Noventa por cento confiam. Vinte e oito por cento recuperam.

As pesquisas de resiliência publicadas ao longo de 2026 chegam ao mesmo lugar por caminhos diferentes: quase todo mundo acredita que recupera dentro do prazo, e quase ninguém já provou isso em condição parecida com a real.

Em uma frase. Nove em cada dez líderes de segurança afirmam que a organização recupera de um ataque dentro do prazo definido, mas menos de três em cada dez vítimas de ransomware recuperaram todos os dados. A lacuna não está na tecnologia de backup, que está instalada na maioria dos ambientes. Está na ausência de ensaio em condição realista.

Uma ressalva metodológica

Pesquisa de resiliência mede duas coisas ao mesmo tempo e costuma apresentá-las como se fossem uma. A primeira é o que o respondente acredita. A segunda é o que aconteceu com quem foi atacado. São populações diferentes respondendo perguntas diferentes, e é exatamente por isso que o contraste entre elas diz alguma coisa: de um lado, confiança declarada por quem ainda não precisou; do outro, resultado apurado por quem precisou.

Os indicadores de 2026

Indicador	Resultado	O que ele mede
Confiança no prazo de recuperação	cerca de 90%	Líderes que acreditam recuperar dentro do prazo definido internamente.
Recuperação integral dos dados	cerca de 28%	Vítimas de ransomware que recuperaram tudo, não apenas parte.
Superestimação da prontidão	65%	Organizações que avaliam a própria capacidade acima do que a evidência sustenta.
Postura nunca demonstrada em condição realista	64,6%	Ambientes em que a recuperação não foi exercitada fora do cenário ideal.
Cópia isolada disponível	62%	Existência de backup fora do alcance do atacante.
Capacidade de validar integridade	36%	Confirmação de que o dado restaurado é utilizável, não apenas legível.
Ambiente limpo pronto para restauração	51%	Local para onde restaurar sem reinfectar a partir do mesmo comprometimento.
Ensaio do plano nos últimos doze meses	menos de 50%	Exercício real, não teste pontual de restauração de arquivo.

Duas linhas dessa tabela merecem leitura conjunta. Sessenta e dois por cento têm cópia isolada; trinta e seis por cento conseguem validar a integridade dela. A diferença de vinte e seis pontos é o espaço onde mora a

maior parte das recuperações que falham. Ter o backup e ter o backup que funciona são estados distintos, e a rotina noturna que termina sem erro só atesta o primeiro.

De onde vem a distância

1. O teste mede a parte fácil

O teste de restauração padrão pega um arquivo, às vezes uma máquina virtual, e devolve para o mesmo ambiente de onde saiu. É um teste legítimo do software de backup. Não é um teste de recuperação. Recuperar depois de ransomware significa restaurar centenas de sistemas interdependentes, em ordem, para uma infraestrutura que ainda não se sabe se está limpa, enquanto o negócio pergunta de hora em hora quando volta.

2. Não há para onde restaurar

Metade das organizações não tem ambiente limpo preparado. Na prática, a recuperação começa por construir o lugar onde ela vai acontecer — provisionar rede, identidade, DNS, autenticação — enquanto a produção está parada. Esse trabalho não estava no cronograma porque, no papel, o plano começava na restauração.

3. A identidade é o gargalo silencioso

Quase nenhum plano de continuidade escrito antes de 2023 trata o diretório de identidade como primeiro item da fila. Em um ambiente comprometido, ele é. Restaurar aplicação sem ter resolvido a autenticação entrega sistema que ninguém consegue acessar, ou pior, sistema acessível com as mesmas credenciais que o atacante já tinha.

4. A ordem de retomada é técnica, não de negócio

Quando a lista de prioridade é um inventário de servidores, a decisão de o que volta primeiro acaba sendo tomada no calor do incidente por quem tem o teclado na mão. Em quase todos os casos em que a recuperação passou de dias para semanas, essa decisão foi revista mais de uma vez no meio do caminho.

O recorte brasileiro

— A comunicação tem prazo e a recuperação não tem. O artigo 48 da LGPD exige comunicação em prazo razoável quando há risco relevante ao titular. Quem ainda tenta subir o diretório de identidade no quarto dia não tem como dizer o que foi acessado.

— O seguro passou a perguntar por evidência. A renovação de apólice cibernética em 2026 já pede registro de ensaio e prova de imutabilidade da cópia. Declaração de intenção não sustenta mais a subscrição.

— Terceiro crítico não entra no ensaio. Folha de pagamento, emissor de nota fiscal, gateway de pagamento e operador logístico estão fora do escopo do exercício na maioria das empresas.

— Setor regulado tem exigência própria. Instituições sob a Resolução Conjunta nº 6 e a Resolução nº 4.893 do Banco Central respondem por continuidade com critério mais duro do que o do restante do mercado.

Três evidências que substituem a pergunta genérica

Perguntar ao time de tecnologia se a empresa consegue se recuperar produz sempre a mesma resposta. Estas três perguntas produzem respostas diferentes entre si, e é isso que as torna úteis em conselho e em comitê de auditoria.

Evidência	O que pedir	Critério de reprovação
Último ensaio completo	Data e escopo do exercício com ambiente limpo, ordem de retomada aplicada e tempo medido até o serviço de negócio disponível.	Data anterior a doze meses, ou escopo restrito a restauração de arquivo.
Validação de integridade	Registro de que o dado restaurado foi verificado e de que a cópia isolada é imutável no período de retenção declarado.	Evidência limitada ao log de conclusão da rotina de cópia.
Ordem de retomada	Lista priorizada de processos de negócio com prazo tolerável definido e assinado pela área dona.	Lista de servidores, ou documento sem assinatura da área de negócio.

Roteiro de noventa dias

Período	Entrega	Como saber que terminou
Dias 1 a 30	Levantar os processos de negócio que não podem parar por mais de vinte e quatro horas, com dono e prazo tolerável declarado por essa pessoa.	Lista assinada, com no máximo quinze processos e um responsável nomeado por linha.
Dias 31 a 60	Verificar a integridade do backup dos três sistemas mais críticos por restauração real em ambiente separado.	Relatório com tempo gasto e a lista de obstáculos encontrados, inclusive os burocráticos.
Dias 61 a 90	Exercício de mesa com comprometimento do diretório de identidade, áreas de negócio presentes e cronômetro visível.	Número único: a diferença entre o prazo do plano e o prazo estimado no ensaio.

Perguntas para o comitê de auditoria

— Quando foi o último exercício completo de recuperação, e qual foi o tempo medido até o primeiro processo de negócio voltar?

— Onde está o registro de validação de integridade do backup dos sistemas críticos, e quem o assina?

— Qual é a ordem de retomada aprovada, e quais áreas de negócio assinaram o prazo tolerável de cada processo?

— Quais terceiros críticos estão no escopo do plano, e algum deles já participou de um ensaio conjunto?

— Se o diretório de identidade for comprometido, qual é o primeiro passo documentado e quem o executa?

Leitura LATAMSEC

A parte desconfortável desta análise não é o percentual de quem falha ao recuperar. É o percentual de quem acredita que não vai falhar. Confiança alta com evidência baixa não é otimismo: é uma medida errada que já foi usada para decidir orçamento, definir apetite de risco e responder a pergunta de conselho.

Corrigir isso não exige comprar nada. Exige trocar a pergunta. Em vez de perguntar se a empresa consegue se recuperar, perguntar quando ela demonstrou isso pela última vez, em que condição, e onde está o registro. As três respostas cabem em uma página, e a maioria das organizações vai descobrir que não consegue escrever essa página hoje.

Fontes

— Arcserve · 65% of organizations overestimate ransomware recovery readiness — dado de superestimação e percentual que nunca demonstrou a postura em condição realista.

— BullWall · 2026 Ransomware Resilience Benchmark Report — contraste entre confiança declarada e prazo de recuperação observado em campo.

— Gartner · IT Resilience Survey for 2026: ransomware recovery and readiness — capacidade existente e não utilizada por falta de estratégia integrada.

— Tech Observer · Cyber recovery confidence gap: only 28% recover ransomware data — percentuais de backup isolado, validação de integridade e ambiente limpo.