definir uma Entidade Mínima Viável?





A IA ESTÁ SE TORNANDO OPERACIONAL ANTES DE SE TORNAR RECUPERÁVEL

Cada premissa explorada neste relatório se torna mais difícil de sustentar quando a IA entra no ambiente. A IA introduz novos sistemas, fluxos de trabalho, modelos e dependências que precisam ser compreendidos, protegidos e recuperados. No entanto, o planejamento de recuperação não acompanhou o ritmo da adoção da IA. Embora 99% dos respondentes do setor de saúde relatem usar sistemas de IA, aplicações, fluxos de trabalho ou modelos de aprendizado de máquina, apenas 37% dizem que seu plano de resposta e recuperação cibernética considera de forma abrangente cenários em que esses poderiam ser atacados.



Em que medida o plano de resposta e recuperação cibernética de sua organização considera cenários de ataque direcionados a sistemas e aplicações de IA, fluxos de trabalho de IA ou modelos de aprendizado de máquina?

37% **De forma abrangente -** nosso plano inclui procedimentos específicos para esses cenários

48% **Parcialmente -** nosso plano inclui alguns procedimentos documentados para esses cenários, mas não cobre todos

15% **Minimamente -** nosso plano cita esses cenários como um risco, mas não inclui procedimentos documentados para eles

A IA ESTÁ SE TORNANDO OPERACIONAL ANTES DE SE TORNAR RECUPERÁVEL

Essa lacuna vai além do planejamento de recuperação. As organizações de saúde também precisam ser capazes de verificar se os modelos de IA, os dados associados e os processos orientados por IA permanecem confiáveis após um incidente. Sessenta e um por cento não estão muito confiantes em sua capacidade de verificar a integridade dos modelos de IA e dos dados relacionados após um ciberataque. A confiança, porém, varia significativamente com base na maturidade do planejamento de recuperação de IA. Entre os participantes que consideram de forma abrangente cenários de ataque específicos de IA em seus planos de recuperação, 72% estão muito confiantes em sua capacidade de verificar a integridade da IA, em comparação com apenas 21% dos que consideram esses cenários parcialmente e 17% dos que os consideram minimamente.

Qual o grau de confiança de sua organização, se houver, na capacidade de verificar a integridade dos modelos de IA e dos dados associados após um incidente cibernético?

39%

Muito confiante

temos procedimentos e ferramentas estabelecidos para verificar a integridade dos modelos de IA e dos dados associados

54%

Razoavelmente confiante

temos alguma capacidade, mas reconhecemos lacunas

6%

Pouco confiante

não temos ferramentas ou processos adequados para verificar a integridade dos modelos e dos dados de IA

1%

Nada confiante

não temos nenhuma capacidade de verificar a integridade dos modelos de IA ou dos dados após um incidente

De forma semelhante, 58% dizem não estar 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. Para organizações de saúde cujos planos de recuperação consideram de forma abrangente cenários relacionados à IA, a preparação aumenta substancialmente (84%). Apenas 18% das organizações cujos planos consideram esses cenários apenas parcialmente dizem estar bem preparadas, caindo para 16% entre aquelas cujos planos os consideram minimamente.

Qual o nível de preparação de sua organização para detectar e conter ações não intencionais ou incorretas realizadas por agentes de IA, copilotos ou fluxos de trabalho de IA, e recuperar sistemas ou dados afetados?

42%

Estamos bem preparados,
com processos estabelecidos e testados para detectar, conter e nos recuperar desses cenários

44%

Temos processos
para detectar, conter e nos recuperar desses cenários, mas eles não estão totalmente desenvolvidos ou testados

13%

Temos capacidade limitada
para detectar, conter ou nos recuperar desses cenários

1%

Não estamos preparados
para gerenciar esses cenários

A IA ESTÁ SE TORNANDO OPERACIONAL ANTES DE SE TORNAR RECUPERÁVEL

A IA muda o que a recuperação deve provar.

Embora a maioria das organizações de saúde já esteja incorporando a IA às operações do dia a dia, muitas acreditam que o maior desafio ainda está por vir. Perguntamos o quanto os planos de recuperação existentes precisariam mudar para continuar eficazes se a IA de fronteira continuasse avançando capacidades como descoberta de vulnerabilidades, desenvolvimento de exploits e intrusões em múltiplas etapas. Essa pergunta não era sobre ataques que as organizações já haviam sofrido. Era sobre se os planos de recuperação estão preparados para o que vem a seguir. Quase todos os participantes do setor de saúde pesquisados (97%) disseram que mudanças são necessárias para lidar com ameaças emergentes das capacidades de IA de fronteira.

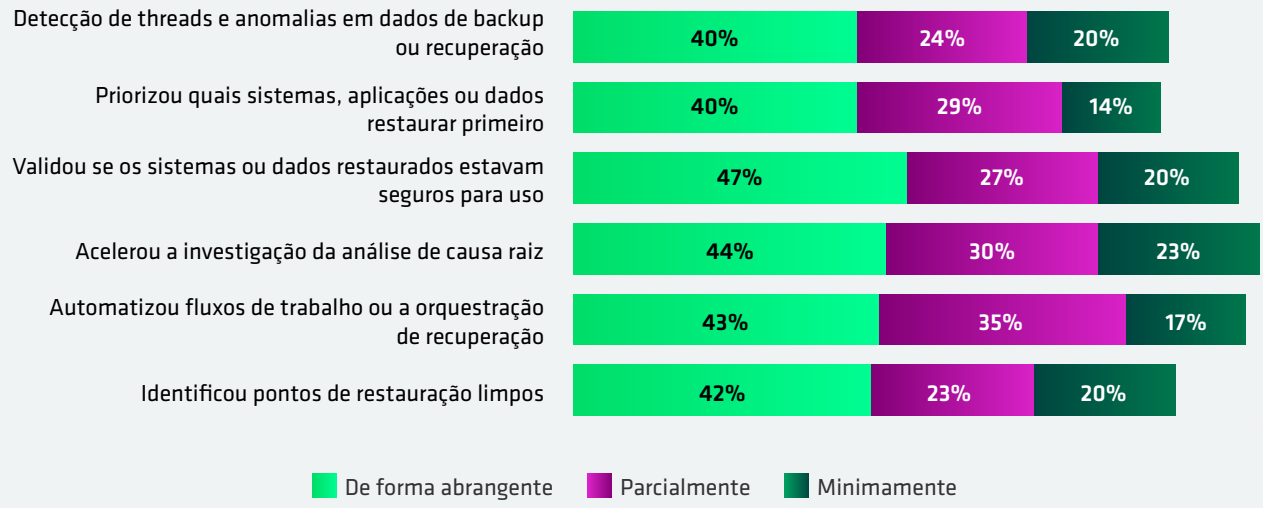
- Apenas 2% dizem que seu plano de recuperação atual está preparado para resistir a elas
- Oitenta e cinco por cento dizem que seriam necessárias mudanças moderadas a significativas para lidar com ataques baseados em IA de fronteira

Onde a IA já está ajudando a defesa.

As organizações de saúde que sofreram um ciberataque relevante nos últimos 12 meses também relatam usar ferramentas com IA em uma ampla gama de processos de resposta e recuperação. Mais de quatro em cada cinco (81%) dizem que essas ferramentas trouxeram uma contribuição moderada a significativa em todas as áreas medidas, em média, desde a detecção de ameaças e análise de causa raiz até a orquestração da recuperação e a identificação de pontos de restauração limpos.

Além disso, as organizações que consideram de forma abrangente cenários de ataque direcionados a sistemas, aplicações, fluxos de trabalho ou modelos de IA também são consistentemente mais propensas a relatar contribuições significativas de ferramentas com IA durante a resposta e a recuperação. As mesmas organizações que se preparam para a IA como parte da superfície de ataque costumam ser as que usam a IA de forma mais eficaz durante um ataque.

As ferramentas com IA contribuíram de forma significativa nas seguintes áreas durante o ciberataque relevante



O plano de resposta e recuperação considera cenários de ataque direcionados a sistemas, aplicações, fluxos de trabalho ou modelos de ML de IA

RECUPERAÇÃO PARA ESTE MOMENTO E PARA O PRÓXIMO

Se a maioria dos planos de recuperação cibernética não foi concebida para um mundo em constante mudança, a próxima geração de planejamento de recuperação precisa ser. Em um ambiente em que as vulnerabilidades são exploradas mais rapidamente, os caminhos de ataque se multiplicam e a IA está remodelando tanto o cenário de ameaças quanto as operações de negócios, a resiliência depende de testar continuamente as premissas antes que uma crise as coloque à prova.

A próxima geração de planejamento de resposta e recuperação começa com algumas mudanças fundamentais:

- Não se limite a documentar seu plano de recuperação. Teste-o em condições realistas.
- Vá além da recuperação de sistemas. Pense nos impactos mais amplos, incluindo o cuidado ao paciente. Defina e teste uma Entidade Mínima Viável.
- Trate a identidade e outras dependências críticas mapeadas como bases da recuperação.
- Garanta que os sistemas e dados recuperados sejam confiáveis, e não apenas restaurados.
- Estenda práticas de recuperação confiáveis a modelos, agentes e fluxos de trabalho de IA.

Descubra ferramentas e orientações para transformar o planejamento em prontidão operacional.

- Explore as soluções de resiliência cibernética para o setor de saúde.

METODOLOGIA

A Cohesity contratou a Vanson Bourne para entrevistar 3.200 tomadores de decisão de TI e segurança em julho de 2026, base destas descobertas. Os respondentes representam organizações nos EUA (500), Brasil (200), Reino Unido (400), Alemanha (400), França (400), Emirados Árabes Unidos/Arábia Saudita (100), Austrália (200), Coreia do Sul (200), Japão (400), Índia (200) e Cingapura (200). Este relatório reflete as percepções de 400 participantes de organizações de saúde. As comparações ano a ano ao longo do relatório referem-se às descobertas de 2025 do Relatório de Resiliência Cibernética da Cohesity para o Setor de Saúde, publicado em fevereiro de 2026.

COHESITY

cohesity.com | 1-855-926-4374 | 2625 Augustine Drive, Santa Clara, CA 95054

© 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. 2000135-001- ptBR