Resiliência cibernética em ação

Referência da prontidão empresarial global para proteger/detectar/recuperar
Discussão de insights
Janeiro de 2026

DELL Technologies

Programação

- Objetivos e perfil das empresas
- A lacuna da resiliência cibernética
- Seguro
- Detectar
- Recuperar
- Complexidade, cultura e o que está por vir

Objetivos de negócios

- Posicionar a Dell como líder de ideias e parceira estratégica para resiliência cibernética
- Reafirmar a decisão de se afastar do rótulo de "proteção de dados" para adotar a "resiliência cibernética"

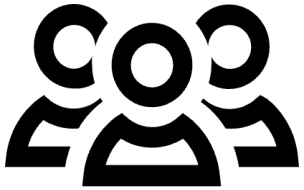
Objetivos da pesquisa

- Avaliar a maturidade e a integração das estratégias de resiliência cibernética
- Avaliar a eficácia das práticas das organizações para proteger, detectar e recuperar
- Entender as barreiras para melhorar a resiliência cibernética, incluindo lacunas de habilidades, orçamento e complexidade
- Descobrir como as organizações estão protegendo o ambiente de TI e os dados contra ameaças de ransomware

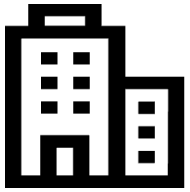
Quem entrevistamos?

As entrevistas foram feitas em julho e outubro de 2025

850 responsáveis pelas decisões de TI de organizações globais



Organizações com mais de 1.000 funcionários



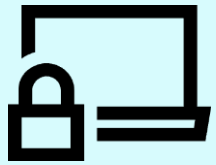
Organizações dos setores público e privado

Foram entrevistados: membros do conselho; gerentes de nível executivo e sênior; gerentes de nível intermediário

Principais constatações

39%

das organizações têm uma estratégia de resiliência cibernética totalmente estabelecida e continuamente otimizada



A otimização contínua é fundamental. Sem ela, as estratégias podem ficar rapidamente desatualizadas contra as ameaças em evolução, deixando as organizações em maior risco

46%

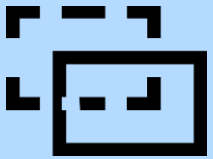
reconhecem que os dados de backup não estão tão protegidos quanto deveriam

Fortalecer a proteção do backup é essencial para garantir que a recuperação continue possível quando os sistemas primários estiverem comprometidos.

Proteger

30%

usam uma plataforma abrangente para detecção de ameaças em rede, backup e armazenamento primário



Sem a detecção unificada, a visibilidade das ameaças e os tempos de resposta podem ser mais lentos, aumentando o risco de violações não detectadas.

Detectar

55%

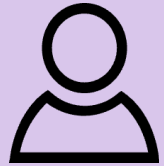
dos que realizaram simulações de ataques cibernéticos mensalmente ou com mais frequência se recuperaram com sucesso de um exercício/incidente cibernético

Os testes frequentes ajudam as equipes a se prepararem para acontecimentos reais. Equipes despreparadas correm o risco de atrasar a resposta e a recuperação nos momentos necessários.

Recuperar

63%

acreditam que a liderança superestima a prontidão da organização para um grande evento cibernético



O excesso de confiança pode atrapalhar os investimentos, atrasar o planejamento de respostas e deixar vulnerabilidades críticas sem tratamento.

DELL Technologies

Seção 1: A lacuna da resiliência cibernética

Entender o problema e a urgência de evoluir

A otimização contínua das estratégias de resiliência melhora a recuperação, mas não garante o sucesso

99,5%

têm algum tipo de estratégia de resiliência cibernética

39%

acreditam estar totalmente estabelecidas e continuamente otimizadas (uma estratégia madura)

57%

não contiveram nem se recuperaram efetivamente durante o último teste ou incidente

Organizações com estratégias maduras de resiliência cibernética têm **2,6 vezes mais chances de se recuperarem** com sucesso

65% versus **25%**

63%

acreditam que a **liderança superestima a prontidão** para um grande evento cibernético

Por que isso é importante agora

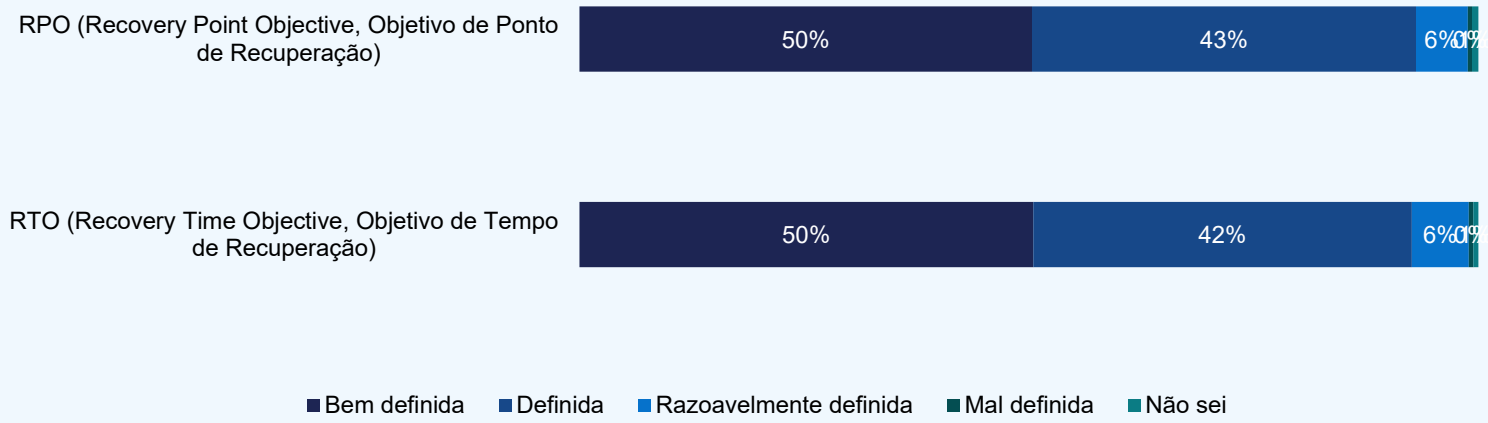
97%

Concordam que a organização precisa se fortalecer continuamente à medida que as ameaças evoluem

78%

acreditam que a organização se concentra mais em prevenir ataques do que na preparação para se recuperar deles

O nível que as organizações definiram:



32%

Têm **ambas as áreas** bem definidas

Com uma estratégia de resiliência cibernética madura

58%

Têm tanto RTO quanto RPO bem definidos

Seção 2: Proteger

Prevenir ataques e fortalecer o patrimônio digital

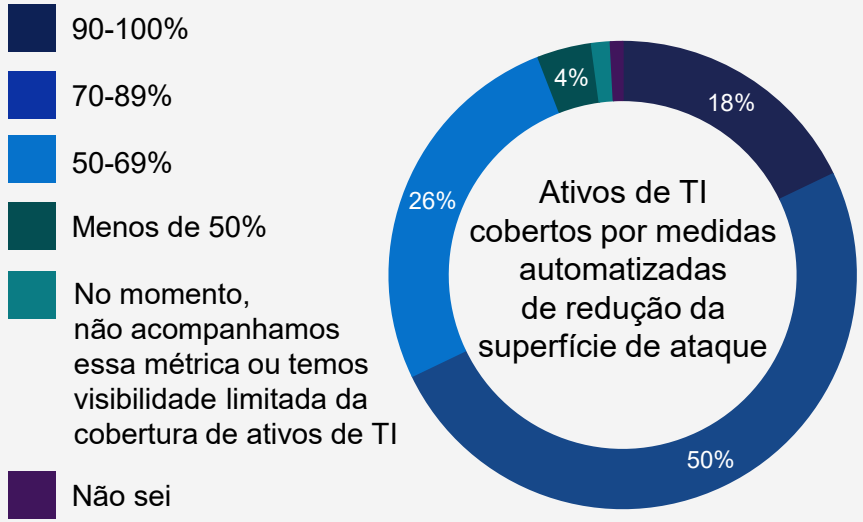
Lacunas de visibilidade e deficiências na proteção

46%

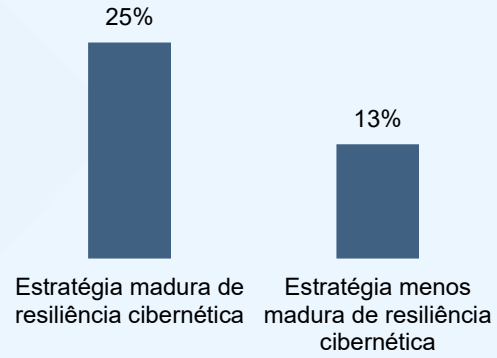
admitem que os dados de backup não estão tão protegidos quanto deveriam

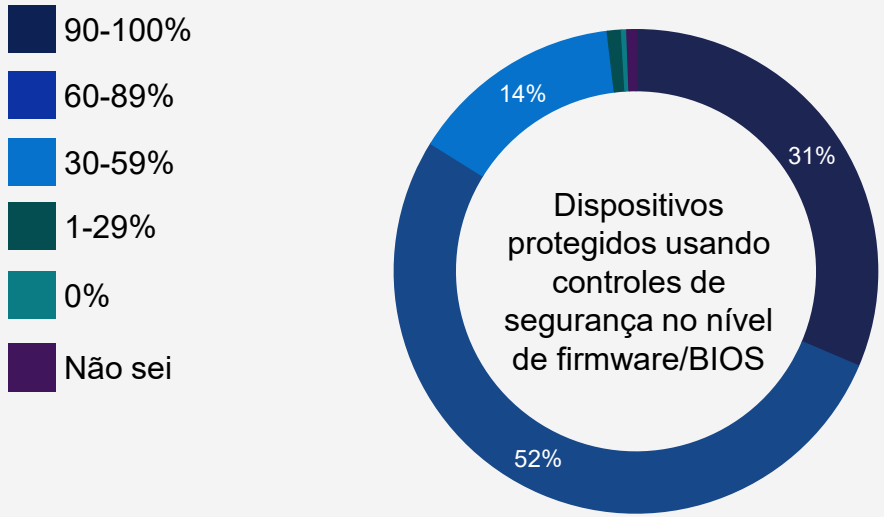
NA	**59%**
EMEA	**43%**
LATAM	**41%**
APJ	**39%**

A otimização contínua não elimina as lacunas de cobertura, mas dá às organizações uma vantagem essencial em resiliência

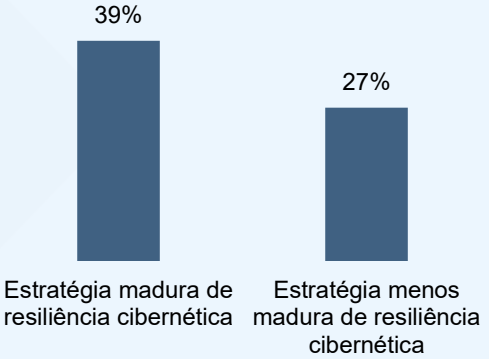


Organizações com cobertura de 90 a 100%:





Organizações com cobertura total ou quase total (90% a 100%):



Da integridade pré-implementação à recuperação pós-ataque: Fortaleça os dois lados da segurança

Processos/métodos usados pelas organizações para garantir a integridade do hardware/software de TI

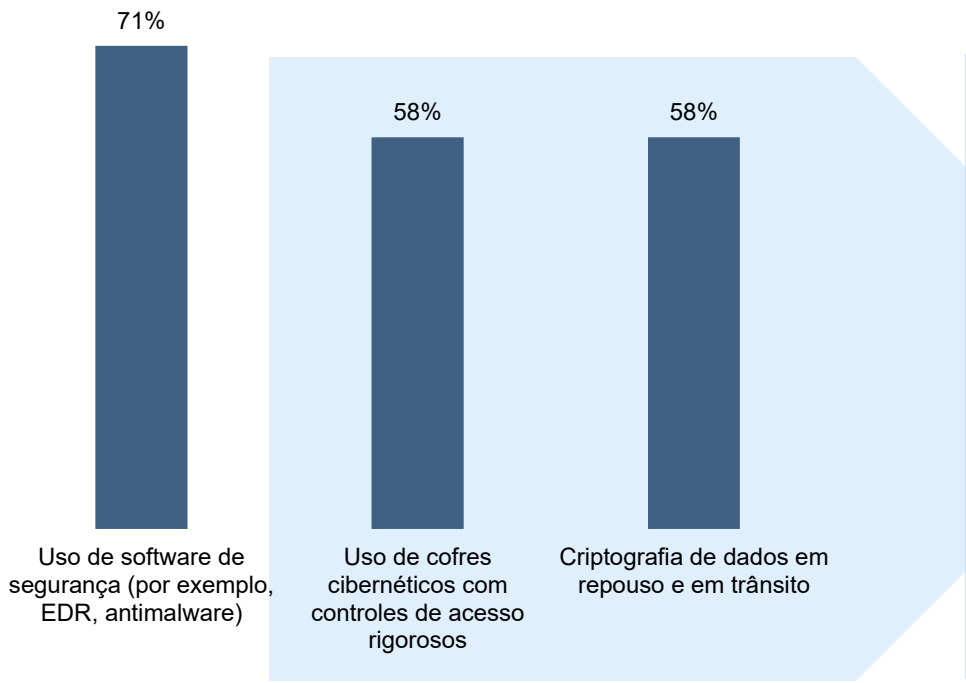
72%

contam com fornecedores para obter certificações, atestados e sistemas com ferramentas incorporadas que verificam a integridade dos componentes

64%

realizam auditorias internas ou análises manuais durante a preparação/implementação

Métodos usados pelas organizações para proteger dados essenciais contra ataques de ransomware



Organizações com estratégias maduras de resiliência são mais propensas a usar:

- **Criptografia de dados (59% versus 57%)**
- **Cofres cibernéticos (63% versus 55%)**

do que organizações com estratégias de resiliência menos maduras

Seção 3: Detectar

Identificar e responder a ameaças antes que causem impacto

Usar IA e automação pode revelar ameaças antes que elas comprometam os backups

38%

das organizações usam ferramentas de IA/ML com guias estratégicos proativos de redução e resposta

Organizações com uma estratégia madura de resiliência cibernética são **3,1 vezes mais** propensas a fazer isto

65% versus **21%**

48%

das organizações usam **IA/ML extensivamente para verificar os dados de backup** em busca de indicadores de comprometimento

O **uso extensivo** de IA/ML ocorre **2,3 vezes mais frequentemente em organizações com uma estratégia madura de resiliência cibernética**

72% versus **32%**

83%

acreditam que os agentes de ameaça estão **atacando cada vez mais os backups** durante ataques de ransomware

62% estão priorizando o investimento em automação e detecção de ameaças com IA/ML

A visibilidade incompleta aumenta os riscos

54%

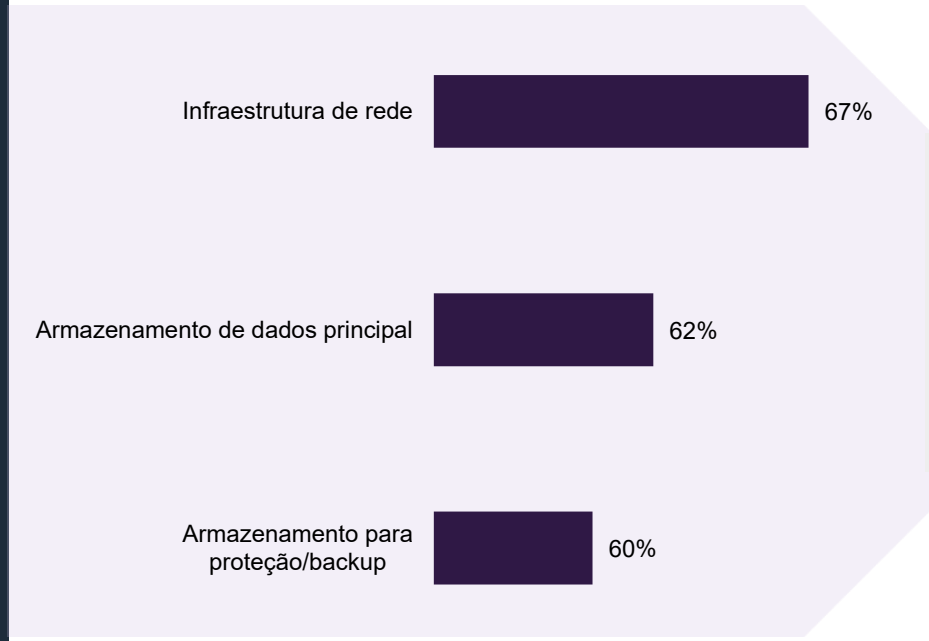
dizem que têm alta visibilidade de atividades suspeitas ou dados comprometidos nos sistemas de backup

74% Organizações com uma estratégia madura de resiliência cibernética

versus

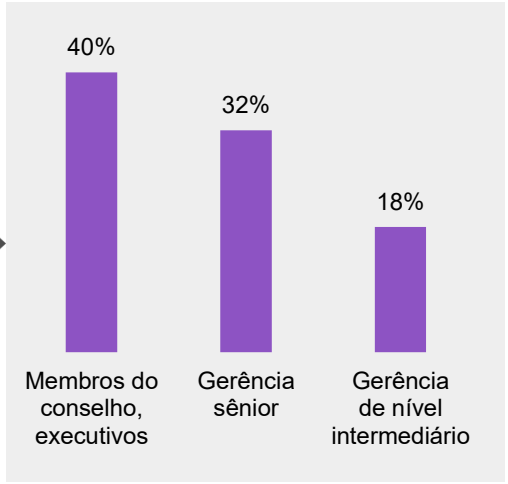
42% das organizações com uma estratégia menos madura de resiliência cibernética

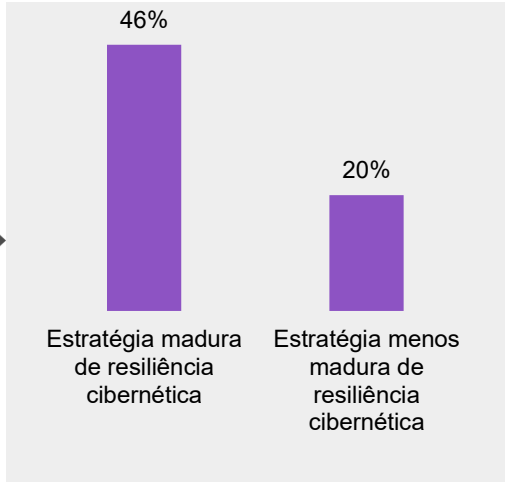
Organizações com uma plataforma robusta para detecção de ameaças nas seguintes áreas



30%

Têm uma plataforma abrangente **em todas as 3 áreas**





Seção 4: Recuperar

Recuperar-se rapidamente e dentro das expectativas do SLA

Estado da recuperação: Muitas organizações alcançam as metas, mas a melhoria contínua é essencial para acompanhar o ambiente de ameaças

40%

contido e recuperado com sucesso e com impacto mínimo

Com **membros do conselho (53%)** mais propensos a afirmar isso do que **gerentes de nível intermediário (30%)**

54%

das organizações alcançaram as **metas de RTO/RPO**

Por posição: Membros do conselho (66%) versus gerência de nível intermediário (45%)

Nº 4

O principal impulsionador do investimento em segurança cibernética é um **incidente cibernético recente ou quase acidente** na organização

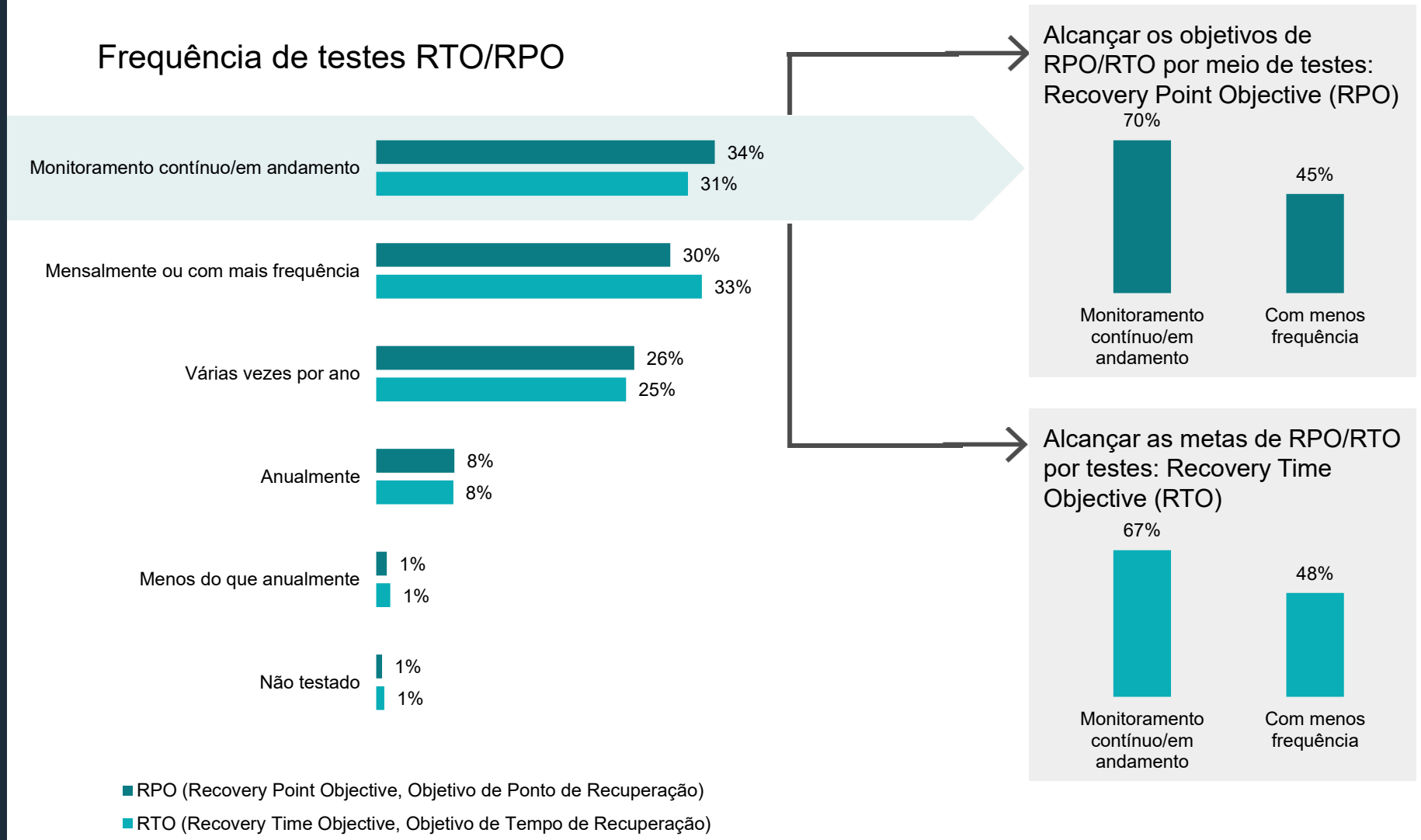
57% estão aprimorando os recursos de resiliência para **atender aos requisitos regulamentares ou de conformidade**

Testes frequentes podem melhorar a recuperação

Enfim, uma cultura de alerta e melhoria constante é o que cria resiliência.

Gerente sênior, Organização de serviços ao consumidor, Brasil

Os testes são essenciais para a resiliência, dando às organizações uma chance melhor de recuperação



Os testes são fundamentais para a resiliência

48%

Afirmaram que os testes de segurança cibernética da organização não simulam de maneira realista as técnicas modernas de ataque

53% de membros do conselho, executivos

versus

48% da gerência de nível intermediário

A prática regular é essencial para impulsionar a recuperação, mas as organizações devem se planejar continuamente para ameaças em evolução

Média de vezes por ano que a organização realiza simulações de ataques cibernéticos

55%

dos que realizaram simulações de ataques cibernéticos **mensalmente ou com mais frequência se recuperaram com sucesso** de um exercício/incidente cibernético

35%

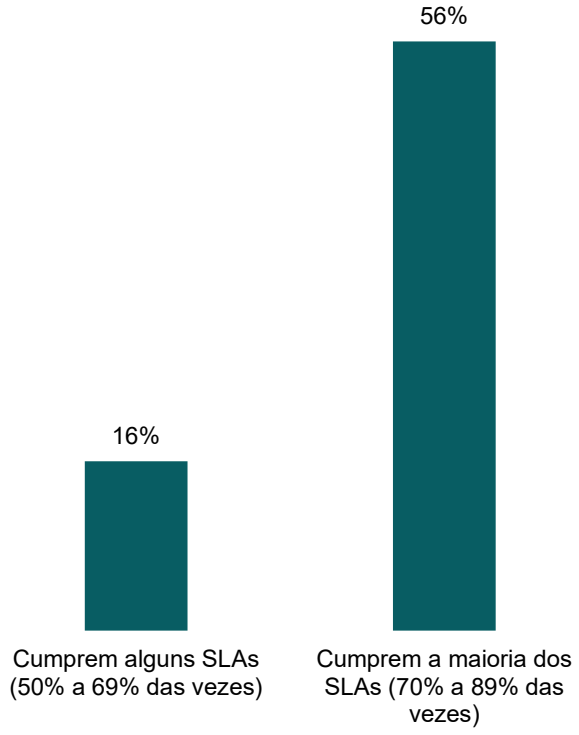
dos que realizaram simulações de ataques cibernéticos **menos do que mensalmente se recuperaram com sucesso** de um exercício/incidente cibernético

> *A necessidade de testar e avaliar de modo abrangente em todas as superfícies de ameaças potenciais, em vez de se concentrar nos testes/ cobertura de pontos.*
>
> Gerente sênior, Tecnologia de TI e telecomunicações, Reino Unido

> *Os ataques cibernéticos nos lembram como é importante realizar exercícios regulares de segurança.*
>
> *O treinamento de conscientização sobre segurança foi fortalecido, permitindo que todos os funcionários identifiquem possíveis ameaças.*
>
> Membro do conselho, Construção e propriedades, Austrália

Os SLAs são a prova disso: Organizações com estratégias maduras cumprem as promessas de recuperação

Frequência de organizações que cumprem os SLAs para recuperação de sistemas essenciais

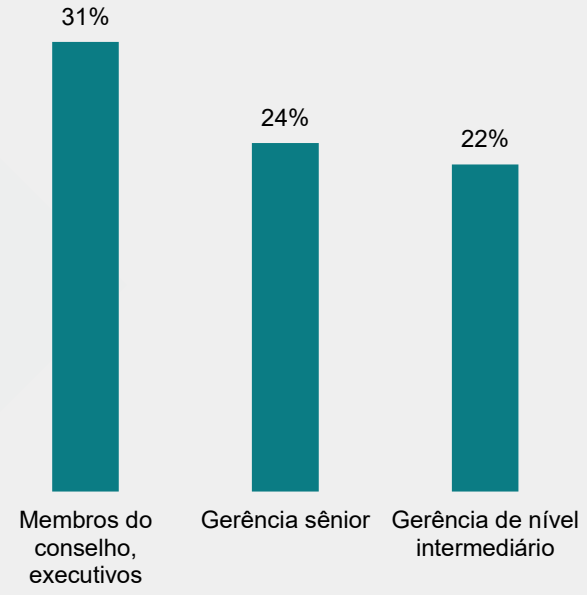


2x

Organizações com estratégias maduras de resiliência cibernética são mais propensas a cumprir consistentemente os SLAs

36% versus **18%**

Por posição:



Seção 5: Complexidade, cultura e o que está por vir

Barreiras organizacionais e planos de investimentos futuros

A complexidade, as lacunas de habilidades e o excesso de confiança ameaçam a resiliência cibernética, mas a IA e o treinamento podem ajudar

Principais desafios:

Ambientes complexos de TI	49%
Limitações de orçamento	42%
Falta de pessoal qualificado	39%
Fragmentação de fornecedores/ ferramentas	38%
Baixa priorização executiva	23%

Organizações maiores têm mais probabilidade de enfrentar isto:

- 50% 5.000 ou mais funcionários
- 50% 3.000 a 4.999 funcionários
- 46% 1.000 a 2.999 funcionários

63%

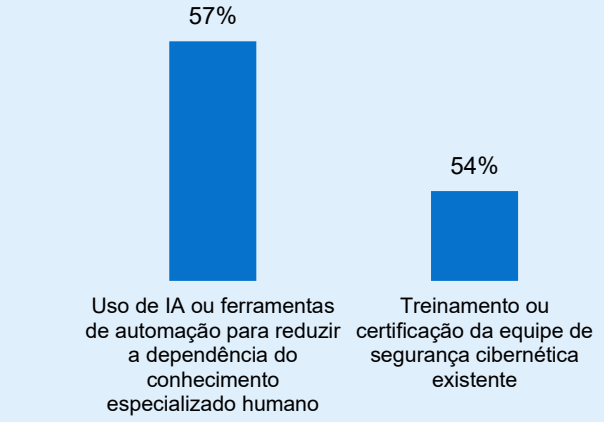
acreditam que a liderança superestima a prontidão da organização para um grande evento cibernético

96%

Reconhecer que existem deficiências em habilidades ou conhecimento especializado em segurança cibernética

MAS...

As organizações estão agindo por meio de:



Pensando em investimentos futuros

Nº 1

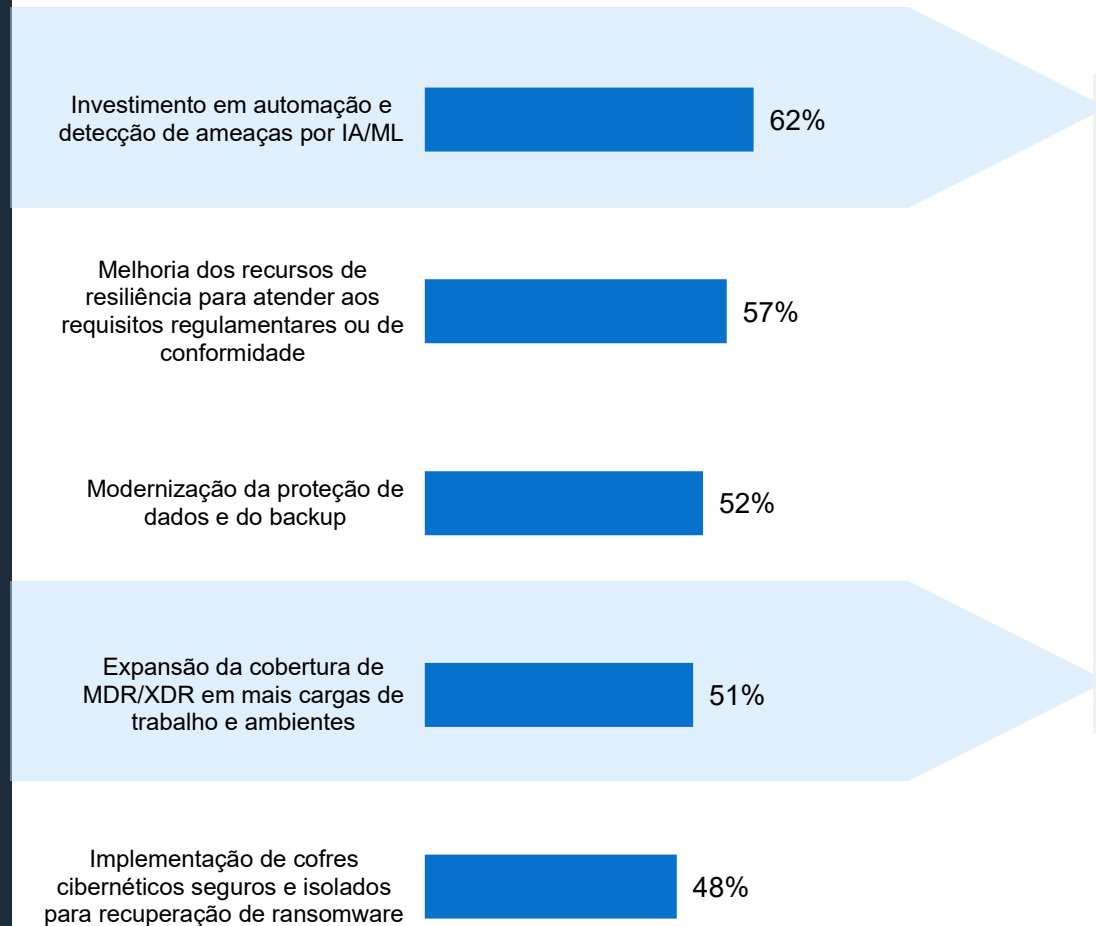
O impulsionador do investimento é o cenário de ameaças em evolução

97%

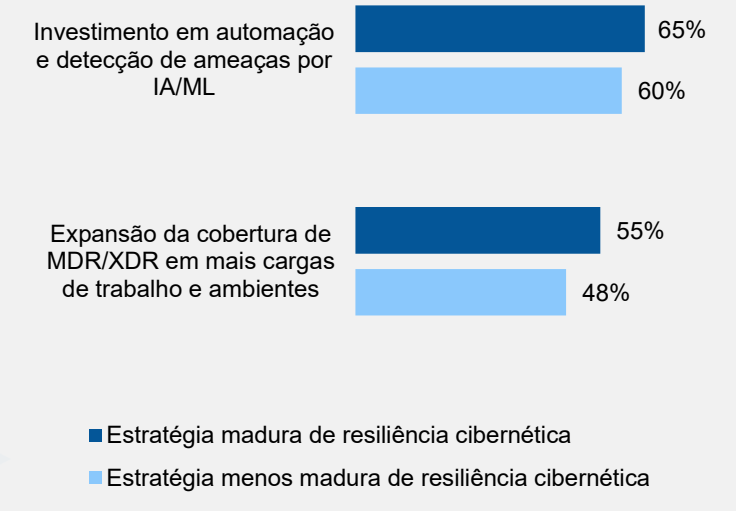
"Minha organização precisa fortalecer continuamente a segurança à medida que as ameaças evoluem"

Para manter uma postura madura, o investimento contínuo e a otimização são o caminho a seguir

Priorização dos investimentos em resiliência cibernética nos próximos 12 meses



Organizações maduras com resiliência cibernética estão investindo continuamente

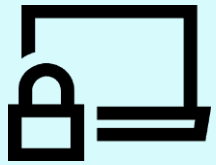


Principais conclusões

Principais constatações

39%

das organizações têm uma estratégia de resiliência cibernética totalmente estabelecida e continuamente otimizada



A otimização contínua é fundamental. Sem ela, as estratégias podem ficar rapidamente desatualizadas contra as ameaças em evolução, deixando as organizações em maior risco

46%

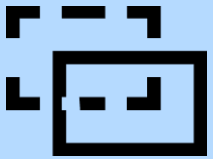
reconhecem que os dados de backup não estão tão protegidos quanto deveriam

Fortalecer a proteção do backup é essencial para garantir que a recuperação continue possível quando os sistemas primários estiverem comprometidos.

Proteger

30%

usam uma plataforma abrangente para detecção de ameaças em rede, backup e armazenamento primário



Sem a detecção unificada, a visibilidade das ameaças e os tempos de resposta podem ser mais lentos, aumentando o risco de violações não detectadas.

Detectar

55%

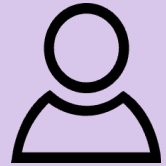
dos que realizaram simulações de ataques cibernéticos mensalmente ou com mais frequência se recuperaram com sucesso de um exercício/incidente cibernético

Os testes frequentes ajudam as equipes a se prepararem para acontecimentos reais. Equipes despreparadas correm o risco de atrasar a resposta e a recuperação nos momentos necessários.

Recuperar

63%

acreditam que a liderança superestima a prontidão da organização para um grande evento cibernético



O excesso de confiança pode atrapalhar os investimentos, atrasar o planejamento de respostas e deixar vulnerabilidades críticas sem tratamento.