Acronis

Além da cibersegurança: construindo resiliência cibernética para garantir a continuidade dos negócios

Por que os líderes de TI modernos
devem criar um plano para a disrupção,
e não apenas para a prevenção.

Cibersegurança vs. Resiliência Cibernética

A cibersegurança se concentra em impedir ataques. A resiliência cibernética garante que o negócio continue operando durante e após um ataque.

Segurança cibernética
Abordagem baseada em prevenção, defesa de perímetro e na redução de incidentes de segurança

Resiliência cibernética
adaptabilidade, recuperação e continuidadedos negócios.

Impacto da continuidade dos negócios em diferentes indústrias

Por que a resiliência cibernética é importante em indústrias críticas?

O tempo de inatividade e a interrupção cibernética afetam todos os setores — mas as consequências variam de acordo com a indústria.

Cuidados de saúde

60%

Organizações de saúde relatam que incidentes cibernéticos interrompem diretamente o atendimento ao paciente.[1]

Por que isso importa:
O tempo de inatividade pode atrasar o tratamento, desviar pacientes e comprometer a segurança.

Varejo

43%

No último ano, os varejistas sofreram uma grande interrupção causada por incidentes de TI ou cibernéticos.[2]

Por que isso importa:
Mesmo interrupções curtas afetam a receita, a visibilidade do estoque e a experiência do cliente final.

Serviços financeiros

91%

As instituições financeiras sofreram pelo menos um incidente cibernético no último ano.[3]

Por que isso importa:
O tempo de inatividade afeta o processamento de transações, a confiança do cliente final e a conformidade regulatória.

Logística e transporte[4]

94%

Organizações afirmam que as interrupções cibernéticas podem causar falhas em cascata na cadeia de suprimentos.[5]

Por que isso importa:
O tempo de inatividade paralisa o rastreamento de remessas, as operações de armazém e as entregas just-in-time.

Administração pública / governo

60%

As interrupções de rede custam às organizações pelo menos US$ 1 milhão em prejuízos operacionais.[6]

Por que isso importa:
Interrupções afetam os serviços aos cidadãos, a resposta a emergências e a confiança pública.

O tempo de inatividade é uma falha de continuidade dos negócios

O tempo de inatividade afeta a receita, as operações e a reputação — não apenas os sistemas de TI.

96%

das organizações experimentaram pelo menos uma interrupção nos últimos três anos.

80%

dizem que as interrupções estão se tornando mais severas.[7]

Por que a redundância tradicional falha contra ransomware

A redundância protege contra falhas de hardware — mas não contra ataques inteligentes e que se propagam.

A replicação pode espalhar infecções

Ferramentas fragmentadas de DR e backup criam pontos cegos

A proliferação de ferramentas aumenta o tempo de recuperação e gera sobrecarga operacional.

A resiliência moderna requer novas métricas de recuperação

Apenas velocidade não é suficiente — a recuperação deve ser limpa e alinhada aos negócios.

RTO
Tempo máximo para restaurar operações

RPO
Perda máxima de dados aceitável

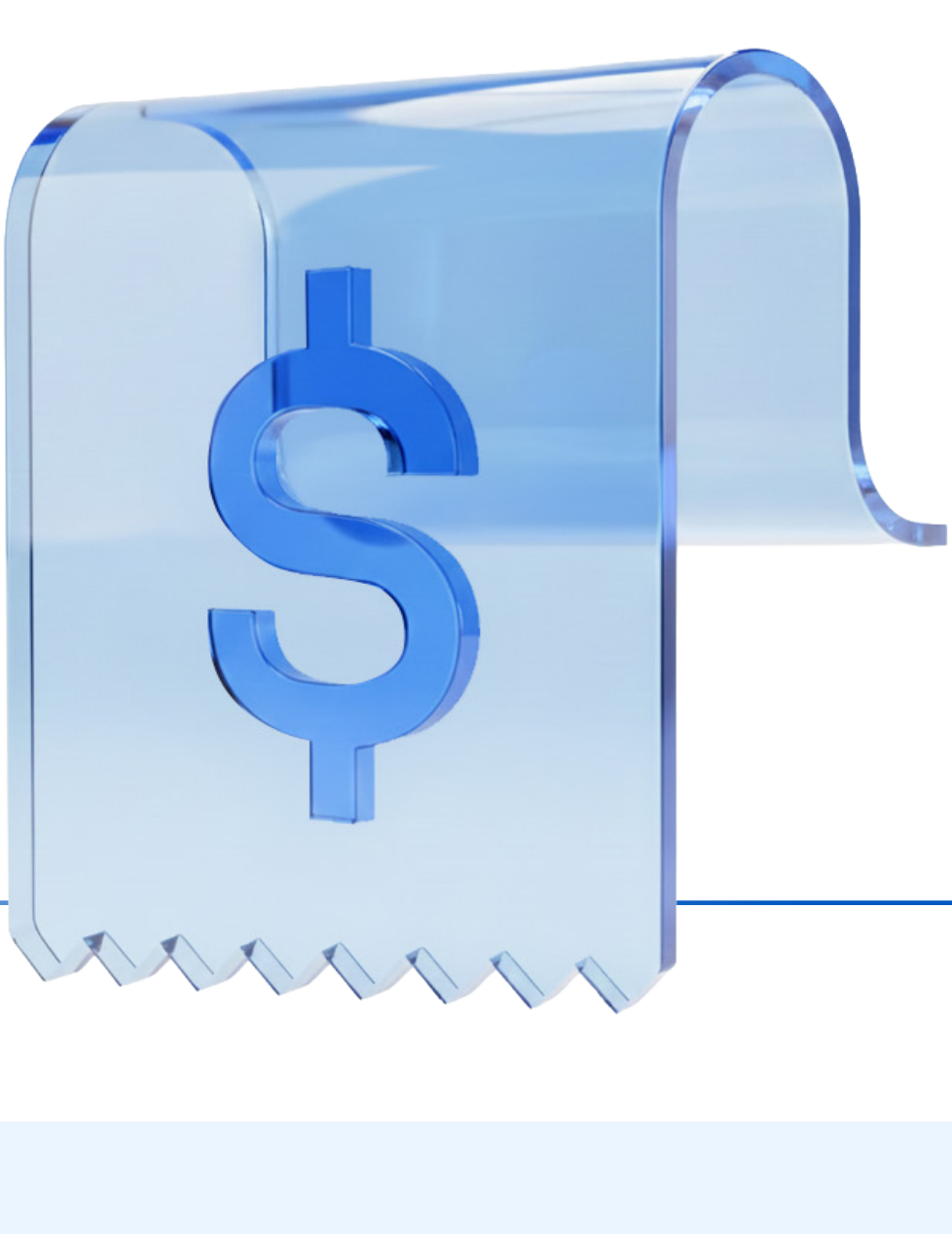
MTD
Tempo máximo tolerável de inatividade antes da falha dos negócios

MTCR
Tempo para restaurar um ambiente verificado e livre de malware

A recuperação limpa é agora um requisito de continuidade

Recuperar rapidamente é insignificante se os sistemas restaurados estiverem comprometidos.

- O custo médio de uma violação de dados é, atualmente, de $4.45 million.
- A interrupção operacional é o maior componente de custo das violações.[8]



O que os líderes de TI das empresas devem priorizar

A resiliência é uma decisão econômica e operacional.

Ações prioritárias (alto nível)

Alinhar a proteção com a criticidade dos ativos.

Testar a recuperação em cenários reais de ciberataques.

Validar backups antes da restauração.

Reduzir a complexidade por meio de plataformas unificadas.

A ciber-resiliência permite continuidade, confiança e controle — mesmo quando os ataques são inevitáveis

Da cibersegurança à ciber-resiliência com Acronis

A cibersegurança depende de mais do que apenas proteção. Isso exige resiliência. Veja como a Acronis pode ajudar você a antecipar ameaças, resistir a ataques, recuperar-se mais rapidamente e adaptar-se para o futuro.

Entre em contato conosco

---

[1] Departamento de Saúde e Serviços Humanos dos EUA (HHS) https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute. "Análise Anual de Interrupções 2023." https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] Fórum Econômico Mundial. "Perspectiva Global de Cibersegurança 2024." https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] Fórum Econômico Mundial – Relatório de Riscos Globais https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid.

[6] Intelligent CIO. "Organizações governamentais dos EUA perdem milhões em uma interrupção ou violação de rede média." https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute. "Análise Anual de Interrupções 2023." https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM. "Relatório de Custo de uma Violação de Dados 2025." https://www.ibm.com/reports/data-breach

Acronis

Copyright © 2003-2026 Acronis International GmbH. Todos os direitos reservados. A Acronis e o logotipo da Acronis são marcas comerciais da Acronis International GmbH nos Estados Unidos e/ou em outros países. Quaisquer outras marcas comerciais ou registradas são propriedade de seus respectivos donos. Pode haver alterações técnicas e diferenças em relação às ilustrações, bem como erros. 2026-01