



DOCUMENTO RESEARCH INSIGHTS DO ESG

# Por que a proteção de dados é importante para os atuais ambientes com várias nuvens

Um estudo de pesquisa que explora a função dos recursos otimizados de proteção de dados no sucesso da nuvem híbrida

Por Christophe Bertrand, analista sênior

Maio de 2020

---

## Conteúdo

As tendências, a evolução e a proliferação de nuvens produzem um ambiente dinâmico para a proteção de dados.....	3
Proteção de dados como um fator essencial para o sucesso da nuvem híbrida .....	6
Benefícios da proteção otimizada de dados para ambientes com várias nuvens .....	6
A grande verdade.....	9
Como a Dell Technologies pode ajudar.....	10
Apêndice – Metodologia da pesquisa e dados demográficos dos entrevistados .....	11

## As tendências, a evolução e a proliferação de nuvens produzem um ambiente dinâmico para a proteção de dados

Atualmente, a nuvem está crescendo em adoção e popularidade em muitas organizações, reformulando a infraestrutura tradicional. A pesquisa do ESG identificou que 76% das organizações dão à nuvem pública uma consideração igual ou maior à que dão à infraestrutura local para novos aplicativos, o que é um voto significativo de confiança. De fato, espera-se que 38% dos dados das organizações residam na nuvem nos próximos 24 meses e que o número de nuvens públicas em uso aumente.

Os usuários dos provedores de serviços em nuvem (CSPs) não colocam todos os seus ovos na mesma cesta: 82% utilizam vários CSPs de infraestrutura no momento e espera-se que 86% façam o mesmo daqui a três anos. Especificamente, espera-se que a proporção que usa mais de três CSPs dobre (31% em comparação com 15%) no mesmo período. Nesse cenário, não é de surpreender que 73% das organizações relatem que o uso da infraestrutura na nuvem pública (ou em várias nuvens públicas) além da infraestrutura local agregou complexidade às operações de TI. O uso de várias nuvens está acontecendo e torna a vida mais complexa!

Isso significa que muitos processos relacionados a dados, como backup e recuperação, precisam se adaptar a esse híbrido em evolução (no qual algumas cargas de trabalho residem no local e, outras, na infraestrutura em nuvem pública) e ao mundo com várias nuvens (no qual as cargas de trabalho são hospedadas em várias nuvens públicas). A proteção de dados "segue" as cargas de trabalho, um relacionamento corroborado pela pesquisa do ESG: as organizações com mais de 500 VMs hospedadas na nuvem em seu ambiente são mais propensas que as organizações com 500 ou menos a utilizar a recuperação de desastres como serviço (DRaaS, 80% em comparação com 57%) e as metas de backup na nuvem (82% em comparação com 69%).<sup>1</sup> Em outras palavras, à medida que o uso de IaaS aumenta, o mesmo acontece com a propensão de uma organização a usar diferentes soluções de proteção.

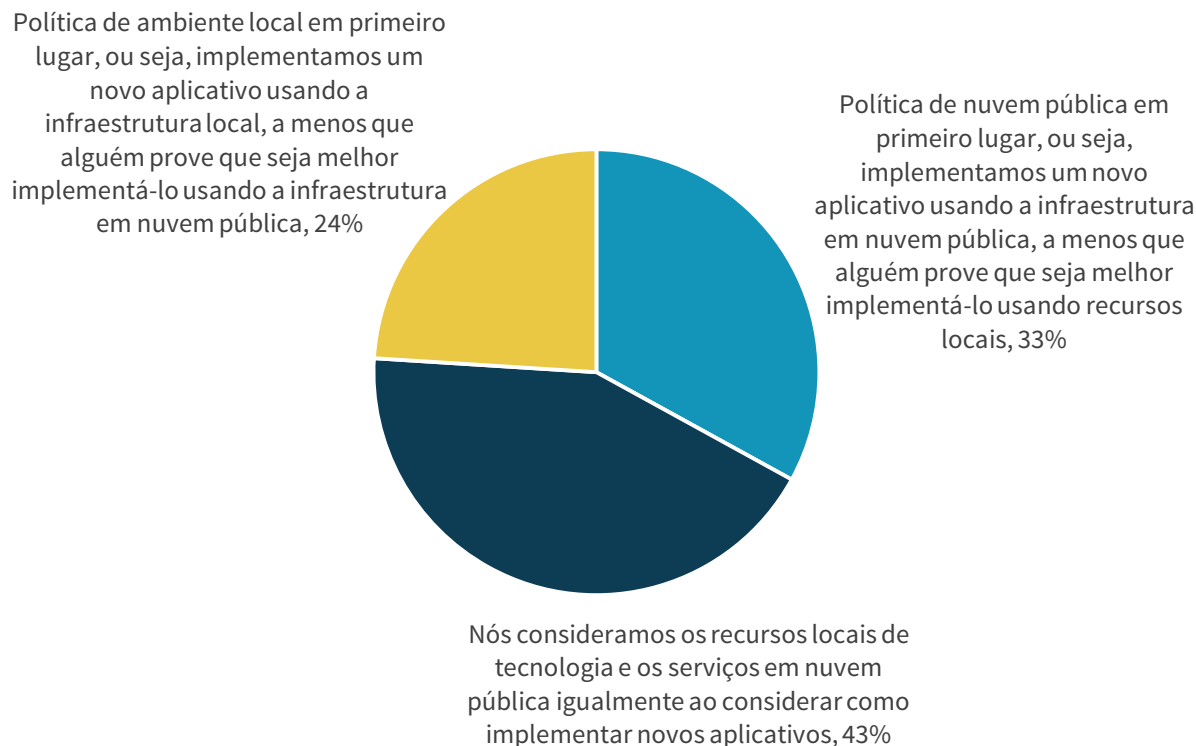
A outra consideração importante é manter objetivos de tempo e ponto de recuperação (RTOs e RPOs) coerentes no que se tornou uma infraestrutura bastante distribuída, com diferentes extensões de controle, segurança e gerenciamento. As implementações de proteção de dados devem unificar os níveis de serviço em ambientes locais e em nuvem. Portanto, há uma oportunidade de evoluir os projetos atuais de arquitetura de proteção de dados para adotar tecnologias que possam lidar com seus ambientes empresariais e em nuvem de forma consistente.

---

<sup>1</sup>Fonte: resultados da pesquisa principal do ESG, [Data Protection Cloud Strategies](#), junho de 2019

**Figura 1. Na nuvem ou no local primeiro?**

**Qual das opções abaixo descreve melhor a abordagem que sua organização adota quando se trata de novas implementações de aplicativos? (Porcentagem de respondentes, N = 1.257)**



Fonte: Enterprise Strategy Group

Muitas decisões sobre soluções de proteção de dados se baseiam no local onde as cargas de trabalho residem e os usuários finais favorecem a flexibilidade da alocação de cargas de trabalho: 83% das organizações consideram a flexibilidade da alocação de cargas de trabalho (ou a capacidade de executar cargas de trabalho na nuvem que quiserem, dentro ou fora do local) com uma das cinco maiores prioridades entre todas as iniciativas tecnológicas. Isso significa que os mecanismos de proteção de dados precisarão demonstrar o mesmo nível de flexibilidade para cumprir os requisitos de backup e recuperação e os níveis de serviço.

Embora haja entusiasmo por ambientes com várias nuvens, os entrevistados **geralmente atribuem a vantagem de funcionalidade aos ambientes locais**. Isso é particularmente válido em relação aos recursos de segurança e capacidade de gerenciamento. Uma das provas disso é que 77% das organizações entrevistadas repatriaram uma carga de trabalho essencial residente na nuvem (em outras palavras, um aplicativo de alta prioridade ou um conjunto de aplicativos no qual a empresa depende) por vários motivos técnicos e operacionais.

Os seguintes exemplos foram relatados por organizações que implementaram aplicativos específicos na nuvem (nem todos eles são usuários do estudo):

- 27% retiraram aplicativos de gerenciamento de cadeia de suprimentos.
- 25% retiraram aplicativos de gerenciamento de relacionamento com o cliente.
- 24% retiraram aplicativos de Enterprise Resource Planning.

Mesmo entre as cargas de trabalho emergentes, as porcentagens foram amplamente consistentes:

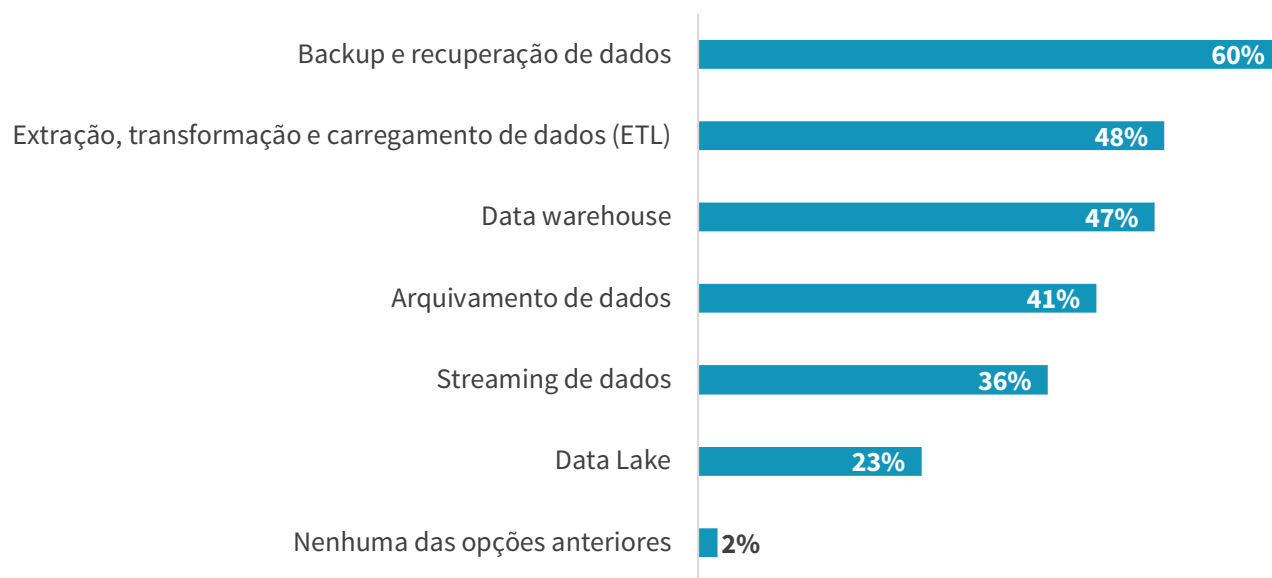
- 25% retiraram uma carga de trabalho de aprendizagem automática.
- 24% retiraram seus ambientes de data lake.
- 23% retiraram cargas de trabalho de lógica analítica de Big Data.
- 21% retiraram cargas de trabalho de aprendizagem profunda.

A dificuldade em implementar medidas de segurança, custos excessivos ou imprevisíveis, problemas de tecnologia e escalabilidade, e backup e recuperação de dados, seguidos de perto pelo arquivamento, são os principais motivos informados pelos entrevistados para repatriar cargas de trabalho. Seja qual for o motivo do repatriamento de um aplicativo específico, como mencionado, os processos de backup e recuperação "seguem" a carga de trabalho, nesse caso, de volta para o local.

Os entrevistados mencionam mais vezes a proteção de dados como uma das cargas de trabalho de gerenciamento de dados mais essenciais de sua organização. Muitas partes interessadas internas podem esperar que a proteção de dados aconteça por padrão, o que, obviamente, não ocorre devido aos muitos motivos que realçamos. No entanto, isso constitui uma exigência para que os profissionais de TI e as partes interessadas dos negócios discutam a função e os níveis de serviço necessários para funções ou aplicativos empresariais específicos, o que, por sua vez, informa a solução ideal que será implementada.

**Figura 2. O backup e recuperação de dados estão no topo da lista de cargas de trabalho de gerenciamento de dados essenciais**

**Quais das seguintes cargas de trabalho de gerenciamento de dados você classificaria como as mais essenciais em sua organização? (Porcentagem de entrevistados, N = 1.257, três respostas aceitas)**



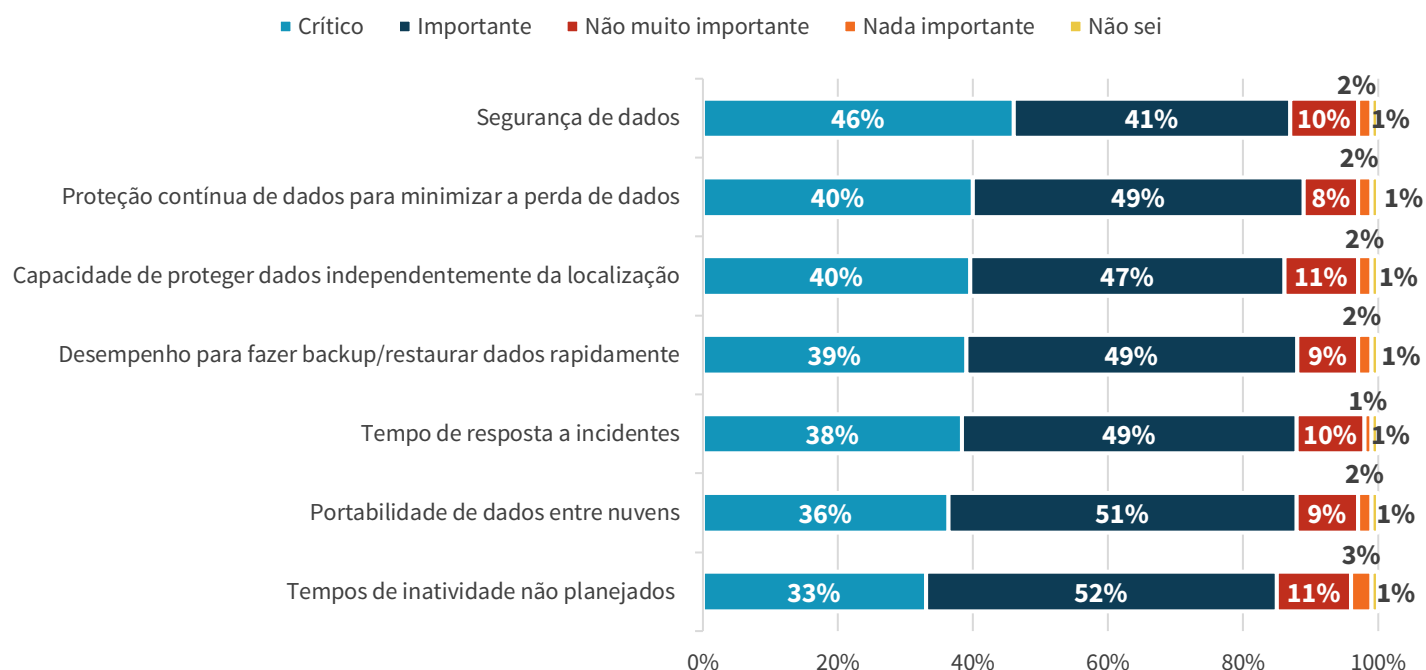
Fonte: Enterprise Strategy Group

## Proteção de dados como um fator essencial para o sucesso da nuvem híbrida

Embora 89% dos profissionais de TI sintam que a proteção contínua de dados é essencial para o sucesso da nuvem híbrida, 87% sentem o mesmo em relação à segurança de dados e à capacidade de proteger os dados independentemente da localização. Isso significa que a solução que eles implementam deve oferecer o tipo de agilidade e funcionalidade que abrange várias localizações, locais ou na nuvem, e topologias que possam seguir as cargas de trabalho. Então, não é de surpreender que a segurança de dados seja uma das principais preocupações das organizações entrevistadas pelo ESG, assim como a capacidade de reduzir a perda de dados ou atingir RPOs baixos.

### Figura 3. A proteção no local é importante para o sucesso na nuvem híbrida

Em sua opinião, qual a importância de cada uma das seguintes características do ambiente local de proteção de dados para alcançar um ambiente de nuvem híbrida eficaz? (Porcentagem de respondentes, N = 1.257)



Fonte: Enterprise Strategy Group

## Benefícios da proteção otimizada de dados para ambientes com várias nuvens

A proteção de dados evoluiu ao longo dos anos e passou por muitas inovações e iterações tecnológicas. Embora não tenhamos o intuito de apresentar uma lista completa neste artigo, com base na pesquisa e na especialização no domínio, o ESG geralmente define proteção “otimizada” de dados como ter a habilidade de realizar backup e recuperação avançada e rica em recursos de dados no local e na nuvem (a nuvem como destino ou como origem), inclusive de SaaS. Isso inclui a capacidade de proteger ambientes físicos e virtuais, bem como aplicativos em execução na infraestrutura de contêineres, e de otimizar o consumo de armazenamento com deduplicação. As soluções otimizadas de proteção de dados são projetadas para serem fáceis de usar, mas oferecem recursos avançados de gerenciamento e geração de relatórios e podem ser executadas como serviços. A proteção otimizada de dados está evoluindo para se tornar um gerenciamento inteligente de dados.

Por adotar uma perspectiva mais ampla sobre a nuvem, em parte, é possível definir que as estratégias bem-sucedidas de nuvem são aquelas com sólidos recursos de nuvem híbrida: a capacidade de escolher entre tecnologias de nuvem pública e nuvem privada de acordo com a carga de trabalho e as necessidades dos negócios, não com fatores arbitrários externos.

A TI deve prestar serviços de forma mais rápida em um mundo centrado na nuvem, mas também com mais economia. As tecnologias otimizadas de proteção de dados ajudam os departamentos de TI a atingir essas metas. Ao permitir que as organizações protejam os dados onde quer que eles residam,

com confiança, essas tecnologias deixam as organizações prontas para implementar novos serviços em nuvem (dentro ou fora do local) rapidamente, sabendo que os mecanismos de proteção por trás desses serviços as manterão protegidas. Para confirmar isso, quando o ESG perguntou aos entrevistados qual porcentagem dos projetos de nuvem é concluída depois do prazo, no prazo ou antes dele, as organizações com ambientes otimizados de proteção de dados relataram que concluem seus projetos antes do prazo com frequência 57% maior (33% em comparação com 21%).

### **Organizações com ambientes otimizados de proteção de dados relataram que concluem seus projetos antes do prazo com frequência 57% maior**

### **Organizações com ambientes otimizados de proteção de dados relataram que concluem seus projetos abaixo do orçamento com frequência 59% maior**

Grande parte do custo de qualquer projeto de nuvem é a mão de obra. O tempo dos desenvolvedores, arquitetos de TI, arquitetos de segurança e especialistas em proteção de dados é caro; portanto, a execução mais rápida dos projetos também significa que eles são feitos de forma mais econômica. Quando o ESG perguntou aos entrevistados qual porcentagem dos projetos de nuvem é concluída abaixo do orçamento, dentro do orçamento ou acima

dele, as organizações com ambientes otimizados de proteção de dados relataram que concluem seus projetos abaixo do orçamento com frequência 59% maior (27% em comparação com 17%).

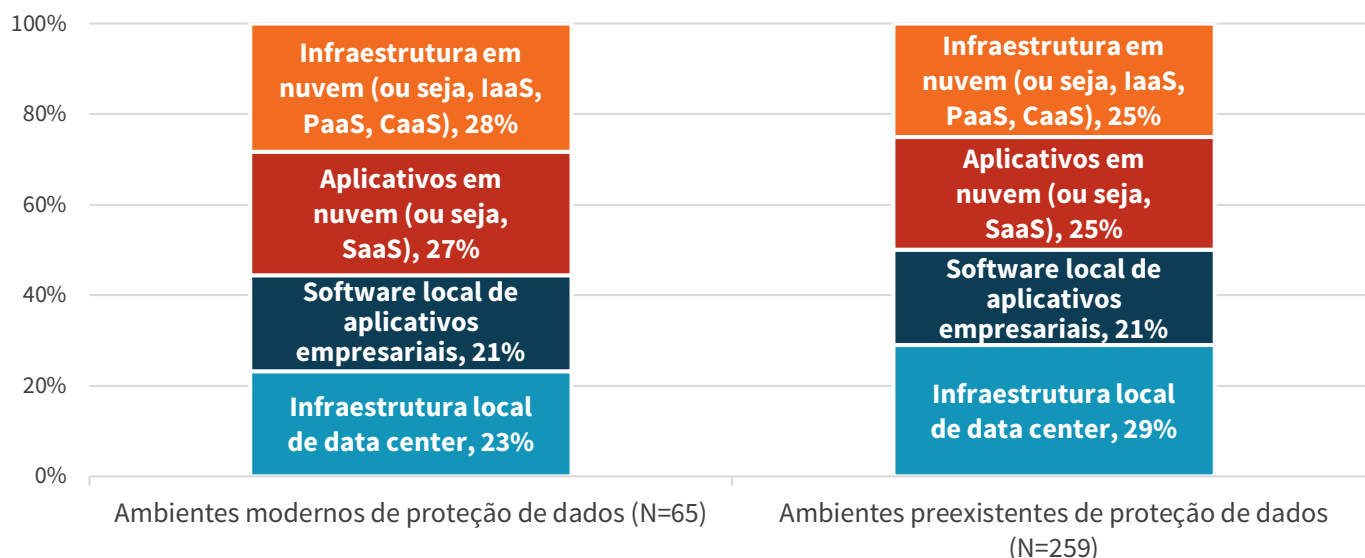
Os investimentos para otimizar a proteção de dados parecem compensar em redução dos gastos com infraestrutura local voltada para o futuro. Os ambientes “preexistentes” de proteção de dados estão alocando 26% a mais de orçamento para modernizar a infraestrutura local (29% em comparação com 23%). Com base na pesquisa anterior do ESG, o orçamento anual de TI de uma empresa média é de aproximadamente US\$ 167 milhões.<sup>2</sup> A oportunidade de realocar 6% do orçamento de TI (ou um pouco mais de US\$ 10 milhões para uma empresa média) para projetos mais estratégicos pode causar um grande impacto.

Uma forma de analisar esses dados como um usuário final é considerar que, se você tiver um ambiente sólido de proteção de dados, não terá que gastar dinheiro para atualizá-lo nem fazer upgrade dele. O gerenciamento do ambiente também será menos demorado. Tudo isso faz parte do motivo pelo qual vemos que esses departamentos de TI precisam alocar 6% a menos de seu orçamento para a infraestrutura local.

<sup>2</sup>Fonte: resultados da pesquisa principal do ESG, 2020 Technology Spending Intentions Survey, janeiro de 2020.

**Figura 4. Eficiências dos gastos com infraestrutura local**

**Aproximadamente, qual porcentagem do orçamento total de hardware e software de sua organização para 2020 será alocada para cada uma das seguintes categorias? (Média)**

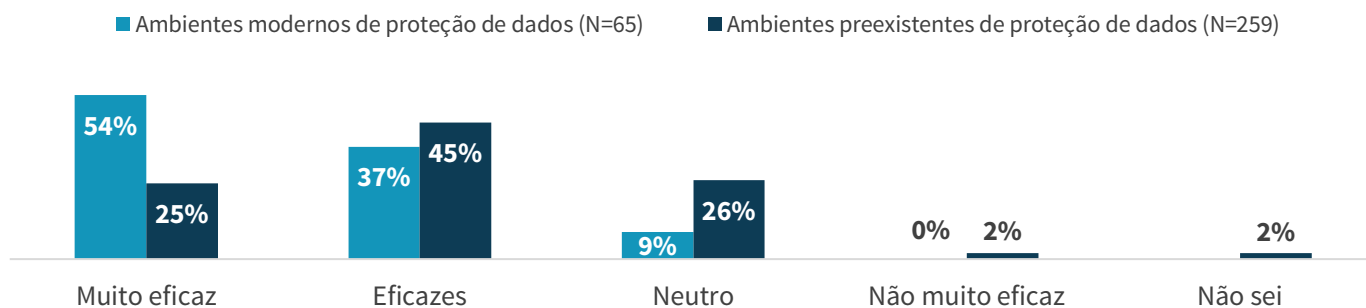


Fonte: Enterprise Strategy Group

A proteção de dados "toca" todos os aspectos da TI em virtude de sua missão e de sua centralização em dados. Parece lógico que ter uma solução otimizada de proteção de dados integrada ou como um ajuste à infraestrutura em evolução ajudará em termos de eficiência operacional, e não só em termos de proteção de dados. Nossa pesquisa realça que, de fato, 91% dos departamentos de TI com ambientes otimizados de proteção de dados relatam que são eficazes na geração de valor com iniciativas de nuvem híbrida (consulte a figura 5). Quando as necessidades de proteção de dados são atendidas e, também, perfeitamente e totalmente integradas em todos os ambientes, elas não só transformam a TI em um herói, mas também liberam o tempo essencial que pode ser gasto em outros lugares, administrando os negócios e conduzindo novas iniciativas.

**Figura 5. As iniciativas de nuvem híbrida são mais eficazes com o armazenamento moderno**

**De modo geral, como você diria que as iniciativas de nuvem híbrida de sua organização foram eficazes para gerar valor? (Porcentagem de entrevistados, por ambiente local de proteção de dados)**



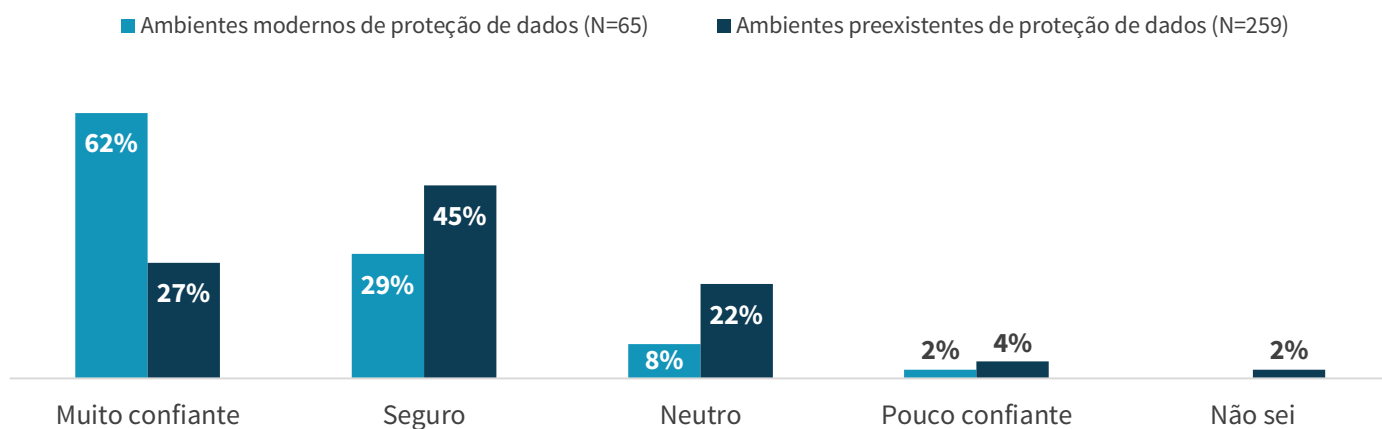
Fonte: Enterprise Strategy Group



Além disso, o sucesso anterior em atingir metas de nuvem híbrida graças à proteção otimizada de dados se traduz em um maior nível geral de confiança na capacidade de uma empresa de atingir suas metas de nuvem híbrida no futuro (consulte a figura 6). Três quintos (62%) das organizações com ambientes otimizados de proteção de dados têm muita confiança em sua capacidade de auxiliar as metas de nuvem híbrida nos próximos três anos, o que equivale a 2,3 vezes a frequência dos ambientes preexistentes de proteção de dados (consulte a figura 7). Além disso, os departamentos de TI de ambientes modernos de proteção de dados são 48% mais propensos que seus colegas de ambientes preexistentes a serem vistos como diferenciais competitivos pela diretoria (40% em comparação com 27%).

**Figura 6. Confiança na TI para auxiliar as metas de negócios para nuvem híbrida**

### O quanto você está confiante de que seu departamento de TI poderá auxiliar as metas de nuvem híbrida da empresa para os próximos 36 meses? (Porcentagem de entrevistados, por ambiente local de proteção de dados)



Fonte: Enterprise Strategy Group

## A grande verdade

As infraestruturas otimizadas de proteção de dados preparam o cenário para sucesso nos ambientes de nuvem híbrida e influenciam o sucesso comercial, técnico e financeiro, além da proteção de dados. Melhorar e otimizar as tecnologias de proteção de dados é uma etapa fundamental na preparação de uma organização para iniciativas bem-sucedidas de nuvem híbrida.

A proteção de dados é uma excelente base de aprendizado para a TI, pois abrange várias disciplinas de TI e deve cumprir os RPOs e RTOs, que podem ser rigorosos, para oferecer suporte à empresa e aos muitos aplicativos dos quais ela depende. As práticas recomendadas e as habilidades geradas com essa iniciativa podem ser aplicadas a muitos outros projetos.

Isso resulta em capacidades aprimoradas para obter sucesso em ambientes de nuvem híbrida e, ao mesmo tempo, aumentar a confiança do nível executivo. Este "ciclo virtuoso" também pode ser identificado em outras áreas. É interessante observar que, em comparação com organizações com infraestrutura preexistente de proteção de dados, aquelas com infraestrutura otimizada de proteção de dados também informam resultados positivos em projetos de nuvem em termos gerais e um maior valor de suas iniciativas de nuvem híbrida.

O futuro da TI é composto por topologias de nuvem híbrida e é nessa área que esperamos ver inovações contínuas na categoria de proteção de dados.

## Como a Dell Technologies pode ajudar

Este documento Research Insights do ESG foi encomendado pela Dell Technologies, pela VMware e pela Intel Corporation, empresas totalmente concentradas em ajudar as organizações a atingir suas metas de nuvem.

Juntas, a Dell Technologies, a VMware e a Intel Corporation estão gerando inovações e recursos de última geração com o mais amplo portfólio de soluções confiáveis de nuvem, infraestrutura e proteção de dados. Esse abrangente portfólio de hardware, software e serviços permite que as organizações adotem tecnologias transformadoras facilmente para maximizar o desempenho, competir e prosperar na nova economia digital.

As soluções Dell EMC Data Protection para nuvem, várias nuvens e nuvens híbridas ajudam os clientes a transformar seus data centers para possibilitar mais eficiência operacional, resiliência e escalabilidade em toda a infraestrutura em nuvem. Além disso, a Dell Technologies On Demand oferece o mais amplo portfólio completo do setor de soluções como serviço e com base em consumo, idealmente adaptadas para o modo como a infraestrutura e os serviços no local são consumidos na economia sob demanda.

Para saber mais sobre as soluções Dell EMC Data Protection para nuvem, comece [aqui](#).

## Apêndice – Metodologia da pesquisa e dados demográficos dos entrevistados

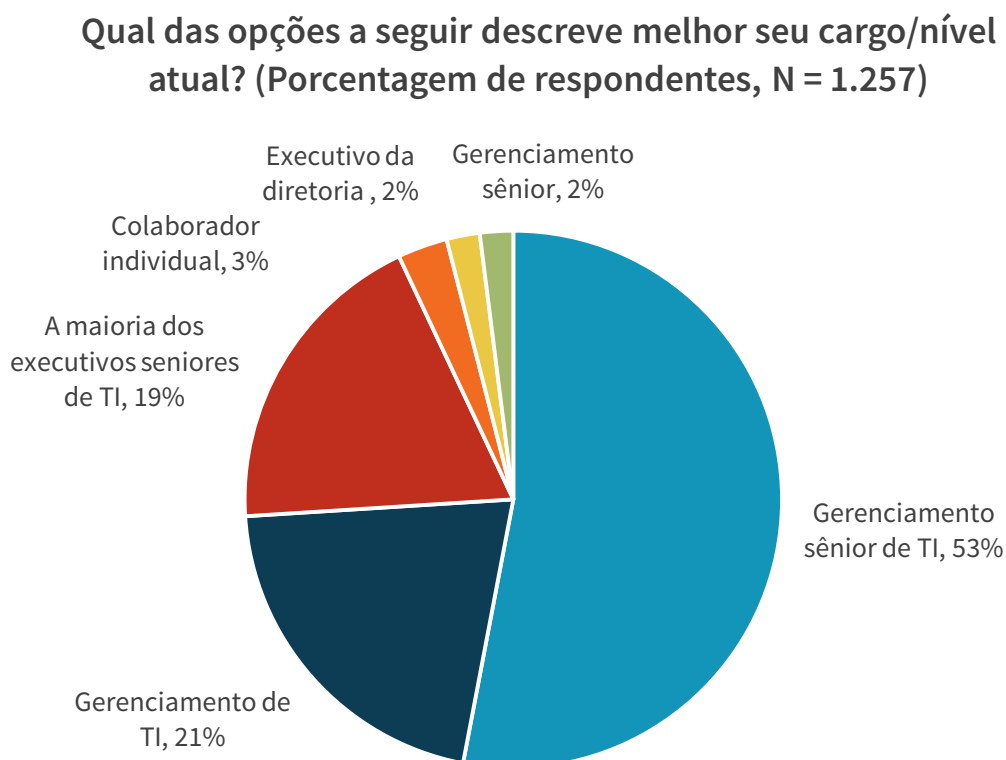
Para coletar dados para este relatório, o ESG conduziu uma pesquisa on-line abrangente com tomadores de decisão de TI de organizações dos setores público e privado de 11 países: EUA (33%), Canadá (4%), Reino Unido (13%), França (9%), Alemanha (7%), Singapura (5%), Austrália (5%), Índia (4%), Hong Kong (3%), Brasil (8%) e México (8%). A pesquisa ocorreu entre 17 de setembro de 2019 e 12 de outubro de 2019. Para qualificar-se a esta pesquisa, os entrevistados precisavam exercer influência sobre a compra de investimentos em nuvem (pública ou privada) em organizações que utilizam uma infraestrutura em nuvem pública e operam ambientes modernizados de data center no local.

Depois de filtrar os entrevistados não qualificados, remover as respostas duplicadas e fazer uma triagem das respostas restantes (de acordo com diversos critérios) para garantir a integridade dos dados, restou uma amostra final de 1.257 entrevistados.

Todos os entrevistados receberam um incentivo para responder à pesquisa na forma de prêmios em dinheiro e/ou equivalentes. Nota: os totais representados em números e tabelas neste relatório podem não chegar a 100% devido a arredondamentos.

Os números a seguir detalham os dados demográficos da base de entrevistados, inclusive as atuais responsabilidades individuais dos entrevistados em seus cargos atuais, bem como o número total de funcionários e o setor principal das organizações.

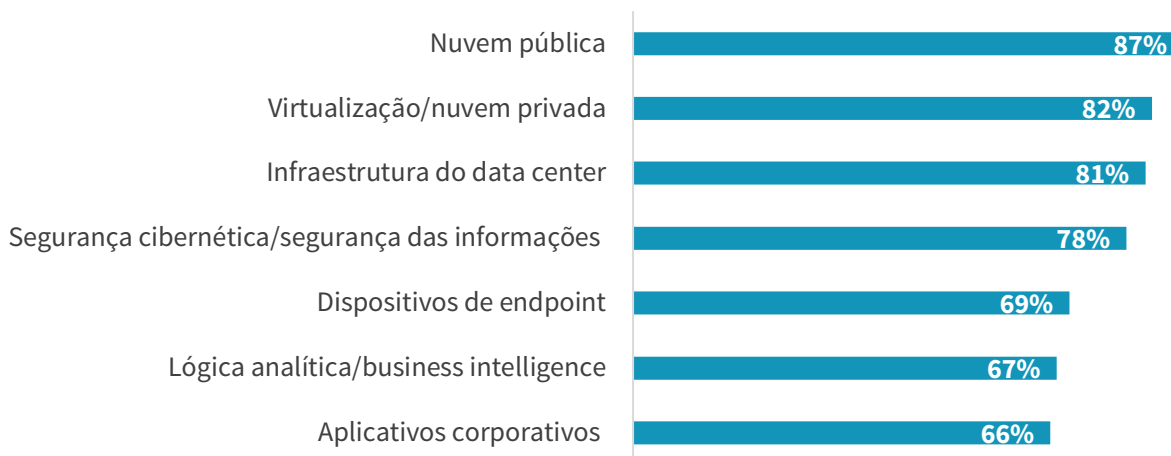
**Figura 7. Entrevistados por cargo/nível**



Fonte: Enterprise Strategy Group

**Figura 8. Entrevistados na pesquisa, por áreas de responsabilidade em TI**

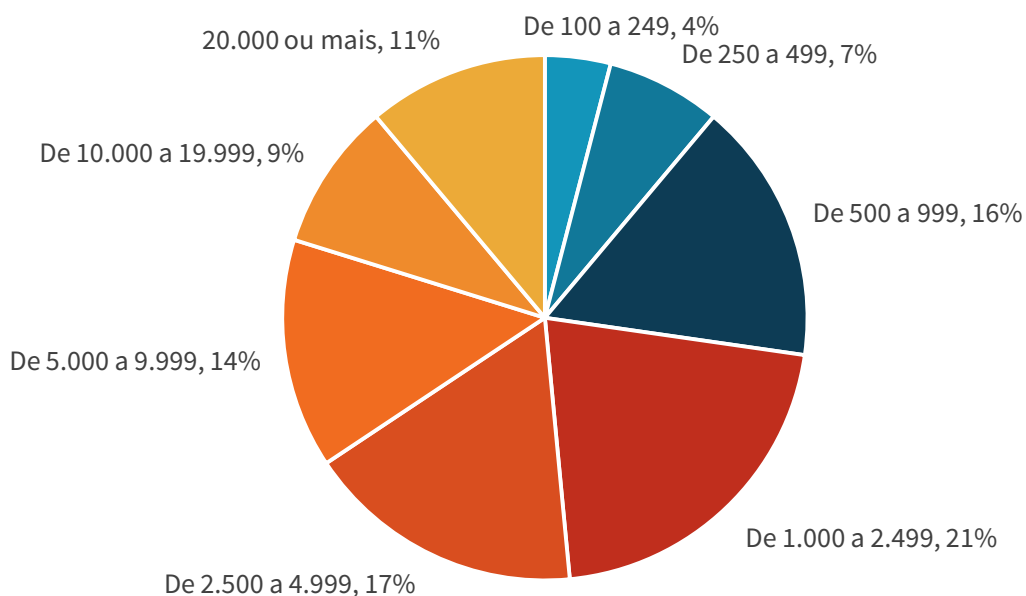
**Em qual das áreas de TI a seguir você tem um envolvimento significativo no processo de compra de sua empresa?  
(Porcentagem de entrevistados, N = 1.257, várias respostas aceitas)**



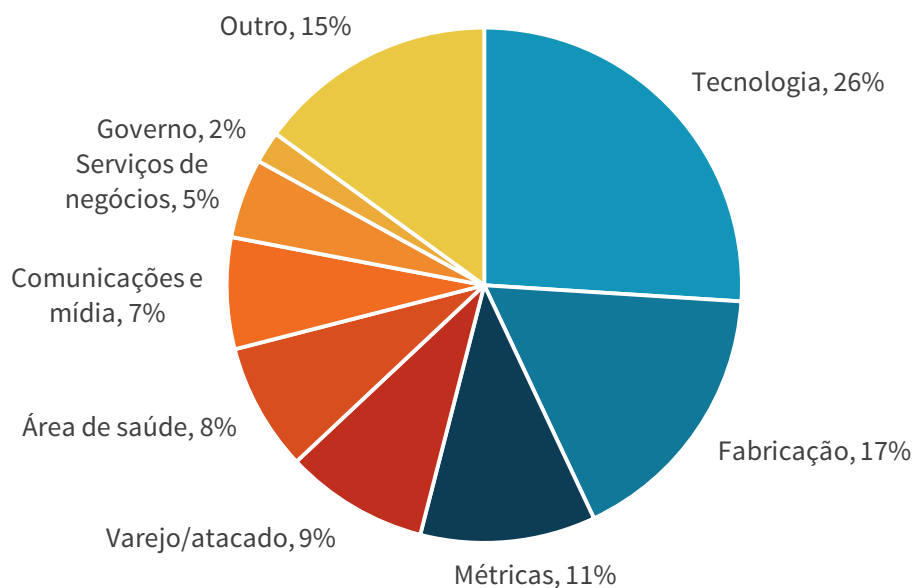
Fonte: Enterprise Strategy Group

**Figura 9. Entrevistados na pesquisa, por tamanho da empresa (número de funcionários)**

**Quantos funcionários, no total, sua organização tem em todo o mundo? (Porcentagem de respondentes, N = 1.257)**



Fonte: Enterprise Strategy Group

**Figura 10. Entrevistados na pesquisa, por setor****Qual é o principal setor de sua organização? (Porcentagem de respondentes, N = 1.257)**

Fonte: Enterprise Strategy Group

Todos os nomes de marcas comerciais pertencem às suas respectivas empresas. As informações contidas nesta publicação foram obtidas por fontes que The Enterprise Strategy Group (ESG) considera confiáveis, mas não são garantidas pela ESG. Esta publicação pode conter opiniões do ESG, as quais estão sujeitas a alterações. Esta publicação é protegida por direitos autorais do The Enterprise Strategy Group, Inc. Qualquer reprodução ou redistribuição integral ou parcial desta publicação, seja em formato impresso, eletrônico ou em qualquer outro formato, para pessoas não autorizadas a recebê-la e sem o consentimento expresso do The Enterprise Strategy Group, Inc. representa uma violação da lei de direitos autorais dos Estados Unidos e estará sujeita a uma ação por danos civis e, se aplicável, a processo criminal. Em caso de dúvidas, entre em contato com o Serviço de atendimento ao cliente do ESG pelo telefone 508.482.0188.



**Enterprise Strategy Group** é uma empresa de estratégias, validação, pesquisa e análise de TI que oferece inteligência de mercado e percepções úteis à comunidade global de TI.