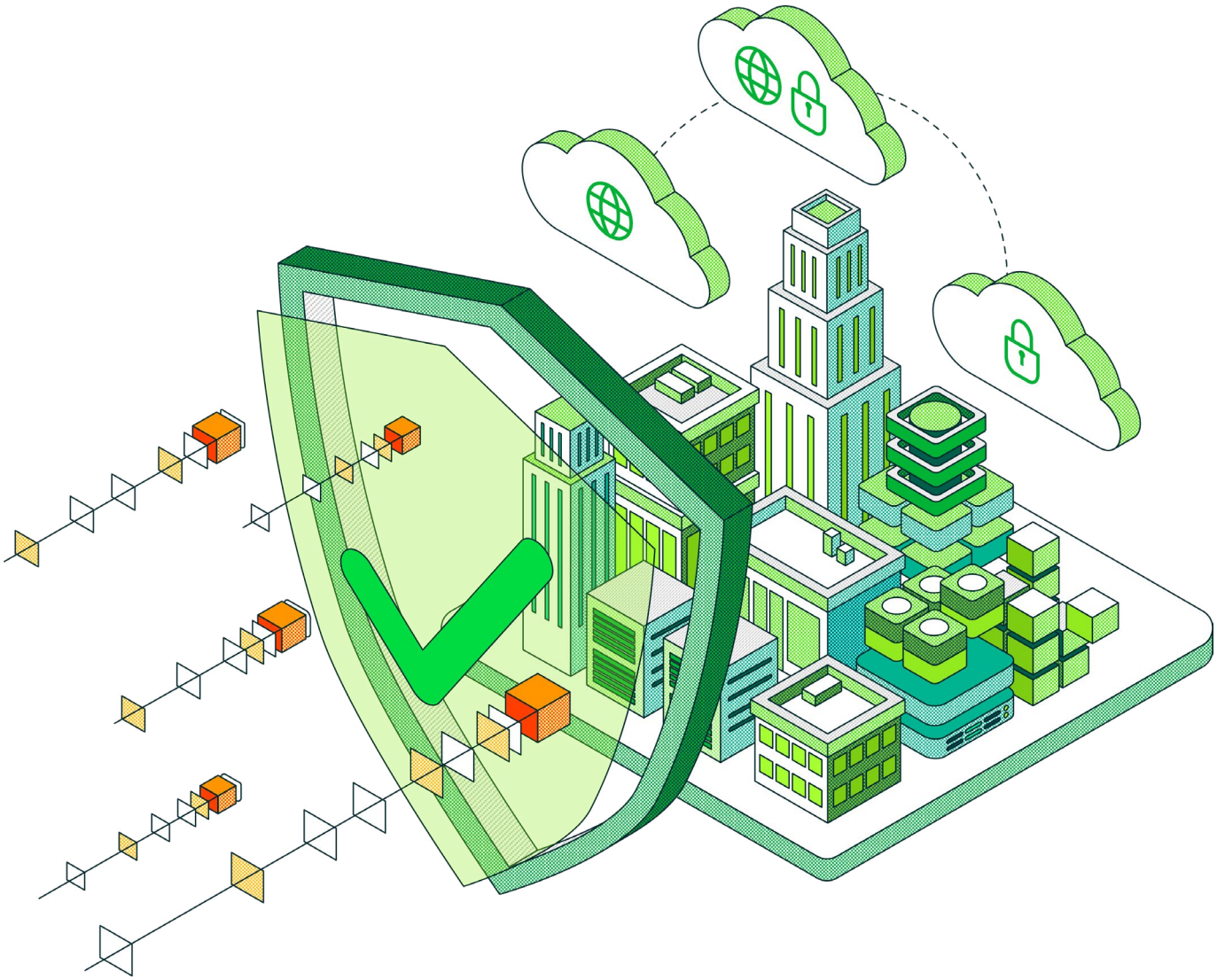
RESUMO EXECUTIVO

2023

Tendências em Proteção de Dados

Edição para a América Latina



No final de 2022, uma empresa de pesquisa independente concluiu um questionário com **4.200** líderes de TI imparciais e implementadores sobre uma variedade de fatores, desafios e estratégias de proteção de dados, incluindo **645** na América Latina. Esse estudo amplo de mercado sobre organizações imparciais é realizado anualmente em nome da Veeam para compreender como o mercado de proteção de dados continua evoluindo, a fim de que a Veeam possa garantir estratégias de produto e iniciativas de marketing alinhadas com a direção do mercado.

Enquanto a Gartner prevê um aumento de **5,1%** nos orçamentos gerais de TI e o IDC preveja um aumento de **5,2%** no gasto geral com TI, essa pesquisa revelou que os orçamentos de proteção de dados devem aumentar em **6,5%** globalmente em 2023. Você pode encontrar a versão completa do Relatório de Tendências em Proteção de Dados - 2023 em https://vee.am/DPR23.

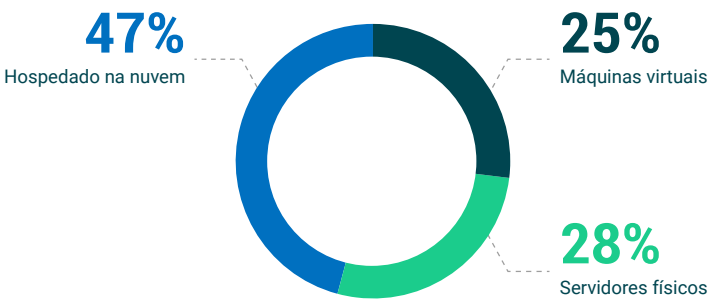
As empresas na América Latina esperam aumentar seus orçamentos de proteção de dados para 2023 em

7,3%

Infraestrutura híbrida de 2020 a 2025

A cada ano, a pesquisa pede às empresas que estimem os servidores locais (físicos e virtuais) e também aqueles hospedados na nuvem, tanto no ano atual, como a expectativa para dois anos no futuro. **Confira nosso relatório completo** para ver um resumo das **12.000** respostas em quatro pesquisas anuais cobrindo de 2020 a 2025, mas em 2023, a distribuição real de instâncias de servidores na TI híbrida de **4.200** empresas, conforme segue:

Panorama real da TI híbrida em 2023 (global)



Em geral, os servidores **físicos** e máquinas **virtuais** machines se estabilizaram em cerca de **50%** do plano geral de TI das empresas, enquanto o resto é **hospedado na nuvem** — com uma mudança contínua, mas gradual, para a hospedagem na nuvem, predominantemente devido à estratégia com prioridade para a nuvem das empresas, que colocam novas cargas de trabalho na nuvem mais rápido do que as cargas de trabalho legadas são descontinuadas no data center, diluindo o data center dentro de uma estratégia geral de TI híbrida.

	GLOBAL	América do Norte	**América Latina**	Europa	MEA	APJ
Servidores físicos	28%	27%	**26%**	28%	29%	29%
Máquinas virtuais	25%	25%	**26%**	26%	25%	25%
Hospedado na nuvem	47%	48%	**49%**	46%	46%	46%

O ponto principal é que as soluções de proteção de dados moderna devem fornecer recursos equivalentes nas três arquiteturas (física, virtual e na nuvem). Além disso, é necessário planejar a mudança de cargas de trabalho entre nuvens e até de volta ao ambiente local, e novamente, a estratégia de proteção de dados deve acomodar essa fluidez.

O que 'backup corporativo' significa?

Pelo segundo ano seguido, o atributo mais importante de uma solução de "backup corporativo" é a **proteção de IaaS e SaaS.** Isso não deve ser uma surpresa ao considerar como as infraestruturas estão mudando para a nuvem.

O que pode surpreender alguns é que garantir a **confiabilidade** é o segundo critério mais importante. Mas ao considerar que muitas empresas podem estar usando soluções de backup legadas que foram projetadas para a era do data center físico, essas soluções provavelmente utilizam abordagens baseadas em agentes para proteger cargas de trabalho da nuvem. Mecanismos de backup legados raramente geram bons resultados ao proteger cargas de trabalho modernas.

Assim sendo, faz sentido que a proteção e a confiabilidade da hospedagem na nuvem estejam juntas e no topo da lista.

15%

das empresas na América Latina em busca de uma solução de backup corporativo consideram **"Proteger cargas de trabalho IaaS e SaaS, assim como o data center"**, como o recurso mais importante

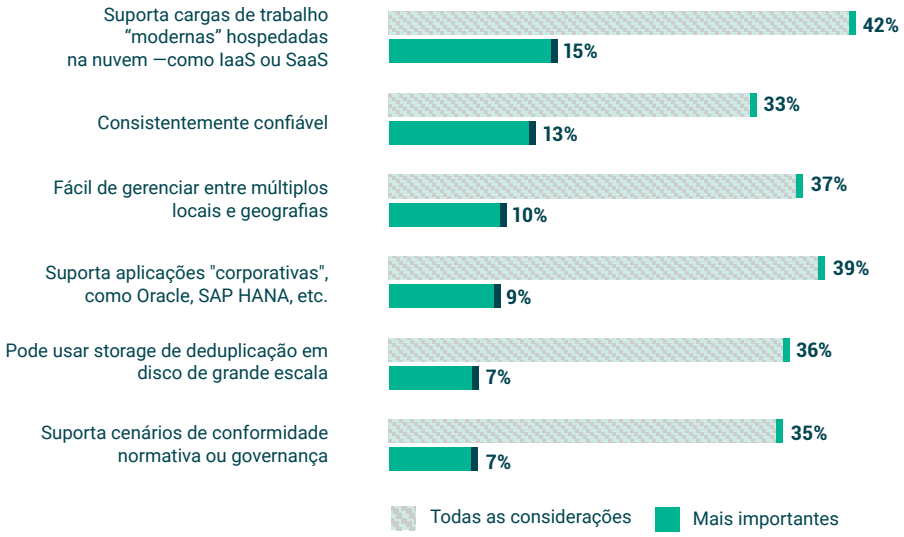


Figura 1.2

O que "backup corporativo" significa para você?

Se a sua empresa estivesse considerando uma nova solução de "backup corporativo" hoje, qual atributo seria o mais importante?

De fato, quando as empresas foram perguntadas o que as levaria a mudar sua solução de backup primária, o motivo mais comum, além de mais importante, foi a **melhoria da confiabilidade,** o que é consistente com o que as empresas procuram em uma soluções de backup corporativo.

39%

das empresas na América Latina declaram que **"melhorar a confiabilidade/ sucesso dos backups"** é a motivação para mudar de solução de backup

Para 2023, a proteção de dados 'moderna' significa 'com resiliência virtual'

Ao considerar o que a proteção de dados moderna deve tratar, vale a pena observar que o relatório completo da pesquisa revela que, pelo terceiro ano seguido, os ataques virtuais continuam sendo a principal causa das paralisações mais impactantes – enquanto a frequência dos ataques de ransomware continua aumentando:

- Em 2021, **76%** das empresas foram atacadas com sucesso por ransomware pelo menos uma vez.
- Em 2022, **85%** das empresas fizeram essa mesma declaração.

	GLOBAL	América do Norte	**América Latina**	Europa	MEA	APJ
Sem ataques em 2022	15%	11%	**11%**	16%	14%	18%
Apenas 1 ataque	18%	16%	**15%**	19%	18%	18%
2 ou 3 ataques	48%	53%	**52%**	46%	48%	45%
4 ou mais ataques	18%	19%	**18%**	17%	21%	19%

Embora essas estatísticas sejam preocupantes, os resultados desses ataques são ainda piores. Quando as empresas foram perguntadas sobre os ataques mais significativos sofridos em 2022:

- **39%** de todo o seu conjunto de dados de produção foi criptografado ou destruído
- Apenas **55%** dos dados criptografados/destruídos puderam ser recuperados

Portanto, não é surpresa que o aspecto mais comum e importante de uma "solução de proteção de dados moderna" seja a integração da proteção de dados com uma estratégia de preparação virtual.

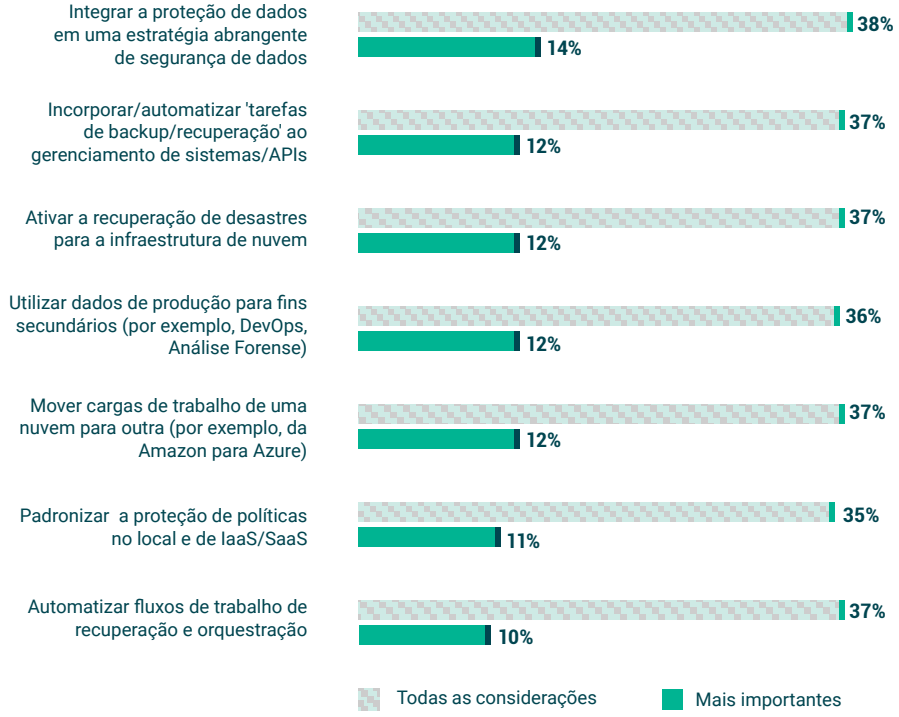


Figura 1.5

O que você consideraria como os aspectos que definem uma solução "moderna" ou "inovadora" de proteção de dados para a sua organização? Mais importantes?

Mas embora a resiliência virtual continue sendo uma preocupação principal para muitos líderes de TI, seria um grande erro estratégico focar todo o seu planejamento de proteção de dados nos ataques. Paralisações de sistemas causadas por falhas na rede, na aplicação ou no hardware, além de problemas com o SO, ainda ocorrem com frequência mesmo nos data centers modernos. As empresas devem estar preparadas para as interrupções que continuam ocorrendo e também para eventos causados por humanos, como erros de usuários e ataques de criminosos virtuais.

Métodos e mecanismos de BC/DR

Conforme os serviços de nuvem se tornam cada vez mais comuns nas estratégias de proteção de dados, muitos se perguntam se devem recuperar os dados de volta para servidores locais ou para infraestruturas hospedadas na nuvem. Embora o resultado da pesquisa mostre um interesse relativamente equilibrado entre recuperações no local e hospedadas na nuvem para 2023, a maioria dos dados de recuperação virá de backups hospedados na nuvem. Isso segue a prática de ter menos pontos de recuperação no local e enviar dados para um storage baseado na nuvem para fins de retenção de dados ou preparação para ransomware ou BC/DR.

Ao considerar a prática recomendada de supor que os especialistas principais não estejam mais disponíveis durante uma crise, uma recomendação importante da maioria dos planejadores de BC/DR é usar fluxos de trabalho orquestrados, de modo que o conhecimento possa ser encapsulado nos processos. Também é recomendado testar os fluxos de trabalho da mesma forma que eles seriam executados durante uma crise real. Infelizmente, os resultados da pesquisa deste ano revelaram que apenas **18%** possuem uma capacidade de fluxo de trabalho orquestrado em sua estratégia atual de proteção de dados ou failover.

53%

das empresas na América Latina esperam usar servidores no local para BC/DR, enquanto **47%** utilizarão uma infraestrutura hospedada na nuvem para BC/DR

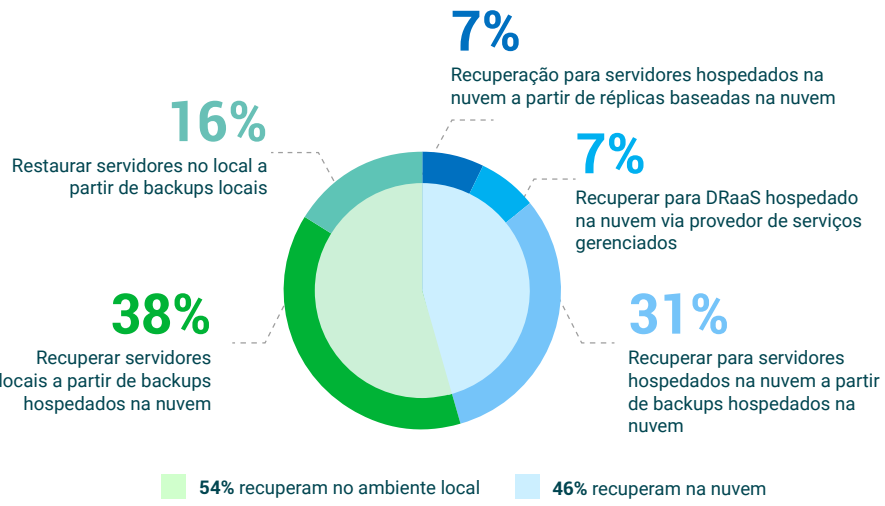


Figura 2.3

Como as operações são retomadas para a função de DR da sua empresa?

A proteção de dados com a tecnologia da nuvem continua ganhando popularidade

O storage baseado na nuvem é o "fim da fita"? De acordo com os resultados da pesquisa, **50%** dos dados ainda são gravados em fita em algum ponto do seu ciclo de vida, enquanto **63%** dos dados agora são armazenados na nuvem em algum momento, embora isso varie conforme o país ou região.

	GLOBAL	América do Norte	**América Latina**	Europa	MEA	APJ
% de dados em fita	50%	50%	**48%**	53%	52%	45%
% de dados em nuvens	63%	63%	**60%**	63%	64%	63%

Muitas empresas têm um modelo operacional de três camadas para retenção de dados, incluindo:

- Disco no local para 90-120 dias
- Cópias na nuvem, incluindo cópias atuais e versões anteriores de dois até cinco anos
- Fita para a minoria dos dados que têm regulamentação para armazenamento por 10 anos ou mais

Como interpretação alternativa à "% de dados usando a nuvem", vale a pena considerar a "% de empresas usando backups na nuvem", com **67%** dos entrevistados globais usando serviços de nuvem como parte de sua estratégia de proteção de dados hoje, com previsão de **74%** até 2025.

Uma das sinergias mais poderosas entre os serviços de nuvem e a proteção de dados é o advento da recuperação de desastres com a tecnologia da nuvem, em que as infraestruturas de nuvem são usadas em vez de, ou em complemento a, um segundo data center. Em 2020, **53%** das empresas tinham recursos de BC/DR, com **71%** sendo capazes de realizar BC/DR em 2023. Mais importante é o reconhecimento de que, embora cerca de **30%** das empresas continuem utilizando múltiplos data centers para sua BC/DR, a porcentagem de empresas usando serviços de nuvem (IaaS/DR ou DRaaS) para BC/DR mais do que dobrou desde 2020 **(23%)** a 2023 **(47%)**, com a previsão de que **55%** usarão DR com tecnologia da nuvem até 2025.

	GLOBAL	América do Norte	**América Latina**	Europa	MEA	APJ
% das empresas usando infraestrutura hospedada na nuvem para BC/DR	47%	50%	**41%**	43%	41%	54%
% das empresas com múltiplos data centers para BC/DR	24%	22%	**27%**	24%	25%	23%

75%

das empresas na América Latina esperam usar serviços de nuvem como parte de sua solução de proteção de dados até 2025

2023 será um ano de 'mudança'?

Diante dos temores sobre ransomware, a pressão de garantir os serviços de TI e os desafios de proteger cargas de trabalho modernas de IaaS e SaaS, pode-se presumir que as empresas provavelmente mudarão suas soluções de backup para se adaptar a essas condições em mudança. E você teria razão! Ignorando os **35%** de respostas quase neutras:

- Apenas **8%** das empresas não devem mudar sua solução de backup primária em 2023
- Enquanto isso, **57%** dos entrevistados expressaram que provavelmente ou certamente mudarão suas soluções de backup

57%

das empresas na América Latina esperam trocar suas soluções de backup em 2023

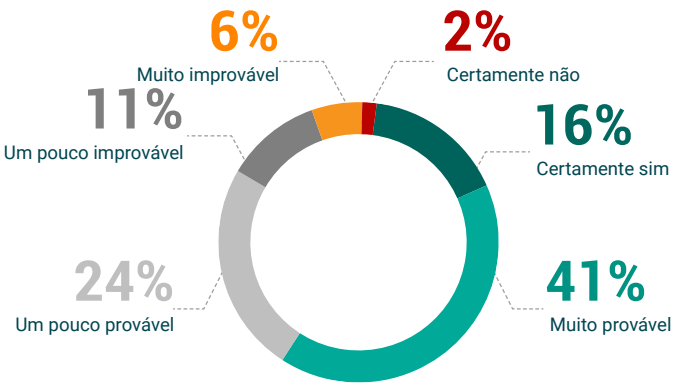


Figura 3.6

Qual é a probabilidade da sua organização mudar as soluções/serviços primários de backup nos próximos doze meses?

A perspectiva da Veeam

A Plataforma de datos Veeam

Conforme as empresas continuam a transformar sua infraestrutura, garantindo o suporte para aspectos da nuvem como o backup, a utilização e a mobilidade, existe a necessidade de uma solução que torne a complexidade compreensível. A Veeam® Data Platform oferece:

- Controle de custos de storage com uma arquitetura de camadas de storage inteligentes
- Backup e restauração nativos e desenvolvidos especificamente para Kubernetes, recuperação de desastres e mobilidade para aplicações em contêineres
- Amplo suporte de cargas de trabalho entre serviços de IaaS/PaaS/SaaS
- Monitoramento e gerenciamento centralizados, combinados com uma cobertura de API abrangente

Os usuários atuais ou novos da Veeam devem conferir o Veeam Backup *for AWS, Azure, Google Cloud, Microsoft 365, Salesforce* e Kasten for Kubernetes para ver os recursos líderes do setor, criados para as necessidades únicas da nuvem híbrida.

Para os usuários da Veeam que estão em busca de "como um serviço," ou de suprir uma lacuna de recursos, a Veeam tem parcerias com uma rede extensiva de provedores de BaaS e DRaaS, e especialistas em serviços profissionais, para garantir que os usuários maximizem seus investimentos na Veeam e na nuvem.

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**