

# Insights sobre resiliência cibernética

Explorando lacunas na resiliência cibernética, ameaças em evolução, defesas baseadas em IA e estratégias de recuperação na região Ásia-Pacífico e no Japão

Os desafios da resiliência cibernética estão se intensificando à medida que os ataques cibernéticos e as lacunas na proteção de dados aumentam os riscos de interrupção. Organizações com estratégias maduras de resiliência\* têm quase três vezes mais chances de se recuperar com sucesso. Ao modernizar as estratégias de resiliência, aprimorar os recursos de detecção e priorizar a otimização contínua, os líderes de TI podem minimizar os riscos e fortalecer a confiança em sua capacidade de adaptação às ameaças em constante evolução.

## Excesso de confiança na liderança

**74% dos profissionais de TI acreditam que a sua liderança sobrestima a preparação para eventos cibernéticos.** A autoconfiança excessiva cria pontos cegos perigosos, atrasando investimentos essenciais e expondo vulnerabilidades.



## A lacuna de confiança versus capacidade

**99,3%**

das organizações já implementam estratégias de resiliência cibernética

No entanto, **55%**

não conseguiram se recuperar efetivamente do último teste ou incidente

## Prevenção versus recuperação: uma abordagem desequilibrada

**87%**

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

Mas apenas

**30%**

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

E somente

**41%**

conseguiram conter e se recuperar de ataques ou simulações de incidentes cibernéticos com o mínimo de impacto

Consequentemente, quando as violações ocorrem, muitas organizações não estão preparadas para a fase de recuperação, que é determinante para a sobrevivência dos negócios.

## O caminho a seguir:

Organizações maduras entregam resultados

**Organizações com estratégias maduras de resiliência cibernética têm quase 2,8 vezes mais chances de se recuperar com sucesso**

A maturidade estratégica, baseada em três pilares essenciais, trabalha em conjunto para criar uma resiliência inquebrantável.



**PROTEJA-SE:**

**Construindo sua base de confiança**

As organizações com estratégias maduras de resiliência cibernética têm:

**1,8 vezes** mais chances de proteger dispositivos usando controles de segurança no nível do firmware/BIOS

**Mais propensos** a utilizar criptografia para dados em repouso e em trânsito

**Mais propensos** a utilizar cofres cibernéticos para proteger dados críticos contra ameaças em constante evolução

Mas a segurança é apenas o começo. A verdadeira vantagem está na detecção inteligente, que identifica ameaças antes que elas comprometam seus ativos mais valiosos.



**DETECTE:**

**Inteligência que nunca dorme**

### O desafio de visibilidade:

Apenas 30% das organizações possuem um sistema robusto de detecção de ameaças no armazenamento de backup, no armazenamento de dados primários e na infraestrutura de rede.

### A solução com IA:

**57%** estão priorizando investimentos em detecção de ameaças com IA/ML

**52%** verificam exaustivamente os dados de backup com IA/ML em busca de indicadores de comprometimento

Organizações com estratégias maduras de resiliência têm **2,3 vezes mais chances** de adotar ferramentas de IA/ML com guias estratégicos proativos de mitigação e resposta



**RECUPERE-SE:**

**Onde preparação e desempenho se encontram**

### A vantagem do teste:

**61%** das organizações que simularam ataques cibernéticos uma vez por mês ou mais se recuperaram de incidentes com sucesso

**59%** das organizações que fizeram testes menos de uma vez por mês não se recuperaram de incidentes com sucesso

### O resultado:

As organizações que realizam testes com frequência têm muito mais chances de atingir os objetivos de tempo de recuperação e os objetivos de ponto de recuperação do que aquelas que realizam testes esporadicamente.

## Seu caminho para a excelência em resiliência cibernética

Organizações com estratégias maduras de resiliência cibernética têm 2,3 vezes mais chances de cumprir os SLAs com consistência

### Construindo sua base robusta

Priorize tanto a prevenção quanto a recuperação rápida.

**Proteja:** reduza os riscos com controles de segurança no nível do BIOS, criptografia de dados e cofres cibernéticos para dados críticos.

**Detecte:** use IA/ML em tempo real para detectar e responder a ameaças em todo o ambiente de armazenamento, do primário ao de backup.

**Recupere:** teste a recuperação com frequência — as organizações que fazem isso mensalmente têm muito mais chances de atingir os objetivos de recuperação.

## Tudo pronto para fortalecer sua resiliência cibernética?

Tudo pronto para fortalecer sua resiliência cibernética? Descubra as principais conclusões da [Pesquisa de insights sobre resiliência cibernética de 2026 da Dell](#).

**DELL**Technologies

Fonte: pesquisa sobre resiliência cibernética 2025, da Vanson Bourne e Dell Technologies. Copyright © Dell Inc. or its subsidiaries. Todos os direitos reservados. Dell e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias. Outras marcas comerciais podem pertencer a seus respectivos proprietários.

\*Organizações com estratégias maduras de resiliência cibernética são definidas como aquelas que possuem uma estratégia totalmente estabelecida e continuamente otimizada, utilizando análises preditivas, automação e insights em tempo real (por exemplo, feeds de inteligência de ameaças, ajustes orientados por ML e KPIs que orientam melhorias)