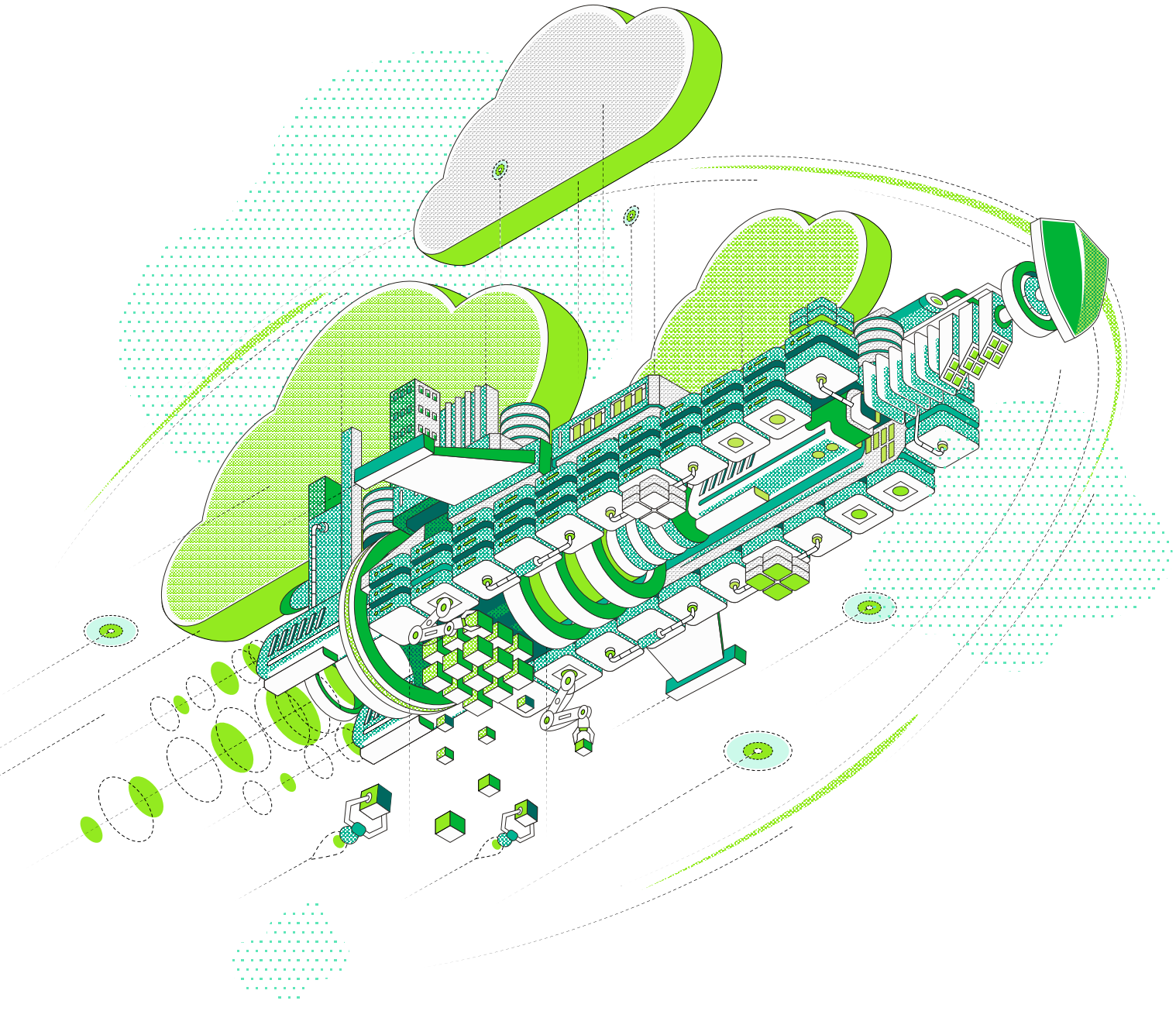
RESUMO EXECUTIVO

2022

Principais tendências da proteção de dados

Edição para a América Latina



O ritmo das mudanças na TI continua aumentando, mas como as empresas estão se adaptando para a proteção de dados moderna? Entre outubro e dezembro de 2021, uma empresa independente de consultoria entrevistou mais de 3.000 tomadores de decisão de TI e profissionais de TI sobre suas estratégias e fatores de proteção de dados para 2022. Quase todos os entrevistados eram de empresas com mais de 1.000 funcionários — de 28 países diferentes, incluindo 334 da América Latina.

Em média, os entrevistados esperam que o orçamento de suas organizações para proteção de dados, incluindo backup e BC/DR, aumente em **5,9%** globalmente em 2022 – **6,5%** na América Latina. Reconhecendo as circunstâncias únicas da estagnação da TI local durante a quarentena da pandemia e dos problemas na cadeia de suprimento resultantes, além da aceleração das iniciativas da nuvem pelos mesmos motivos, é compreensível que 2022 tenha investimentos significativos em proteção de dados para adequação aos ambientes de produção diversos em uso hoje.

Sendo o terceiro estudo anual de tendências em proteção de dados, a pesquisa deste ano foi projetada para quantificar as mudanças nas preocupações/objetivos gerais e estratégias de proteção de dados, além de obter uma compreensão do panorama atual do mercado de proteção de dados, recuperação de desastres, segurança virtual/ransomware e contêineres.

"Híbrida" e "Multi" chegaram para ficar

Com mais de **8.000** pontos de dados globais em três anos consecutivos desta pesquisa, fica claro que o "novo normal" para a TI moderna está dividido de forma equivalente entre servidores locais e servidores hospedados na nuvem. Dentro do data center, existe uma expectativa consistente em relação a plataformas físicas e virtuais. Na nuvem, existe uma combinação saudável do uso de infraestruturas de hiperescala e hospedadas em provedores de serviços gerenciados.

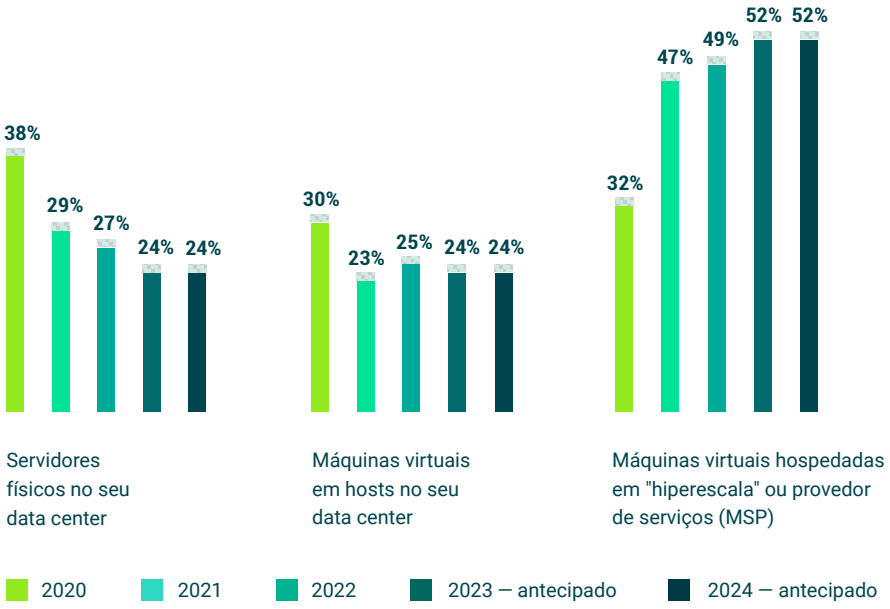


Figura 1.1

Atualmente, qual é a porcentagem de servidores da sua organização em cada formato? E qual é a porcentagem prevista para daqui a dois anos?

20%

das empresas apontaram uma economia melhor como motivo principal para a troca de soluções de backup, enquanto 22% buscam mais confiabilidade e a redução de RPO/RTO

68%

das empresas usam serviços de nuvemcomo parte de sua estratégia de PD

76%

das empresas tiveram pelo menos um ataque de ransomware no último ano

Em 2022, na América Latina, 26% são servidores físicos, 24% são virtuais e 50% são hospedados na nuvem. Essas tendências apresentam dois pontos principais:

- O data center não está morto, nem morrendo. Existem tantos bons motivos para executar uma carga de trabalho no local quanto na nuvem, mesmo para empresas com uma estratégia com prioridade para a nuvem
- Sua estratégia de proteção de dados precisa incluir cargas de trabalho físicas, virtuais e hospedadas na nuvem

A "lacuna" entre as expectativas de negócio e as entregas da TI nunca foi tão grande

A lacuna entre o que as unidades de negócios esperam e o que a TI pode entregar continua a aumentar, conforme registrado nos últimos cinco anos desse projeto. Em 2022, na América Latina:

- **95%** dos líderes de TI acreditam que suas organizações têm uma **"lacuna de disponibilidade"** entre os SLAs esperados e a velocidade com que a TI pode retornar à produtividade.
- **94%** dos líderes de TI acreditam que suas empresas têm uma **"lacuna de proteção"** entre quantos dados podem perder e a frequência com que os dados são protegidos.

A explicação mais provável para essas lacunas é a importância crescente de mais cargas de trabalho. Mas existe uma relação óbvia entre os principais motivadores de mudança — a melhoria do RTO (disponibilidade), RPO (proteção) e confiabilidade (Figura 1.3 no relatório) — versus essas "lacunas" percebidas. As lacunas de percepção dos líderes de TI e os motivadores de mudanças para os implementadores de TI — em relação à redução de perda de dados e tempo de inatividade — é ainda mais justificada ao se considerar que **40%** dos servidores (globalmente) sofrem pelo menos uma paralisação por ano.

40%

dos servidores terão pelo menos uma paralisação não planejada

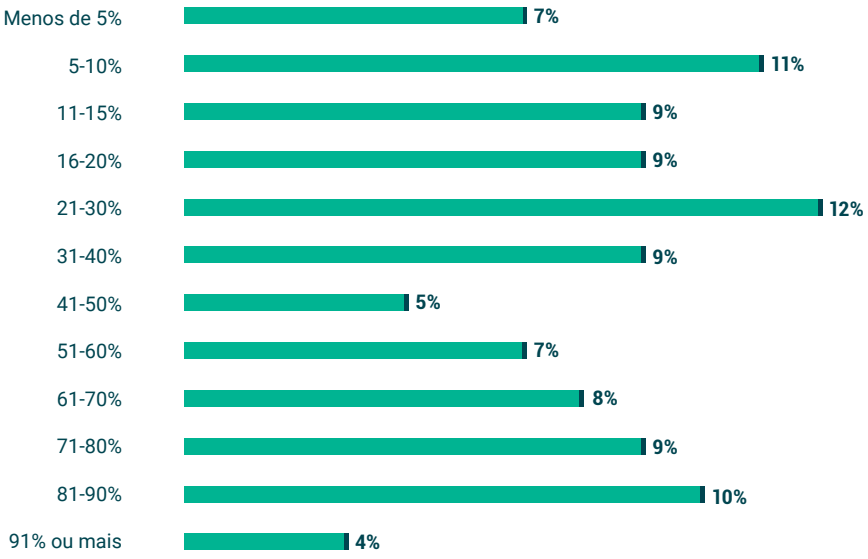


Figura 1.2

Qual porcentagem dos seus servidores teve pelo menos uma paralisação inesperada (ou mesmo uma reinicialização não programada) nos últimos 12 meses?

Não existe muita diferença entre dados de "alta prioridade" e dados "normais"

Embora sempre existam certas cargas de trabalho ou dados com uma importância maior, as expectativas entre essas cargas de trabalho importantes e o resto da TI não são muito diferentes.

Perda de dados — Globalmente, 56% dos dados de "alta prioridade" e 49% dos dados "normais" têm uma tolerância de perda de dados de não mais que uma hora. Organizações na América Latina citam 64% de dados de "alta prioridade" e 61% de dados "normais" tendo uma tolerância de "uma hora ou menos". Isso significa:

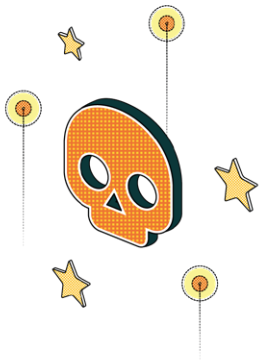
- Não há muita diferença entre dados de "alta prioridade" e o resto, todos os dados são importantes;
- O backup apenas não é suficiente, pois não é executado de hora em hora. Em vez disso, os backups precisam ser combinados com snapshots e/ou replicação.

Essas estatísticas ficam mais interessantes ao considerar-se a tendência de três anos dosrespectivos relatórios de pesquisa global de tendências em proteção de dados. Aqui está um resumo da frequência média de proteção de dados (em minutos) para minimizar a perda de dados de "alta prioridade" e "normais":

	2019	2020	2021
Frequência de proteção de "alta prioridade"	205 minutos	198 minutos	121 minutos
Frequência de proteção "normal"	663 minutos	423 minutos	171 minutos

É razoável as empresas continuem aprimorando sua proteção de dados de "alta prioridade" de forma incremental ao longo do tempo; de cada **205** minutos em 2019 para **121** minutos em 2021. É bastante revelador que, ao longo dos mesmos dois anos, as organizações tenham aprimorado radicalmente a frequência de proteção do resto dos dados, de cada **663** minutos (mais ou menos 8 horas, ou "a cada noite") para **171** minutos (a cada 3 horas, o que significa várias vezes durante o dia). Isso está muito próximo da proteção de "alta prioridade", apoiando a hipótese de que "todos os dados importam" e o apelo universal de combinar (normalmente todas as noites) backups com snapshots, replicação ou ambos.

Tempo de inatividade — Similar à tendência de perda de dados, existe uma variação de apenas **6%** entre o tempo de inatividade tolerável para aplicações de "alta prioridade" e "normais" de até uma hora — revelando as mesmas realidades de que todos os dados importam e da necessidade de backups melhores do que os tradicionais diários.



47%

das organizações tiveram paralisações por causa do ransomware. E pelo segundo ano consecutivo, os ataques virtuais causaram a maioria das paralisações

36%

dos dados em média não foram recuperados após um ataque de ransomware

O que isso significa para 2022?

Nos dois últimos anos, houve uma modernização significativa da TI, especialmente nas áreas em que serviços hospedados na nuvem puderam ser utilizados. Isso é devido a iniciativas contínuas de transformação digital, além da adoção acelerada da nuvem durante a pandemia global. **A rápida modernização da produção forçou muitas organizações a reconhecer que sua proteção não foi modernizada no mesmo ritmo, apesar de sua dependência dos dados e de sua insatisfação com o status quo estarem mais altas do que nunca, revelando três tendências principais para 2022:**

- A proteção de dados será uma área de investimentos crescentes para proteger as cargas de trabalho modernas, muitas vezes hospedadas na nuvem, que já estão em produção;
- Os motivadores de mudanças serão baseados predominantemente na melhoria qualitativa da confiabilidade, frequência de proteção e recuperações ágeis, a fim de melhorar RPOs e RTOs. Além disso, a melhoria do valor econômico e do consumo, junto com a proteção para IaaS/SaaS/contêineres e o uso da nuvem para backups operacionais e recuperação de desastres, serão iniciativas essenciais.
- A melhoria da proteção de dados está sendo impulsionada em grande parte pelo reconhecimento de que os ataques virtuais, especialmente o ransomware, não são uma questão de "se", mas de "quando" para a maioria das empresas, com uma recuperação confiável sendo a parte de correção na estratégia de preparação virtual das organizações. Dessa forma, é universalmente compreendido que “o ransomware é um desastre” e que a recuperação orquestrada a partir dos backups é um componente essencial de qualquer plano de segurança virtual e BC/DR.

42%

dos líderes de TI consideram que o aspecto mais importante de qualquer solução de backup corporativo é a amplitude das cargas de trabalho que ele protege

A perspectiva da Veeam

A plataforma de backup e gerenciamento de dados da Veeam

Agora mais do que nunca, é essencial que as empresas continuem confiantes de que seus dados estejam protegidos e sempre disponíveis, seja no local, na borda ou na nuvem. A Veeam fornece uma única plataforma para ambientes na nuvem, virtuais, físicos, SaaS e Kubernetes. Nossos clientes têm a confiança de que suas aplicações e dados estão protegidos contra ransomware, desastres e agentes maliciosos, e sempre disponíveis com a plataforma mais simples, flexível e avançada do setor.

A Veeam dá aos clientes a confiança para acelerar a transformação digital, proteger contra o crime virtual e impulsionar a resiliência dos negócios, garantindo que seus dados estejam sempre protegidos e disponíveis. Reduza o custo e a complexidade e alcance seus objetivos de negócio com a Veeam: o melhor backup e recuperação.

Para saber mais, acesse **https://www.veeam.com/br**.

Clique aqui para ver o relatório completo da pesquisa global

Perguntas relacionadas aos dados e insights dessa pesquisa podem ser direcionadas para StrategicResearch@veeam.com